
DC4EU project is Co-funded by the European Union ´s Digital Europe Programme
under Grant Agreement no. 101102611


# Deliverabe 5.1
# Business Blueprint (BBP)

**Version 2.0**

| | |
|---|---|
| Work package | WP 5 |
| Task | 5.1. Business Blueprint |
| Submission date | 26/12/2024 |
| Deliverable lead | Spanish Ministry for Digital Transformation and Civil Service |
| Version | 2.0 |
| Authors | Spanish Ministry for Digital Transformation and Civil Service |
| Reviewers | WP 5 Partners<br>DC4EU Work Package Leaders |

| | |
|---|---|
| Abstract | This document proposes the business requirements, scenarios, and interoperability requirements as well as use case governance model design. The Business Blueprint provides a roadmap for the successful implementation of the large-scale pilots in education and professional qualifications due to the integration of digital credentials into the European education and professional qualifications landscape. |
| Keywords | DC4EU, eID, EAA, eIDAS, EUDIW, EUDIW Toolbox, EBSI, dPKI, Trust, ID, IR, Issuer, LoA, LSP, PID, PRC, QR, TSP, VC, RP, Verifier, VP, Holder |

Co-funded by the European Union

## Document Revision History

| Version | Date | Description of change | List of contributors |
|---|---|---|---|
| V0.7 | 16/04/2024 | 1st drafty version of the deliverable for comments | WP5 tasks 1.1, 1.2, 1.4 leaders |
| V0.8 | 18/04/2024 | 1st version of the deliverable for comments | WP5 partners |
| V0.9 | 30/04/2024 | 2nd version of the deliverable for comments | DC4EU consortium (through WP leaders) |
| V1.0rc | 10/08/2024 | 3nd version of the deliverable for comments and approval | DC4EU SC |
| V1.0 | 17/08/2024 | Deliverable version to be published | WP1 |
| V2.0rc1 | 14/11/2024 | Implemented interim report observations | WP5 partners |
| V2.0rc2 | 21/11/2024 | Applied WP5 partners' observtions.Shared to WP leaders | DC4EU consortium (through WP leaders) |
| V2.0rc3 | 25/11/2024 | Applied WP leaders' obervations. Shared to SC | DC4EU SC |
| V2.0rc4 | 29/11/2024 | Applied SC' observations. | WP5 coordination |
| V2.0 | 01/12/2024 | Deliverable version to be published | WP1 |

## Deliverables version history and future releases

| Version | Date of submission or due date | Description | Version acceptance |
|---|---|---|---|
| V1 | 17/08/2024 | First version submitted to European Commission. | Changes requested during interim review |
| V2 | 26/12/2024 | Current version. Changes implemented after revision of deliverable v1. | Pending Commission's review. |
| VN | - | Subsequent versions if current version not accepted. | - |

Co-funded by the European Union

## DISCLAIMER

The information, documentation and figures available in this deliverable are written by the "Digital Credentials For Europe" (DC4EU) project's consortium under the EU's Digital Europe Programme under Grant Agreement No. 101102611 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.



| Project co-funded by the European Commission in the Digital Europe Programme | | |
|---|---|---|
| **Nature of the deliverable:** | **R** | |
| **Dissemination Level** | | |
| **PU** | Public, fully open, e.g. web | **x** |
| CL | Classified, information as referred to in Commission Decision 2001/844/EC | |
| CO | Confidential to DC4EU project and Commission Services | |

** R: Document, report (excluding the periodic and final reports)*
*DEM: Demonstrator, pilot, prototype, plan designs*
*DEC: Websites, patent filings, press and media actions, videos, etc.*
*OTHER: Software, technical diagram, etc.*

## EXECUTIVE SUMMARY

The DC4EU WP5 Business Blueprint is a strategic document developed to guide the integration and adoption of digital credentials across the European Union, enhancing the digital transformation of education and professional qualifications. This blueprint aligns with the European Commission's 2030 Digital Education Action Plan, focusing on interoperability, accessibility, quality assurance, sustainability, and stakeholder engagement.

Interoperability: The blueprint proposes the creation of a unified framework that ensures the seamless integration of digital credentials across EU member states. It leverages standards such as eIDAS and the European Digital Identity Wallet to facilitate cross-border educational and professional mobility.

Accessibility and Inclusion: It aims to make digital learning and credentialing systems universally accessible, enabling all European citizens to participate in and benefit from the digital economy. This involves removing barriers for underserved communities and developing multilingual systems to cater to all EU citizens.

Quality Assurance and Trust: The blueprint emphasizes the implementation of robust quality assurance mechanisms to standardize the validation of digital credentials. This will enhance trust among institutions, employers, and learners, ensuring that credentials are recognized and respected across borders.

Sustainability and Scalability: The document outlines plan to build sustainable, scalable systems capable of adapting to emerging technologies and evolving educational needs. This includes piloting innovative technologies such as electronic ledger for secure and transparent credential verification.

Stakeholder Engagement and Collaboration: A key aspect of the blueprint is fostering collaboration across public and private sectors to support innovation in educational technologies and practices. This collaborative approach is vital for the development of practical and, effective solutions that can be implemented on an EU-wide scale.

Strategic Actions:

- Establish clear legal and governance frameworks to support the digital credentialing ecosystem.
- Enhance quality assurance processes to maintain high education standards across the EU.
- Promote equity by developing inclusive, accessible educational technologies.
- Conduct pilot tests to refine solutions, followed by scaling successful practices across member states.
- Implement continuous monitoring and evaluation to assess the effectiveness of implemented strategies and make necessary adjustments.

Co-funded by the European Union

Expected Outcomes:

- A standardized, EU-wide digital credential system that is secure, interoperable, and widely recognized.
- Enhanced mobility for students and professionals across the EU.
- Improved alignment of educational outcomes with labour market needs, facilitating smoother career transitions and skill verification.

By addressing these strategic areas, the DC4EU WP5 Business Blueprint aims to foster a cohesive and inclusive European educational space that leverages digital innovation to improve learning outcomes, employability, and system efficiencies. This initiative not only supports the educational and professional development of EU citizens but also contributes significantly to the EU's competitiveness in the global digital economy.

The document provides a comprehensive business view of the EUDIW ecosystem in the context of education and professional qualifications, covering the following aspects:

☐ Chapter 1: Business blueprint introduction and objectives - Outlines the purpose, vision and scope of implementing trust frameworks for digital credentials in European education and professional qualifications. Establishes key objectives including facilitating cross-border recognition, ensuring compliance with EU regulations, supporting interoperability, and promoting trust and security. Details the alignment with European strategies and analyzes impacts across stakeholder groups including educational institutions, students, professional bodies and employers.

☐ Chapter 2: The European Education and Qualifications Landscape - Analyzes the complex and diverse landscape of education systems across Europe, examining approaches to institutional licensing, credential issuance, and data management. Details regulated education levels, administrative practices, and the challenges of current digital solutions. Explores how digitalization creates opportunities for improved credential management while respecting national autonomy and educational traditions.

☐ Chapter 3: Current challenges and needs in educational and professional credential management - Examines key challenges in managing educational credentials across Europe including credential verification difficulties, recognition of qualifications, data interoperability issues, and varying technological infrastructure. Details stakeholder needs and concerns while highlighting opportunities for digital solutions to enhance trust, efficiency and mobility.

☐ Chapter 4: Operational Model - Presents a comprehensive framework for managing educational and professional credentials, implementing a non-delegated trust model that maintains institutional autonomy while ensuring interoperability. Details credential lifecycle management, roles and responsibilities, compliance monitoring, and infrastructure requirements. Outlines benefits including enhanced mobility, streamlined operations, and improved security.

☐ Chapter 5: Natural persons and legal entities onboarding process - Provides detailed procedures for onboarding students, professionals and organizations into the digital credential

ecosystem. Covers admission, enrollment and credential issuance phases for educational institutions, and registration, verification and authorization processes for professional bodies. Includes technical requirements, user journeys and implementation guidelines.

☐ Chapter 6: The education and professional qualifications sectorial rulebook - The education and professional qualifications sectorial rulebook aims to establish a standardised approach for managing digital educational and professional credentials within the European Union. The rulebook sets the foundation for trusted digital credential management, encompassing identity, trust, data models, and operational processes. This framework balances member state sovereignty with European integration needs, creating a unified system that supports educational mobility while respecting national and institutional autonomy.

☐ Chapter 7: Use Cases and implementation scenarios - Presents real-world applications demonstrating how the trust framework operates in practice. Details specific use cases for non-foundational identity credentials, learning achievements, and professional qualifications. Each use case includes context, actors, processes, benefits, challenges and technical requirements. Demonstrates practical value through detailed user journeys.

☐ Chapter 8: Technical framework and sectorial EAA's catalogue - Details the technical architecture implementing W3C Verifiable Credentials and European Learning Model standards. Covers core data models, country-specific extensions, implementation guidelines and maintenance requirements. Includes visual representations of system components and business flows to illustrate technical concepts for stakeholders.

☐ Chapter 9: Data models - The data models section provides standardised structures for representing educational and professional credentials, ensuring consistency and interoperability across European systems. This includes detailed specifications for various credential types, from educational qualifications to professional certifications, supporting the technical implementation of the trust framework. The models address both core European requirements and country-specific needs, enabling credential portability while maintaining compliance with national regulations.

☐ Chapter 10: Implementation roadmap - Provides a structured approach for adopting the trust framework across EU member states in four phases: preparation and assessment, pilot implementation preparation, full-scale rollout, and ongoing management. Details key activities, success metrics and evaluation criteria for each phase while ensuring alignment with EU regulations and initiatives.

☐ Annexes - Comprise detailed supporting materials including: (A) Comprehensive glossary defining key technical and domain-specific terms, (B) Technical diagrams illustrating key business flows and system relationships, (C) Detailed data models for credentials and identifiers, and (D) References to relevant EU regulations and frameworks governing digital credentials and identity.

Co-funded by the European Union

# CONTENT

## Table of Contents



Co-funded by the European Union

Co-funded by the European Union

Co-funded by the European Union

## List of acronyms and abbreviations

BBP - Business Blueprint
BFUG - Bologna Follow-up Group
BQM - Basic Quality Management
CGCOM - General Council of Official Medical Colleges (Consejo General de Colegios Oficiales de Médicos)
COM - Doctors' Official College (Colegio Oficial de Médicos)
CPD - Continuous Professional Development
DC4EU - Digital Credentials for Europe
DEAP - Digital Education Action Plan
DID - Decentralized Identifier
DLT - Distributed Ledger Technology
DUO - Dutch Education Executive Agency
EBSI - European Blockchain Services Infrastructure
EDCI - Europass Digital Credentials Infrastructure
EDSSI - European Digital Student Service Infrastructure
EEA - European Education Area
EHEA - European Higher Education Area
eIDAS - Electronic Identification, Authentication and Trust Services
ELM - European Learning Model
ELMO - European Learner Mobility Ontology
EMREX - Electronic Data Exchange in Higher Education
EQF - European Qualifications Framework
ESCO - European Skills, Competences, Qualifications and Occupations
ESI - European Student Identifier
EU - European Union
EUDI - European Digital Identity
EUDIW - European Digital Identity Wallet
EWP - Erasmus Without Paper
FMC - Further Medical Competence
GDPR - General Data Protection Regulation
IMI - Internal Market Information System
ISCED - International Standard Classification of Education
KPI - Key Performance Indicator
LSP - Large Scale Pilot
OOP - Once-Only Principle
PID - Personal Identity Data
PQD - Professional Qualifications Directive
QR - Quick Response
SDG - Single Digital Gateway
SEAFORMEC - Spanish Foundation for Medical Education and Training Accreditation
TAO - Trusted Accreditation Organization
UEMS - European Union of Medical Specialists
VC - Verifiable Credentials
VPC - Validation of Professional Competence

Co-funded by the European Union

W3C - World Wide Web Consortium
W3C-VC - W3C Verifiable Credentials
W3C-VCDM - W3C Verifiable Credentials Data Model
WP - Work Package

Co-funded by the European Union

# Executive summary

## Purpose and Scope

This Business Blueprint provides a comprehensive framework for implementing trusted digital credentials across European educational and professional qualification sectors. It addresses the growing need for secure, verifiable, and portable digital credentials that can be easily shared and verified across borders while maintaining privacy and institutional autonomy.

## Key Challenges Addressed

The framework addresses several critical challenges in European education and professional qualifications:

1. Cross-Border Recognition
   - Difficulty in verifying qualifications across different countries
   - Time-consuming manual verification processes
   - Varied national requirements and standards
2. Administrative burden
   - Resource-intensive credential management
   - Complex verification procedures
   - Redundant documentation requirements
3. Credential security
   - Risk of credential fraud
   - Need for secure verification methods
   - Privacy protection requirements

## Solution Overview

The framework implements a non-delegated trust model where educational institutions and professional bodies maintain direct control over their credentials while ensuring EU-wide recognition. Key features include:

1. Standardized Digital Credentials
   - Common format across European institutions
   - Support for multiple languages
   - Privacy-preserving verification
2. Institutional Autonomy
   - Direct control over credential issuance
   - Maintained institutional identity
   - Flexible implementation options
3. Cross-Border Compatibility
   - Seamless qualification recognition
   - Standardized verification processes
   - Support for professional mobility

Co-funded by the European Union

### Benefits for Stakeholders

- Educational Institutions
  - Reduced administrative costs
  - Enhanced credential security
  - Streamlined student mobility
  - Simplified verification processes
- Students and Professionals
  - Easy sharing of qualifications
  - Protected privacy
  - Improved mobility opportunities
  - Lifelong learning support
- Employers and Professional Bodies
  - Quick credential verification
  - Reduced hiring risks
  - Enhanced talent mobility
  - Efficient qualification checking

### Implementation Approach

The framework provides a phased implementation roadmap:

1. Preparation and Assessment
   - Stakeholder engagement
   - Infrastructure evaluation
   - Regulatory compliance review
2. Pilot Implementation
   - Controlled testing
   - Process refinement
   - User feedback collection
3. Full-Scale Rollout
   - Phased deployment
   - Training and support
   - System integration
4. Continuous Improvement
   - Regular monitoring
   - Performance optimization
   - Stakeholder feedback integration

### Regulatory Alignment

The framework aligns with key European regulations and initiatives:

- eIDAS Regulation (EU) 2024/1183
- General Data Protection Regulation (GDPR)
- Single Digital Gateway Regulation

- European Education Area objectives
- Digital Education Action Plan

### Document Navigation

This Business Blueprint is organized into nine chapters:

0. Learning Belongs to the Learner: Introduction through a student's journey, demonstrating how the framework empowers learners to control their educational achievements
1. Introduction: Context, vision, and objectives
2. European Education Landscape: Current state analysis
3. Challenges and Needs: Problem space definition
4. Operational Model: Framework structure and governance
5. Onboarding Process: Implementation procedures
6. Use Cases: Practical applications and scenarios
7. Technical Framework: Data models and architecture
8. Implementation Roadmap: Deployment guidance

Supporting annexes provide detailed technical specifications, process flows, and regulatory references.

### Expected Outcomes

Implementation of this framework will deliver:

- Enhanced educational and professional mobility
- Reduced administrative costs
- Improved credential security
- Better support for lifelong learning
- Increased European educational integration

This Business Blueprint provides educational institutions, professional bodies, and other stakeholders with the guidance needed to implement secure, efficient digital credential management while supporting European educational and professional mobility objectives.

Co-funded by the European Union

# Chapter 0: The learning belongs to the learner

## A student's journey

Meet Jacob, a bright student from Malta with aspirations to pursue a Master's degree in the Netherlands. His academic record speaks of excellence, having graduated from one of Europe's most prestigious universities. Yet, what should have been a straightforward application process turned into a maze of bureaucratic hurdles and unexpected costs.

The first shock came when Jacob contacted his former university to obtain his degree credentials. Despite having paid substantial tuition fees throughout his studies, he discovered he needed to pay an additional fee merely to access his own academic records through their proprietary system. This payment wasn't just a small administrative cost - it represented an unexpected financial burden for a recent graduate.

But the challenges didn't end there. After paying the fee and sharing his credentials with the Dutch university, Jacob faced a new obstacle. The receiving institution couldn't verify his qualifications through the digital service provided. The system, though modern in appearance, lacked cross-border recognition. What's more, the Dutch university couldn't authenticate the digital identity of Jacob's former institution.

Weeks turned into months as university staff manually processed his application. They made numerous phone calls, sent countless emails, and spent considerable time researching the equivalence of his courses. All this effort to verify information that should have been readily available and trustworthy.

These challenges are systematically addressed through the operational model detailed in Chapter 4 and the technical framework outlined in Chapter 8.

## The root of the problem

Jacob's experience brings to light several critical issues in current educational systems:

1. Ownership and access rights
    - Students must pay to access their own academic achievements
    - Universities maintain exclusive control over educational records
    - Learners lack sovereignty over their own educational data

2. Trust and verification
    - No standard method exists for cross-border credential verification
    - Manual processes dominate verification procedures
    - Digital solutions remain fragmented and incompatible

Co-funded by the European Union

3. Data portability
   - Educational records stay locked within institutional systems
   - No common format exists for sharing credentials
   - Students cannot easily transfer their records between institutions

## The educational journey: two perspectives

From an institutional viewpoint, education appears as distinct segments. Each school, university, and training centre operate independently, maintaining separate systems, different credential formats, and unique verification processes. These institutions see only their piece of a student's educational path.

Yet for students like Jacob, education forms one continuous journey. From primary school through university and into professional life, each achievement builds upon previous ones. This personal learning path knows no institutional boundaries - it's a single story of growth and development.

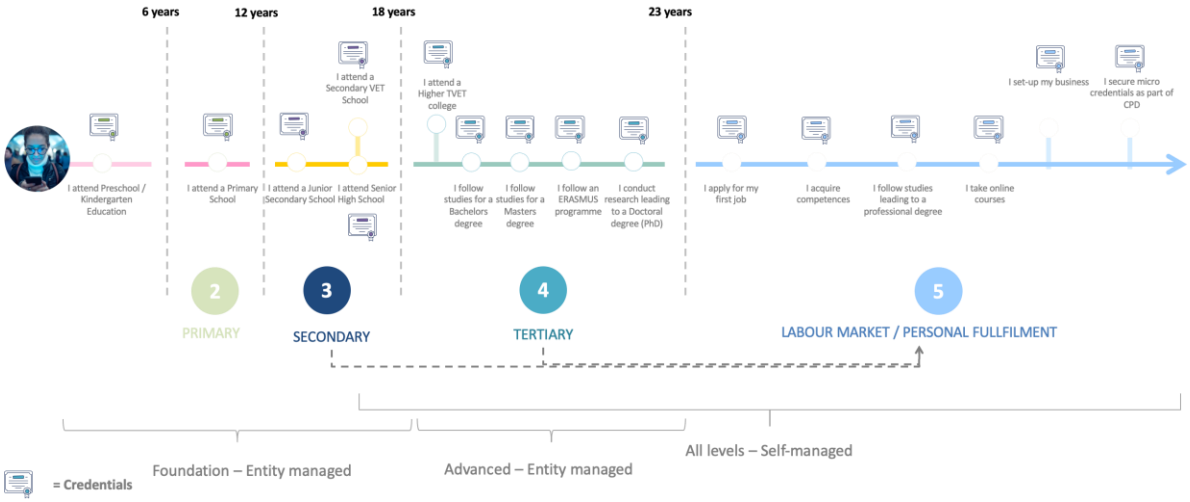



*figure 1 - educational journey*

The European educational space adds another layer of complexity. Different directorates manage various aspects of education, each with its own systems and requirements. This fragmentation makes cross-border mobility particularly challenging for students and professionals.

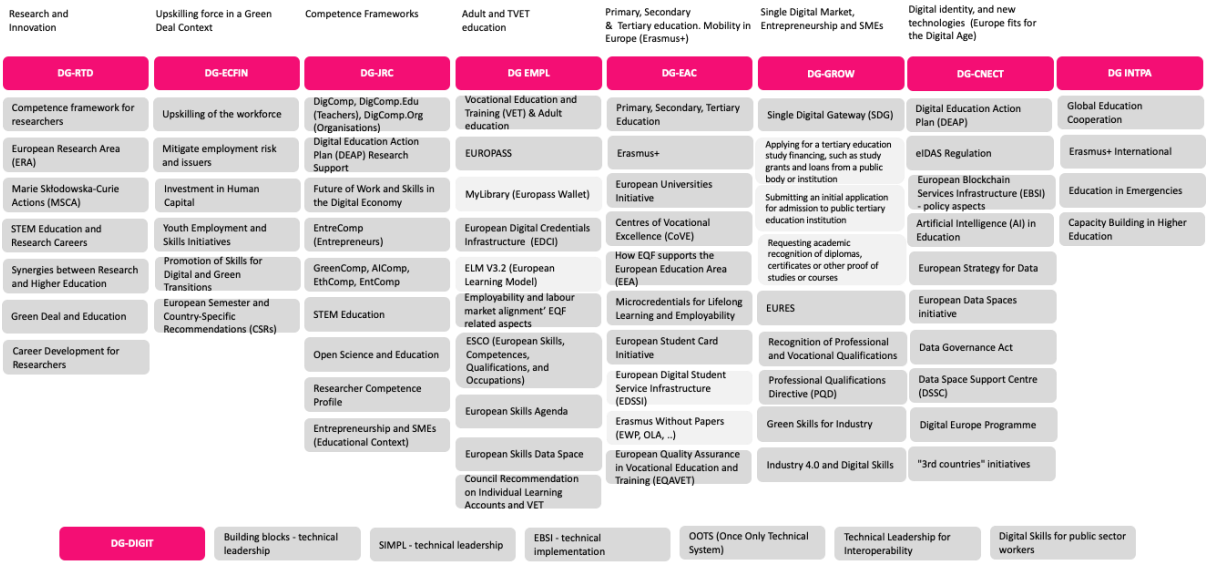



*figure 2 - EC educational landscape*

## A new paradigm through eIDAS 2.0

The European Digital Identity framework (eIDAS 2.0) introduces revolutionary changes to address these challenges. At its core sits the European Digital Identity Wallet - a secure digital container where citizens can store and manage their credentials.

For students like Jacob, this means:

- Complete control over their educational records
- Instant sharing capabilities with any institution
- Guaranteed acceptance across European borders
- Privacy protection by default

The wallet works alongside a comprehensive trust infrastructure that:

- Validates credentials without compromising privacy
- Supports existing educational frameworks
- Enables automatic verification
- Functions across borders and institutions

## DC4EU: Making it real

The DC4EU project focuses on turning this vision into reality for education and professional qualifications. Through detailed technical specifications and practical implementations, it demonstrates how:

- Students can store all their qualifications in their personal wallet
- Universities can issue and verify credentials instantly
- Employers can trust and verify qualifications easily

Co-funded by the European Union

- Professional bodies can recognise qualifications across borders

The technical infrastructure includes:

- Standard formats for educational credentials
- Secure verification protocols
- Privacy-preserving mechanisms
- Cross-border recognition systems

This infrastructure ensures that:

- Credentials remain valid and verifiable
- Privacy stays protected
- Institutions maintain their authority
- Students control their data

Through these changes, learning truly returns to the learner. Students like Jacob will no longer face unnecessary barriers when pursuing their educational goals. They'll have full control over their achievements while institutions maintain their role as trusted credential issuers.

The practical implementation of these solutions is demonstrated through the use cases in Chapter 7, with specific guidance for adoption provided in Chapter 8.

Co-funded by the European Union

# Chapter 1: Introduction

The European education system faces a significant change in how academic and professional qualifications are managed. As students and professionals become more mobile, the need for trusted digital credentials grows. This chapter outlines a comprehensive approach to digital credentials that serves the entire European education community.

## 1.1 Building a new approach to credentials

Digital credentials represent a step forward in how we handle qualifications across Europe. When a student completes their studies at a university in one European country and applies for a job in another, their qualifications need to be trusted and easily verified. Our blueprint shows how this can work.

The education sector needs common rules for creating and managing digital versions of qualifications. These rules ensure that a digital degree carries the same trust as a traditional paper diploma. A university in Spain issuing a digital degree needs to know that employers and universities in Germany or Poland will recognise and trust that credential.

Digital verification removes barriers to mobility. Rather than waiting weeks for paper documents to be checked and translated, organisations can verify qualifications immediately. This makes it easier for people to study and work across Europe while maintaining the high standards that education requires.

Educational institutions and professional bodies need practical guidance to make this change. The blueprint provides step-by-step instructions for moving from paper to digital credentials. It explains what systems institutions need and how they can work together across borders.

## 1.2 Creating trust in digital education

Trust in educational credentials comes from clear rules and reliable processes. A medical student graduating in France needs their digital qualification to be accepted by hospitals in Sweden or medical authorities in Italy. This trust stems from common standards in how credentials are created, shared, and checked.

Digital credentials change how educational organisations work together. A university can share student records securely with another institution. Professional bodies can check qualifications instantly. Employers can verify degrees without lengthy correspondence. These connections rely on clear agreements about who can do what within the system.

Co-funded by the European Union

Personal information in educational records needs protection. When a student shares their degree with a potential employer, they should control exactly what information is shared. The system protects privacy while making verification simple. Students choose when to share their credentials, and organisations can check only what they need to see.

Moving qualifications across borders becomes straightforward. A degree earned in one country can be understood and trusted in another because the digital credential includes standardised information. This helps students continue their studies in different countries and professionals practice their careers across Europe.

## 1.3 Supporting the education community

Different parts of the education system need different support for digital credentials:

Universities and colleges face particular challenges with student records. They need to issue thousands of degrees and transcripts each year. Digital credentials allow them to move away from printing and posting paper documents. When a student graduates, their digital degree can be shared instantly with employers or other universities.

Professional training organisations provide specialised qualifications. Their certificates need to show exactly what someone has learned and can do. Digital credentials can include detailed information about skills and knowledge, linking directly to professional standards. This helps employers understand exactly what a qualification means.

Schools need efficient ways to record student achievements. Digital diplomas make it easier for students to apply to universities or start their careers. Their grades, courses, and achievements become part of a secure digital record that follows them through their education.

## 1.4 Connecting with Europe's Digital Future

The European Union aims to make education more accessible across borders. Our approach to digital credentials supports these plans in several ways:

The European Education Area promises to remove barriers between national education systems. Digital credentials help deliver this promise. A student with a bachelor's degree from Greece can apply to a master's programme in Denmark without waiting weeks for paperwork. Their digital credentials provide immediate proof of their qualifications.

Different countries have different ways of describing qualifications. Digital credentials solve this by using common European reference points. When a university in Poland issues a degree, the digital credential includes information that makes sense to universities and employers across Europe. This makes it easier to understand what someone has learned and what they can do.

Co-funded by the European Union

Learning now happens throughout life, not just in traditional education. People take courses, gain certificates, and develop new skills continuously. Digital credentials create a complete record of these achievements. Someone might have a university degree, professional certifications, and specialised training – all stored securely in their digital wallet.

Digital education needs reliable records. As more learning happens online, we need trusted ways to record achievements. Digital credentials provide this trust through secure technology and clear standards. Whether someone completes an online course or a traditional degree programme, their digital credential proves their achievement.

## 1.5 Making a difference

Digital credentials change how people manage their education and careers:

For students and working professionals, control over educational records becomes simpler. Their digital wallet holds all their qualifications securely. When applying for jobs or further study, they choose what to share. The system protects their privacy while making it easy to prove their achievements.

Educational institutions gain new efficiency. Issuing and checking qualifications becomes faster and more reliable. Instead of processing paper documents, they can verify credentials instantly. This saves time and money while improving service to students.

The changes support people moving between countries and institutions. A digital credential proven valid in one country works across Europe. This helps people study where they choose and work where they are needed.

Let me continue with the narrative transformation:

## 1.6 Managing changes to qualifications

Sometimes qualifications need to be changed or withdrawn. Different European countries handle this in different ways, and our system adapts to these national approaches:

When fraud is discovered, qualifications must be cancelled. The digital system makes this process clear and effective. If someone obtained a qualification dishonestly, the issuing institution can cancel it. This cancellation becomes visible immediately to anyone checking that credential, protecting the value of genuine qualifications.

National rules about cancelling qualifications vary. Some countries have strict legal processes, others give more authority to educational institutions. The digital system

works with these different approaches. When a qualification's status changes in one country, this information becomes clear to organisations across Europe.

Some countries allow qualifications to be suspended temporarily. This might happen during an investigation into serious concerns. Where national laws permit suspension, the digital system supports it. The qualification's status shows clearly to anyone checking it, but the system protects individual rights by following proper procedures.

## 1.7 Building connections

Digital credentials create new ways for organisations to work together:

Educational institutions share information more effectively. When a student moves from one university to another, their digital credentials show exactly what they have studied. The receiving institution can check these credentials instantly, making transfers simpler for everyone involved.

Professional bodies and educational institutions work closely together. Professional organisations set standards for entering their professions, and educational institutions prepare students to meet these standards. Digital credentials make it clear when qualifications match professional requirements.

Employers need to trust qualifications quickly. Whether checking a university degree or professional certification, they need reliable information. Digital credentials provide this assurance instantly, speeding up recruitment while maintaining high standards.

## 1.8 Running the system

Making digital credentials work across Europe requires clear organisation:

Each institution maintains control of its own credentials. Universities and professional bodies issue their own qualifications, following common standards that make their credentials work across Europe. This preserves their independence while ensuring their credentials work everywhere.

National authorities keep their role in education. Each country continues to set its own rules for education and professional qualifications. The digital system works within these national frameworks while making cross-border recognition possible.

European-level coordination helps everything work together. Common standards and practices make qualifications work across borders. Regular checks ensure the system stays effective, and feedback from users leads to improvements that keep it practical and useful.

Co-funded by the European Union

Security remains central to everything. The system protects personal information while allowing necessary verification. Strong security features prevent fraud and maintain trust in qualifications. When people share their credentials, both privacy and security are protected.

# Chapter 2: The European education and qualifications landscape

The European education and qualifications landscape presents a complex and diverse picture, characterised by varied approaches across member states. As digital technologies advance, this sector faces significant challenges and opportunities for transformation.

This chapter explores the complex landscape of education and qualifications across EU Member States, highlighting the decentralised authority that shapes each country's approach to credential issuance, verification, and recognition. By identifying the varied administrative processes, regulatory frameworks, and licensing requirements, this chapter underscores the challenges and opportunities for implementing a unified digital credential system. Understanding these diverse structures is crucial for developing solutions that respect national autonomy while facilitating cross-border educational and professional mobility.

## 2.1 Decentralised authority and Member State autonomy

One of the defining features of the European education system is its balanced approach between national autonomy and coordinated standards. The Bologna Process, initiated in 1999, established a crucial framework for harmonizing higher education systems while respecting member states' educational sovereignty. This process created the European Higher Education Area (EHEA), implementing key tools like:

- A common three-cycle system (Bachelor's/Master's/Doctorate)
- The European Credit Transfer and Accumulation System (ECTS)
- The Diploma Supplement
- Shared quality assurance standards

While education remains primarily under member state jurisdiction per the principle of subsidiarity, the Bologna Process provides a voluntary framework that has successfully standardized many aspects of higher education. This achievement demonstrates how European cooperation can respect national autonomy while creating effective common standards.

Unfortunately, neither the Bologna Process nor the Lisbon Recognition Convention provides specific rules dedicated to digital credentials. However, both frameworks create a foundation that can be adapted to incorporate and support the recognition and use of digital credentials within the European Higher Education Area (EHEA).

The absence of a single European-level body governing education standards has led to a rich variety of educational approaches across the continent. Each member state maintains its own system for curriculum design, assessment methods, and qualification recognition. This autonomy allows countries to tailor their educational systems to their specific cultural, economic, and social needs. For example, the German dual education system, which combines apprenticeships in a company with vocational education at a vocational school, reflects the country's strong emphasis on practical skills and industry involvement in education.

However, this autonomy also presents challenges for cross-border recognition of qualifications and student mobility. A degree or qualification that is well-understood and valued in one country may not be easily recognised or appreciated in another. This can create barriers for students wishing to study abroad or professionals seeking employment in different EU countries (National differences in qualification frameworks create administrative barriers for students studying abroad and professionals seeking work in other member states).

The operational model addressing these varying requirements is detailed in Chapter 4, with specific technical solutions presented in Section 7.3.

## 2.2 Regulated education levels and licensing requirements

Analysis of 17 DC4EU participant countries shows the following licensing requirements:

- Universities: 100% require licensing
- Universities of Applied Sciences: 88% require licensing
- General upper secondary education: 88% require licensing
- Technical and Vocational Education: 82% require licensing
- Primary education: 81% require licensing
- Liberal adult education: 46% require licensing

These figures show high regulation levels in formal education sectors. Liberal adult education sees lower regulation rates due to its broader scope and non-formal structure.

## 2.3 Approaches to licensing educational institutions

Educational institution licensing follows three primary models across member states:

- Centralised model: Ministry-level institutions manage licensing, with authority distributed among departments by education level. This represents the most common approach among surveyed countries.
- Regional model: Federal states such as Germany assign licensing authority to regional governments. Each region maintains independent educational licensing systems under national guidelines.

Co-funded by the European Union

- Mixed model: Some member states combine central and regional authority. Sweden exemplifies this approach, with municipalities managing school licensing through secondary level, whilst a national body licenses higher education institutions.

These models align with established national administrative structures. Federal states typically employ regional systems, whereas unitary states maintain centralised licensing.

## 2.4 Administrative vs legislative approaches

Educational licensing combines administrative and legislative processes:

- Finland, Portugal and Romania use specific legislation to establish universities
- National frameworks grant autonomy to local authorities for primary education oversight

These legal variations require flexible approaches in European digital credential systems.

License duration and renewal requirements differ by member state:

- Several countries issue permanent licenses with ongoing compliance monitoring
- Other states mandate periodic reviews, such as Romania's five-year evaluation cycle for pre-university institutions

These variations in licence validity periods affect credential verification procedures, requiring adaptable monitoring systems.

## 2.5 Lifecycle of licenses

The duration and renewal processes for educational licenses also vary considerably:

- Many countries grant licenses with indefinite validity, subject to continued compliance with requirements.
- Some countries, like Romania, implement periodic evaluations. For instance, Romanian pre-university education institutions undergo evaluation every 5 years.

This diversity in license lifecycles presents challenges for creating a unified system of credential verification across Europe, as the status and validity of an institution's license may need to be checked at different intervals depending on the country.

## 2.6 Information management on licensed institutions

Licensed institution data management follows three patterns:

- Central management (70% of respondents): National ministries maintain records for all education levels.

Co-funded by the European Union

- Split management (24% of respondents): Central authorities oversee higher education data, with regional bodies managing pre-higher education records.
- Regional management (6% of respondents): Local authorities control all institutional data.

These different data management structures require specific interfaces for European-wide credential systems.

This distribution of information management approaches has significant implications for the development of a European-wide digital credential system. A system would need to interface with various national and regional databases, each potentially structured differently and operating under different regulatory frameworks.

## 2.7 Electronic Diploma issuance

Electronic diploma adoption shows four implementation patterns:

- Full implementation (33% of respondents): Denmark, Greece, Lithuania, Netherlands, Norway and Portugal use electronic certificates as primary credentials for selected education levels.
- Permissive framework (17% of respondents): Finland and Sweden allow institutions to select certificate formats through non-restrictive legislation.
- Active transition (28% of respondents): Estonia, Latvia, Poland, Romania and selected German states are developing electronic certificate systems through legal reforms and national digital storage services.
- Paper requirement (22% of respondents): Cyprus, Hungary, Italy and Spain maintain legal requirements for paper certificates.

This mixed electronic and paper-based environment requires systems supporting both formats.

## 2.8 Educational data and registers

Electronic register implementation rates by sector:

- Universities and Universities of Applied Sciences: 80% use national machine-readable registers
- General Upper Secondary Education: 76% maintain national registers
- Primary Education and Technical/Vocational Education: Mixed national and local register usage
- Liberal Adult Education: 33% lack electronic registers.

## 2.9 Data models and ontologies

Data model and ontology adoption rates indicate current interoperability levels:

Data model implementation:

- University education: 59%
- Upper secondary education: 53%
- International standard alignment (ELMO): 18%

Ontology implementation:

- National education ontologies: 40%
- International standard alignment: Limited adoption

These rates show gaps in cross-border data exchange capacity between member states.

## 2.10 Quality assurance and security standards

Quality assurance requirements in educational data management:

- National legislation: 35%
- National authority guidelines: 24%

Security measures in educational registries:

- National legislation compliance: 18%
- ISO/IEC 27001 implementation: 12%

## 2.11 Limitations of current solutions

While various initiatives have been launched to address the challenges in the European education landscape, many of these solutions have their own limitations:

- Institution-focused design: Many current solutions prioritise the needs of educational institutions and employers over those of students and graduates.
- Inadequate revocation mechanisms: Popular platforms like Europass EDCI lack effective methods for revoking or updating qualifications.
- Federation constraints: National federations and systems like eduGAIN provide authentication services but not comprehensive qualification verification and portability.
- Interoperability issues: Many existing solutions struggle to work seamlessly across different member states or sectors.
- Limited scalability: Current approaches often face difficulties in scaling to serve millions of users across Europe.

## 2.12 New paradigm due to digitalisation

Co-funded by the European Union

The European education and qualifications landscape is characterised by diversity, autonomy, and historical separation from an organisational perspective (different processes, different credentials, different schemes). While this diversity allows for tailored approaches to education in different countries, it also presents significant challenges for cross-border recognition of qualifications and student mobility.

The European education system balances member state autonomy with cross-border coordination needs. Digital solutions must accommodate national education frameworks while supporting qualification recognition and student mobility.

Digital wallets could provide students and professionals with a secure, portable means of storing and sharing their educational credentials.

Digital solutions for current limitations:

- Technical capabilities:
  - Secure credential storage through EUDI wallets
  - Verifiable records using distributed ledger technologies
  - Standardised data exchange formats
- Implementation requirements:
  - Common data standards
  - Privacy protection measures
  - Cross-border interoperability protocols

However, the successful implementation of these technologies would require addressing several challenges, including ensuring widespread adoption, maintaining data privacy, and creating standardised formats for educational data that can be used across different systems and countries.

As Europe moves forward, the challenge will be to harness digital opportunities while respecting the autonomy of member states and the rich diversity of educational traditions across the continent.

These opportunities are realised through:

- The operational model detailed in Chapter 4
- The technical framework specified in Chapter 8
- The implementation roadmap outlined in Chapter 8 Practical examples of these solutions are demonstrated in the use cases presented in Chapter 7.

Co-funded by the European Union

# Chapter 3: Current challenges and needs in educational and professional credential management

The management of educational credentials in Europe is at a critical juncture, facing a myriad of challenges stemming from the diverse and decentralised nature of the continent's education systems. This chapter examines the current state of credential management, identifying key challenges and needs within the European educational ecosystem.

The trust framework's solution to these challenges is detailed in Section 4.1, with technical specifications provided in Section 7.2.

## 3.1 Credential issuance and verification

### *3.1.1 Diversity in credential formats*

Educational institutions across Europe issue credentials in a wide range of formats, from traditional paper-based documents to advanced digital certificates. This diversity reflects deep-rooted institutional practices and national regulations.

Paper-based credentials remain common in many European countries, often incorporating security features such as watermarks or holograms. However, these present challenges in terms of verification, especially across borders, and are vulnerable to loss or damage.

Digital credentials are gaining traction, with formats ranging from simple PDF documents to more sophisticated verifiable credentials-based certificates. Some institutions issue hybrid credentials, providing both paper and digital versions. The adoption of digital credentials varies significantly between countries and institutions.

This diversity in credential formats creates challenges for employers and educational institutions attempting to verify qualifications from different countries. Each format may require different verification methods, leading to inefficiencies and potential security risks.

### *3.1.2 Verification processes*

The verification of educational credentials remains a complex and often manual process in many parts of Europe. Methods used for verification vary widely, reflecting the diverse credential formats and institutional practices.

Many institutions still rely on direct communication with the issuing body for verification. This method, while potentially thorough, is time-consuming and resource-intensive. It can lead to significant delays in processes such as university admissions or job applications, particularly when credentials need to be verified across borders.

Co-funded by the European Union

Some countries have implemented digital verification platforms at a national level. For example, the Netherlands has developed a system called DUO, which allows for the digital verification of Dutch educational credentials. While such systems can streamline the verification process within a country, they often lack interoperability with systems from other countries, limiting their usefulness in a pan-European context.

There's a need for a trust infrastructure must provide:

- Distributed verification capabilities
- Redundant record keeping
- Independent verification pathways
- Protection against single points of failure

Such infrastructure is a potential solution for credential verification, offering the potential for near-instantaneous verification and could significantly reduce the administrative burden of credential checking.

The lack of a standardised, digitalised cross-border verification system creates inefficiencies and potential security risks. It also poses barriers to student mobility and professional recognition across Europe, as the time and effort required to verify credentials can discourage institutions and employers from considering applicants with qualifications from unfamiliar systems.

#### *3.1.3 Building on Bologna Process achievements*

The current digital credential challenges mirror those addressed by the Bologna Process for degree structures and quality assurance. The Bologna Process demonstrated that:

- Common standards can coexist with national autonomy
- Voluntary frameworks can achieve widespread adoption
- Practical tools (like ECTS) can solve complex cross-border challenges
- Quality assurance can be standardized while respecting institutional diversity

These lessons inform our approach to digital credential standardization. Just as ECTS created a common "currency" for academic credit, digital credentials need standardized formats and trust frameworks that work across borders while respecting institutional and national requirements.

## 3.2 Recognition of qualifications

#### *3.2.1 Academic recognition*

The recognition of academic qualifications for further study presents several challenges, largely stemming from the autonomy granted to educational institutions in many European countries.

Institutional autonomy in recognition practices leads to inconsistencies in how qualifications are valued and recognised. An academic qualification that is readily

accepted for further study in one institution may be viewed differently by another, even within the same country. This variability can create uncertainty for students and potentially lead to unfair outcomes.

The methods used for evaluating and recognising prior qualifications vary widely. Some institutions conduct case-by-case manual evaluations, which can be thorough but time-consuming and potentially subjective. Others use more standardised procedures based on systems like the European Credit Transfer and Accumulation System (ECTS). While ECTS has helped to standardise credit recognition within the European Higher Education Area, its application is not uniform across all institutions and programmes.

The lack of automation in recognition processes is a significant issue. Few institutions reported automated recognition processes, with most relying on human evaluation. This reliance on manual processes can lead to delays and inconsistencies, particularly when dealing with a high volume of applications or unfamiliar qualifications.

### *3.2.2 Professional recognition*

The recognition of professional qualifications faces its own set of challenges, often more complex due to the regulatory nature of many professions.

Each EU member state has its own regulations for professional recognition, particularly for regulated professions. This regulatory complexity can make it difficult for professionals to have their qualifications recognised when moving between countries, even within the EU.

The responsibility for recognition is often distributed among numerous authorities based on professional fields. For example, medical qualifications might be recognised by a health authority or by the national body representing the corresponding professional corporations, while engineering qualifications fall under a different body. This fragmentation can make the recognition process confusing and time-consuming for applicants, who may need to navigate multiple systems and requirements.

While some countries have implemented digital services for professional recognition applications, many processes remain paper-based and time-consuming. The European Professional Card, an electronic procedure for recognising professional qualifications between EU countries, is a step towards digitalisation but is currently limited to a few professions.

These challenges significantly hinder professional mobility within Europe. Professionals may face lengthy and complex processes to have their qualifications recognised in different countries, potentially discouraging them from seeking opportunities abroad or leading to underemployment when they do move.

The operational model addresses these challenges through mechanisms detailed in Section 4.2, with practical examples demonstrated in Section 6.3.1.

Co-funded by the European Union

## 3.3 Data management and interoperability

### *3.3.1 Data models and standards*

The lack of widely adopted standards for data models in the education sector is a significant barrier to interoperability. Our research found that only 18% of surveyed countries reported aligning their educational data models with international standards like ELMO - ELMO is a data format for the exchange of (education) result information. ELMO is an implementation of the European (CEN) standards ELM-AI (European Learner Mobility – Achievement Information, EN 15981) and MLO (Metadata for Learning Objects, EN 15982).

The adoption of common data models varies across education levels. Higher education tends to have higher adoption rates (59% of surveyed countries), likely due to initiatives like the Bologna Process which have encouraged standardisation in this sector. However, adoption rates are lower for other levels of education, creating challenges for lifelong learning recognition.

This lack of standardisation hampers data interoperability and complicates the process of comparing and recognising qualifications across borders. When educational data is stored and structured differently in various systems, it becomes difficult to create automated processes for qualification recognition or to provide comprehensive views of an individual's educational achievements.

### *3.3.2 Data sharing and privacy*

While all surveyed countries adhere to the General Data Protection Regulation (GDPR), the implementation of education or professional-specific data protection measures varies. This variability can create uncertainty about what data can be shared and how, potentially hindering efforts to create comprehensive systems for credential recognition.

There are limited mechanisms for secure, efficient cross-border exchange of educational data. While initiatives like EMREX aim to facilitate such exchange in higher education, their adoption is not universal. The lack of established channels for data exchange can lead to reliance on less secure methods or create barriers to recognition processes.

Balancing data sharing for recognition purposes with stringent privacy requirements presents an ongoing challenge. Educational institutions and regulatory bodies must navigate the need to verify and recognise qualifications while respecting individuals' rights to data privacy and control over their personal information.

## 3.4 Technological infrastructure

The development of technological infrastructure to support digital credential management varies significantly across Europe, creating disparities in the ability to issue, manage, and verify digital credentials.

Some countries have implemented national platforms for issuing and verifying digital credentials. For example, Estonia's e-government infrastructure includes provisions for digital educational certificates. However, these advanced systems are not universally adopted across Europe.

Trusted ledger initiatives for credential management are being explored by some institutions, offering potential for secure, decentralised credential verification. However, widespread adoption remains limited, often confined to pilot projects or specific institutions.

Many institutions still rely on legacy systems that are not easily integrated with newer digital solutions. This reliance on older technology can create barriers to adopting more advanced credential management systems and can hinder interoperability efforts.

The disparity in technological readiness across European educational institutions poses challenges for implementing unified digital credential solutions. Institutions with more advanced systems may be reluctant to adopt new standards that require significant changes, while those with less developed infrastructure may struggle to implement more advanced solutions.

## 3.5 Legal and regulatory framework

The legal and regulatory landscape for educational credentials in Europe is complex and varied, reflecting the diversity of national education systems and the evolving nature of digital credentials.

Many countries have specific legislation governing the issuance and recognition of educational credentials. These laws may not always align with digital transformation goals, potentially creating legal barriers to the adoption of digital credentials or new verification methods.

EU-level initiatives like the European Qualifications Framework aim to improve the comparability of qualifications across countries. However, implementation and recognition at the national level remain inconsistent, highlighting the challenges of creating truly pan-European solutions in education.

The evolving landscape of digital identity regulations, including the amended eIDAS Regulation framework, presents both opportunities and challenges for digital credential management. While these regulations aim to create a common framework for electronic

Co-funded by the European Union

identification across Europe, their application to educational and professional credentials is still developing.

According to Recital (55) of the eIDAS 2 Regulation, “an electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes”, a principle that ensures the validity of any electronic attestation of attributes, especially when a sector-specific EU or national legislation already allows issuing documents to specific bodies. One relevant example for the educational and professional domain is the Professional Qualifications Directive, where the issuers of the credentials would be the competent authority, typically an authentic source of the information contained within.

Thus, Article 1(c) of the amended eIDAS Regulation “establishes a legal framework for”, among others, “electronic attestation of attributes”, which is defined by Article 3(44) as “an attestation in electronic form that allows attributes to be authenticated”. The amended eIDAS Regulation considers two specific subtypes of electronic attestations of attributes (named as “qualified electronic attestation of attributes” and “electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source”), which receive direct legal recognition, but enshrining the validity and judicial admissibility of all electronic attestations of attributes. According to Article 45b(1) of the amended eIDAS Regulation, “an electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes”.

This legal approach, which is common to the different legal evidentiary institutions enabled by trust services, ensures that innovative approaches can be used in real world use cases requiring legal validity.

Navigating this complex regulatory environment while pushing for innovation in credential management requires careful consideration, to be explored during the Large-Scale Pilots. Depending of the results, it may necessitate legislative updates at both national and EU levels (especially to the eIDAS Implementing Acts) to fully enable the potential of digital credentials while ensuring appropriate safeguards and recognition. This is potentially one of the most relevant contributions to the evolution of the eIDAS ecosystem, where some gaps have already been identified.

## 3.6 Stakeholder needs and concerns

Different stakeholders in the educational ecosystem have varying needs and concerns regarding credential management. Understanding and addressing these diverse perspectives is crucial for developing effective solutions.

Educational institutions seek ways to reduce the administrative burden associated with issuing and verifying credentials. They also express concerns about balancing

standardisation with institutional autonomy in credential issuance and recognition. Many institutions face challenges in adapting to new technologies for credential management, including costs and training needs.

Students and graduates demand easily portable and universally recognised credentials to support mobility for study and work. They express concerns about data privacy and desire greater control over their educational records. There's an increasing need for recognition of non-traditional learning experiences and micro-credentials, reflecting changing patterns of learning and career development. Students are seeking more flexible ways to showcase their skills and knowledge, beyond traditional degree certificates.

Employers and professional bodies seek quick and reliable methods to verify candidates' qualifications. This need is particularly acute in sectors with high mobility or where specific qualifications are crucial for regulatory compliance. There's a growing emphasis on recognising specific skills and competencies beyond formal qualifications, as employers look for more granular information about candidates' capabilities. Multinational employers face particular challenges in comparing and recognising qualifications from different educational systems, which can complicate international recruitment processes.

Regulatory bodies are tasked with ensuring the quality and integrity of educational and professional credentials while adapting to technological changes. They must balance the need for innovation with maintaining rigorous standards. There's an increasing need for cross-border cooperation between national regulatory bodies to facilitate smoother recognition processes. Developing robust systems to prevent credential fraud remains a key concern, particularly as digital credentials become more prevalent.

## 3.7 Opportunities for digital solutions

The trust framework offers five key opportunity areas for transforming credential management:

1. Digital transformation
    - Standardized digital credential formats across Europe
    - Secure, verifiable digital documents replacing paper
    - Integration with existing information systems
    - Support for emerging credential types
    - Digital workflow automation
2. Cross-border mobility
    - Automated qualification recognition
    - Standardized credential verification
    - Multilingual credential support
    - Simplified professional licensing
    - Enhanced student mobility
3. System efficiency

- Reduced manual verification needs
- Streamlined administrative processes
- Lower operational costs
- Faster credential processing
- Improved data accuracy

4. Data protection and privacy
   - Enhanced personal data control
   - Secure credential storage
   - Privacy-preserving verification
   - Compliance with GDPR
   - Selective information sharing
5. Innovation support
   - New educational service models
   - Enhanced labour market matching
   - Support for lifelong learning
   - Improved policy analytics
   - Cross-institutional collaboration

These opportunities are realised through:

- Operational processes detailed in Chapter 4
- Technical implementations specified in 8
- Practical use cases demonstrated in Chapter 7 Implementation guidance is provided in Chapter 8

The current state of educational credential management in Europe presents a complex landscape of challenges and opportunities. Key issues include the diversity of issuance and verification practices, inconsistencies in recognition processes, limited data standardisation and interoperability, varied technological readiness, and a complex regulatory environment.

Addressing these challenges requires a multifaceted approach that considers the needs of all stakeholders while leveraging technological innovations. The development of solutions like the European Digital Identity Wallet and associated frameworks offers promising avenues for addressing many of these challenges. By providing a standardised, secure platform for storing and sharing digital credentials, such systems could significantly improve the portability and recognition of qualifications across Europe.

However, successful implementation will require careful consideration of the diverse national contexts, regulatory requirements, and stakeholder needs identified in this analysis. It will also necessitate ongoing dialogue and cooperation between educational institutions, employers, regulatory bodies, and technology providers to ensure that solutions meet the needs of all parties and can be effectively integrated into existing systems.

Co-funded by the European Union

Co-funded by the European Union

# Chapter 4: Operational Model

The operational model for managing educational and professional credentials across Europe combines robust governance with efficient processes to ensure trust, security, and interoperability. This chapter first establishes the fundamental trust model and governance framework that underpins all credential operations, then details the specific processes and responsibilities for credential management.

The framework adopts a non-delegated trust model where educational institutions and professional bodies maintain direct responsibility for their credentials. This approach ensures clear accountability while respecting institutional autonomy, supporting both the integrity of credentials and the privacy of individuals. The governance structure provides clear oversight at European and national levels while enabling efficient operations at the institutional level.

Building upon this foundation, the chapter explores the complete lifecycle of credentials, from issuance through verification, and details how different stakeholders interact within the framework. The operational model addresses several critical needs in the European education and professional qualification landscape:

- Trust establishment: Creating and maintaining trusted relationships between credential issuers, holders, and verifiers across borders.
- Privacy protection: Ensuring individual control over personal data while enabling efficient credential verification.
- Institutional autonomy: Supporting the independence of educational institutions while maintaining interoperability.
- Cross-border recognition: Facilitating qualification recognition and professional mobility throughout Europe.
- Regulatory compliance: Ensuring alignment with European regulations while supporting national requirements.

This chapter provides stakeholders with a clear understanding of their roles, responsibilities, and interactions within the trust framework. Through detailed explanations of governance structures, operational processes, and implementation guidelines, it offers a comprehensive blueprint for implementing trusted credential management across the European education and professional qualification sectors.

The following sections detail:

- The trust model and governance framework that underpins all operations
- The complete credential lifecycle management process
- Roles and responsibilities of various stakeholders
- Compliance requirements and quality assurance measures
- Benefits and outcomes of the operational model

Co-funded by the European Union

This operational model provides the foundation for transforming credential management in Europe, supporting increased mobility, lifelong learning, and a more dynamic and efficient labour market.

## 4.1 Trust model and Governance framework

The trust framework for European educational and professional credentials builds upon proven approaches to cross-border cooperation in education. Drawing key lessons from the Bologna Process's successful implementation of voluntary standards, it establishes governance mechanisms that respect institutional autonomy while ensuring consistent quality across borders. Like the Bologna Follow-up Group (BFUG), it creates clear coordination structures while preserving institutional independence in implementation.

The framework adopts a non-delegated trust model, mirroring the Bologna Process's approach where common standards are implemented independently by institutions according to their local context. This model ensures both standardization where needed and flexibility where required, supporting the diverse needs of European education while maintaining interoperability.

The technical implementation of this trust model is detailed in Section 7.2, with practical examples demonstrated in Chapter 7.

### *4.1.1 Trust Framework foundation*

The European education and professional qualification sectors require a trust framework that balances institutional autonomy with reliable cross-border credential verification. At its core, this framework implements a non-delegated trust model, where educational institutions and professional bodies maintain direct responsibility and authority over their credentials.

In this non-delegated approach, trust flows directly between credential issuers and verifiers, without requiring intermediary authorities to establish credential validity. This direct trust relationship ensures that the authentic sources of information -educational institutions and professional bodies- maintain complete control over their credential issuance and status management processes.

The trust framework implements a non-delegated trust model where educational institutions and professional bodies maintain direct responsibility for their credentials. This approach ensures:

- Direct accountability
    - Each institution remains directly responsible for its credentials
    - Clear lines of authority and responsibility
    - Immediate control over credential status

Co-funded by the European Union

These accountability mechanisms are implemented through specific processes detailed in Section 4.4: Compliance and monitoring framework.

- Institutional autonomy
  - Organizations implement framework according to their needs
  - Maintenance of institutional identity
  - Support for local requirements

  The practical implementation of institutional autonomy within the framework is demonstrated through specific use cases in Section 6.7.

- Privacy Protection
  - Individual control over credential sharing
  - Selective disclosure capabilities
  - Privacy-preserving verification

  Technical implementation of these privacy measures is detailed in Section 7.2: Core Data Model Architecture.

This direct trust relationship ensures that the authentic sources of information maintain complete control over their credential issuance and status management processes. The practical implementation of these processes is detailed in Chapter 5: Natural persons and legal entities onboarding process.

### *4.1.2 Governance structure*

#### European level oversight

At the European level, designated authorities establish and maintain the framework's core requirements. These authorities:

- Define framework standards and protocols that ensure consistency across implementations. These standards support interoperability while allowing flexibility in how institutions meet requirements.
- Monitor framework compliance through regular assessments and audits. This oversight ensures the framework maintains high standards of trust and security across all participating institutions.
- Facilitate cross-border recognition by maintaining alignment with relevant European initiatives and regulations. This coordination ensures the framework supports broader European objectives for educational and professional mobility.
- Provide guidance on framework implementation, helping institutions understand and meet requirements while maintaining their autonomy.

This oversight aligns with European strategies and regulations as outlined in Section 1.4 and Annex C: Regulatory references.

#### National level coordination

National authorities serve as coordinators within their jurisdictions, providing a crucial link between European oversight and institutional implementation. These bodies:

Co-funded by the European Union

- Maintain authoritative registries of qualified credential issuers within their territory. These registries provide verifiers with reliable information about authorized institutions.
- Ensure alignment between framework implementation and national regulations. This coordination prevents conflicts between European and national requirements.
- Support national institutions in framework adoption, providing guidance and resources that facilitate effective implementation.
- Monitor compliance at the national level, ensuring institutions meet both framework requirements and national standards.

The diverse approaches to national coordination are explored in Section 2.1: Decentralised authority and Member State autonomy.

#### Institutional level implementation

Individual institutions—universities, professional bodies, and other authorized organizations—maintain operational control over their credential processes while adhering to framework standards. At this level, institutions:

- Manage their credential issuance processes according to framework requirements. This includes maintaining secure systems for credential creation and management.
- Control credential status information, including updates and revocations. This direct control ensures immediate response to any required status changes.
- Implement required security and privacy measures that protect both institutional and individual interests.
- Maintain compliance with framework standards while preserving their institutional identity and autonomy.

Practical examples of institutional implementation are provided in the use cases in Chapter 7, particularly Sections 7.7.1 and 7.7.2.

### *4.1.3 Trust Framework components*

#### Core requirements

The trust framework is built on four fundamental requirements that drive all operational elements and governance processes. These core requirements establish the foundation for secure, interoperable, and privacy-preserving credential management across Europe.

- Standardization
  The framework ensures consistent credential handling across all participating institutions through:
  - Credential Format Standardization
    - Implementation of W3C Verifiable Credentials Data Model
    - Alignment with European Learning Model specifications
    - Standardized attribute definitions and structures
    - Common metadata requirements

The choice of the W3C Verifiable Credentials (VC) Data Model as the foundational format for credential issuance was driven by its robust support for cross-border interoperability, privacy-preserving features, and its alignment with global digital identity standards. The W3C VC model enables selective disclosure, allowing users to share only the necessary portions of their credentials, thus enhancing user privacy while maintaining data integrity. This ensures that institutions across the EU can issue, verify, and trust digital credentials uniformly, meeting the diverse regulatory requirements of different member states. It is also important to remark that European Learning Model (ELM) is based on W3C-VCDM and several European solutions re-use ELM as a core (Europass, European Digital Credentials Infrastructure, European Blockchain Services Infrastructure, European Employment Service - EURES, European Skills Data Space).

The integration of the European Learning Model (ELM) alongside the W3C Verifiable Credentials framework addresses key challenges such as cross-border recognition and compatibility with varying credential verification processes across EU member states. The ELM ensures that credentials maintain a standardized, interoperable structure, promoting seamless data exchange between educational institutions and professional bodies. By employing these data models, the BBP not only adheres to established EU educational frameworks but also supports a scalable, adaptable approach for future credentialing needs.

Detailed implementation in Section 4.2: Credential lifecycle management

- Process Standardization
  - Unified credential issuance procedures
  - Common verification protocols
  - Standardized status management processes
  - Consistent privacy protection measures

  Detailed implementation in Section 4.3: Roles and responsibilities
- Interoperability Requirements
  - Cross-border credential recognition
  - Multi-system compatibility
  - Standard data exchange formats
  - Common API specifications

  Technical details in Section 7.2: Core data model architecture

- Security

  The framework maintains credential integrity and system trust through:
  - Credential security
    - Cryptographic protection of credentials
    - Tamper-evident mechanisms
    - Secure issuance protocols
    - Protected storage requirements

    Implementation details in Section 4.5: Infrastructure requirements
  - System security
    - Access control mechanisms

        - Authentication requirements
        - Audit logging
        - Incident response procedures

      Detailed in Section 4.4: Compliance and monitoring framework
    - Operational security
        - Secure communication channels
        - Data protection measures
        - Backup procedures
        - Recovery protocols

      Technical implementation in Section 7.5: Implementation guidelines

- Privacy

  The framework ensures privacy protection and individual control through:
    - Privacy by design
        - Data minimization principles
        - Purpose limitation
        - Storage restrictions
        - Processing safeguards

      Alignment with requirements in Annex C: Regulatory references
    - Individual control
        - Selective disclosure capabilities
        - Consent management
        - User authorization requirements
        - Data subject rights protection

      Implementation in Section 4.2: Credential lifecycle management
    - Privacy-preserving operations
        - - Anonymous credential presentation
        - - Unlikable transactions
        - - Usage tracking prevention
        - - Secure deletion procedures

      Technical details in Section 7.3: Model structure

- Quality assurance

  The framework maintains high operational standards through:
    - Process quality
        - Defined quality standards
        - Process monitoring
        - Performance metrics
        - Continuous improvement procedures

      Detailed in Section 4.4: Compliance and monitoring framework
    - Credential quality
        - Issuer verification
        - Credential validation
        - Status accuracy
        - Content integrity

      Implementation in Section 4.2: Credential lifecycle management

- Service quality
  - Performance standards
  - Availability requirements
  - Response time metrics
  - Support procedures

  Operational details in Section 4.5: Infrastructure requirements

These core requirements form the foundation for all operational processes and technical implementations detailed in subsequent sections. Each requirement is realized through specific operational elements, compliance measures, and technical specifications. The requirements are designed to be technology-neutral while ensuring consistent implementation across the framework.

All core requirements support cross-border credential recognition and verification while accommodating national requirements and local regulations. This enables seamless operation across European member states while respecting institutional autonomy and national sovereignty.

The core requirements are designed to accommodate emerging technologies and evolving needs while maintaining backward compatibility and operational stability. Regular review processes ensure requirements remain current and effective.

These requirements are elaborated in detail in Section 4.5: Infrastructure requirements.

### Operational Elements

The trust framework's operational elements define how credentials are managed throughout their lifecycle while maintaining security and institutional autonomy.

1. Credential management
   - Issuance
     - Verification of qualification completion before issuance
     - Creation of credentials according to framework standards (providing composed complex credentials if needed: e.g. Master credential including a programme' quality assurance credential)
     - Application of institutional authorization
     - Secure delivery to recipient's EUDI wallet
   - Storage
     - Secure maintenance in authorized EUDI wallets
     - Institutional record-keeping of issued credentials
     - Privacy controls protecting credential information
     - Regular status information updates
   - Presentation
     - Selective sharing of credential information
     - Privacy-preserving presentation methods
     - Prevention of unauthorized tracking
     - Cross-border sharing support

- Verification
  - Direct confirmation of issuer authority
  - Real-time status verification
  - Privacy-preserving verification methods
  - Cross-border verification support

The technical implementation of these credential management processes is detailed in Section 7.3: Model structure.

2. Status management
   - Active status maintenance
     - Regular confirmation procedures
     - Automated monitoring systems
     - Timely status updates
     - Clear validity indicators
   - Suspension mechanisms
     - Defined suspension criteria
     - Immediate status update capabilities
     - Clear reinstatement procedures
     - Transparent communication processes
   - Revocation processes
     - Strict revocation protocols
     - Immediate status updates
     - Clear documentation requirements
     - Permanent record maintenance

   Specific status management scenarios are demonstrated in use cases 6.7.3.1 through 6.7.3.5.

3. Quality controls
   - Process monitoring
     - Regular assessment of operations
     - Performance metrics tracking
     - Stakeholder feedback collection
     - Continuous improvement procedures
   - Security measures
     - Access control systems
     - Encryption requirements
     - Audit logging
     - Incident response procedures

   These controls are aligned with the quality assurance standards described in Section 2.10.

4. Cross-border operations
   - Recognition support
     - Standardized format implementation
     - Clear status communication

        - Efficient verification processes
        - Multi-jurisdiction support
    - Jurisdictional alignment
        - National system compatibility
        - Regulatory compliance
        - Language support
        - Local requirement accommodation

    Implementation challenges and solutions for cross-border operations are discussed in Section 3.2: Recognition of Qualifications.

5. Privacy framework
    - Data protection
        - Minimization principles
        - Selective disclosure mechanisms
        - Access control systems
        - Audit capabilities
    - User control
        - Individual authorization requirements
        - Usage tracking prevention
        - Secure storage mechanisms
        - Clear sharing permissions

    Technical implementation of privacy measures is detailed in Section 7.5: Implementation guidelines.

6. Integration components
    - System connections
        - Educational management systems
        - Professional body platforms
        - Verification services
        - Digital wallet interfaces
    - Data exchange
        - Standardized protocols
        - Secure transmission methods
        - Privacy-preserving mechanisms
        - Cross-system compatibility

    Specific integration requirements are elaborated in Section 4.5.4: Integration requirements.

The operational elements described here are implemented through specific processes detailed in Chapter 5 and demonstrated through use cases in Chapter 7.

### Compliance framework

This framework implements regulatory requirements outlined in section 1.4 and detailed in Annex C. The compliance framework ensures trust framework integrity through

comprehensive oversight while respecting institutional autonomy and privacy requirements.

1. Regulatory compliance
    - European Level Requirements
        - eIDAS Regulation alignment
            - Trust service requirements
            - Electronic identification standards
            - Legal recognition provisions
            - Cross-border validity
        - GDPR Implementation
            - Privacy by design principles
            - Data processing requirements
            - Individual rights protection
            - Cross-border data transfer rules
        - Single Digital Gateway Support
            - Once-only principles' implementation
            - Cross-border service access
            - Administrative simplification
            - Interoperability requirements
    - National level requirements
        - Education regulations alignment
            - National qualification standards
            - Professional licensing requirements
            - Local accreditation rules
            - Institutional autonomy respect
        - Data protection compliance
            - National privacy laws
            - Sector-specific regulations
            - Local security standards
            - Jurisdictional requirements

2. Quality assurance
    - Operational standards
        - Process requirements
            - Credential issuance procedures
            - Verification protocols
            - Status management rules
            - Documentation standards
        - Security measures
            - Access control requirements
            - Data protection standards
            - System security protocols
            - Incident response procedures
        - Privacy standards
            - Data minimization principles

        - Consent management requirements
        - Information sharing rules
        - Rights protection measures
- Implementation requirements
    - Technical standards
        - Infrastructure requirements
        - Integration specifications
        - Security protocols
        - Performance standards
    - Process standards
        - Operational procedures
        - Workflow requirements
        - Documentation rules
        - Quality metrics

3. Monitoring framework
    - Continuous Monitoring
        - System performance tracking
            - Operational metrics
            - Security indicators
            - Privacy compliance
            - Service levels
        - Compliance verification
            - Regular checks
            - Automated monitoring
            - Issue detection
            - Response tracking
    - Audit programs
        - Internal audits
            - Regular self-assessments
            - Process reviews
            - Compliance checks
            - Performance evaluation
        - External audits
            - Independent verification
            - Compliance validation
            - Security assessment
            - Privacy review

4. Risk management
    - Assessment framework
        - Risk identification
            - Threat analysis
            - Vulnerability assessment
            - Impact evaluation

        - Probability assessment
    - Mitigation planning
        - Control measures
        - Response procedures
        - Recovery plans
        - Prevention strategies
- Security controls
    - Access management
        - Authentication requirements
        - Authorization controls
        - Access logging
        - Audit trails
    - Data protection
        - Encryption standards
        - Storage requirements
        - Transmission security
        - Backup procedures

5. Improvement framework
    - Performance Analysis
        - Metric tracking
            - Key performance indicators
            - Success measures
            - Issue tracking
            - Trend analysis
        - Feedback management
            - Stakeholder input
            - User experience data
            - Issue reports
            - Improvement suggestions
    - Enhancement process
        - Planning
            - Priority setting
            - Resource allocation
            - Timeline development
            - Impact assessment
        - Implementation
            - Change management
            - Testing procedures
            - Deployment controls
            - Validation measures

6. Reporting framework
    - Regular Reporting
        - Performance reports

        - Operational metrics
        - Compliance status
        - Security incidents
        - Privacy compliance
    - Status updates
        - System health
        - Issue tracking
        - Resolution progress
        - Improvement initiatives
- Communication
    - Stakeholder updates
        - Regular briefings
        - Issue notifications
        - Change communications
        - Progress reports
    - Transparency measures
        - Public reporting
        - Stakeholder access
        - Information sharing
        - Feedback channels

The practical implementation of these compliance requirements is demonstrated through the use cases in Chapter 7, particularly in sections 6.7.3.4 and 6.7.3.5 for professional qualifications.

Through this comprehensive trust model and governance framework, the system ensures reliable credential management while supporting institutional autonomy and individual privacy. The non-delegated trust model, combined with clear governance structures and robust accountability mechanisms, provides a solid foundation for secure and efficient credential operations across Europe.

## 4.2 Credential lifecycle management

### *4.2.1 Overview*

The credential lifecycle encompasses all stages from initial issuance through eventual expiration or revocation. Operating within the non-delegated trust model established in Section 4.1, this lifecycle ensures secure, efficient credential management while maintaining privacy and institutional control.

Each stage of the lifecycle requires careful management to maintain credential integrity, protect privacy, and support efficient verification. Educational institutions and professional bodies maintain direct control throughout the lifecycle, ensuring immediate response to any required changes while supporting cross-border recognition and mobility.

The technical framework supporting these processes is detailed in Section 7.3, whilst implementation guidance is provided in Chapter 8.

### *4.2.2 Core lifecycle stages*

#### Issuance

The credential lifecycle begins with issuance by an authorized institution. During this stage, the institution:

- Verifies qualification completion or achievement of required standards. This verification ensures credentials accurately reflect earned qualifications.
- Creates the credential according to framework standards. This includes all required information while maintaining data minimization principles.
- Applies institutional authorization, establishing the credential's authenticity. This step creates a direct trust relationship between the issuing institution and the credential.
- Delivers the credential to the recipient securely. This transfer gives the recipient control over their credential while maintaining its integrity.

#### Storage and management

Once issued, credentials require secure storage and ongoing management:

- Recipients maintain their credentials in authorized EUDI wallets. These wallets give individuals control over their credentials while ensuring security.
- Institutions maintain authoritative records of issued credentials. These records support status management and verification processes.
- Privacy controls protect credential information throughout its lifecycle. These controls prevent unauthorized access while enabling legitimate use.
- Regular status updates ensure credential information remains current. These updates maintain the credential's reliability for verification purposes.

#### Presentation and sharing

Credential holders' control when and how to share their credentials:

- Selective sharing allows holders to reveal only necessary information. This capability protects privacy while meeting verification needs. Issuer's disclosure policies shall be taken into account, to avoid non-desired or non-properly contextualized usage of legal binding issued Electronic Attestations of Attributes.
- Secure presentation methods prevent credential tampering. These methods ensure credentials remain reliable for verification.
- Privacy-preserving protocols prevent tracking of credential usage. This protection ensures individual privacy while maintaining credential utility.
- Cross-border sharing supports educational and professional mobility. This capability enables credential recognition across European borders.

#### Verification

Authorized parties can verify credentials efficiently while respecting privacy:

- Direct verification confirms credential authenticity. This process checks the issuing institution's authorization through official registries.
- Status checking ensures current validity. This verification confirms the credential has not been revoked or suspended.
- Privacy-preserving methods protect individual interests. These methods prevent creation of usage traces while enabling legitimate verification.
- Cross-border verification supports mobility. This capability enables credential recognition throughout Europe.

### *4.2.3 Status Management*

Throughout the credential lifecycle, status management ensures current validity information remains available:

#### Active status

Credentials in active status indicate current validity:

- Regular confirmation maintains active status. This process ensures credentials remain reliable for verification.
- Automated monitoring identifies any issues requiring attention. This surveillance supports early problem detection.
- Status updates reflect any relevant changes. These updates maintain credential reliability.

#### Suspension

Temporary suspension may occur under specific circumstances:

- Clear procedures guide suspension decisions. These procedures ensure fair and consistent handling of suspension cases.
- Immediate status updates reflect suspension. These updates prevent reliance on suspended credentials.
- Defined processes govern reinstatement. These processes ensure appropriate handling of suspension resolution.

#### Revocation

Permanent revocation occurs in cases of serious issues:

- Strict protocols govern revocation decisions. These protocols ensure appropriate use of revocation.
- Immediate status updates reflect revocation. These updates prevent continued use of revoked credentials.
- Clear documentation supports revocation decisions. This documentation maintains accountability for revocation actions.

### *4.2.4 Privacy protection*

Privacy protection remains paramount throughout the credential lifecycle:

#### Data minimization

The framework implements data minimization principles:

- Only essential information appears in credentials. This limitation protects individual privacy.
- Selective disclosure enables controlled information sharing. This capability gives individuals control over their data.
- Privacy-preserving verification prevents unnecessary data exposure. These methods protect privacy during verification.

#### Usage control

Credential holders maintain control over their information:

- Individual authorization required for sharing. This requirement ensures controlled credential use.
- No tracking of credential usage patterns. This protection prevents creation of behaviour profiles.
- Secure storage prevents unauthorized access. This security protects credential confidentiality.

### *4.2.5 Cross-border considerations*

The credential lifecycle supports European mobility through:

#### Recognition support

The framework facilitates credential recognition across borders:

- Standardized formats support consistent interpretation. These standards enable understanding across jurisdictions.
- Clear status information supports recognition decisions. This clarity facilitates cross-border acceptance.
- Efficient verification enables quick recognition. This capability supports mobility and opportunity.

#### Jurisdictional alignment

The framework maintains alignment with varying requirements:

- Respect for national education systems. This consideration supports institutional autonomy.
- Compliance with local regulations. This alignment ensures legal operation across borders.
- Support for multiple languages. This capability enables broad understanding.

### *4.2.6 Quality assurance*

Quality assurance throughout the lifecycle ensures:

#### Operational excellence

Continuous monitoring maintains high standards:

- Regular assessment of lifecycle processes. These reviews ensure continued effectiveness.
- Performance metrics track system operation. These measurements support improvement efforts.

- Stakeholder feedback informs enhancements. This input ensures the system meets user needs.

#### Compliance verification

Regular audits confirm framework adherence:

- Assessment of institutional practices. These reviews ensure standard compliance.
- Verification of privacy protection. These checks confirm privacy safeguards.
- Evaluation of security measures. These assessments maintain system integrity.

The credential lifecycle management system ensures reliable, efficient operation while protecting privacy and supporting mobility. Through careful attention to each stage, the system maintains credential integrity while enabling legitimate use and verification.

## 4.3 Roles and responsibilities

### *4.3.1 Overview*

Within the non-delegated trust framework, each participant holds specific responsibilities that support the integrity and efficiency of the credential ecosystem. These roles reflect both the direct trust relationships and the need for clear accountability in credential management. Understanding these roles and their interrelationships proves essential for effective framework operation.

### *4.3.2 Educational institutions*

Universities and other educational institutions serve as primary credential issuers, maintaining direct responsibility for their credentials throughout their lifecycle.

#### Core responsibilities

Educational institutions maintain comprehensive responsibility for credential management:

- They verify the completion of academic requirements and achievement of qualifications before issuing any credentials. This verification ensures credentials accurately reflect educational accomplishments.
- They maintain authoritative records of all issued credentials, including current status information. This record-keeping supports efficient verification while maintaining credential integrity.
- They implement and manage status changes, including suspension or revocation when necessary. This control ensures immediate response to any required credential status updates.
- They protect the privacy of credential information while supporting legitimate verification needs. This balance maintains individual rights while enabling necessary credential validation.

#### Quality assurance

Institutions must maintain high standards in their credentialing processes:

- They establish and follow clear procedures for credential issuance and management. These procedures ensure consistent, reliable credential handling.

- They conduct regular internal audits of credentialing processes. These reviews maintain operational excellence and identify improvement opportunities.
- They participate in external quality assurance programs that validate their credentialing practices. This participation ensures alignment with framework standards.

#### Operational management

Daily operations require careful attention to several areas:

- They maintain secure systems for credential management that protect both institutional and individual interests. These systems support efficient operations while ensuring security.
- They train staff in proper credential handling procedures, including privacy protection requirements. This training ensures consistent, appropriate credential management.
- They respond promptly to verification requests while maintaining privacy protections. This responsiveness supports credential utility while protecting individual rights.

### *4.3.3 Professional bodies*

Professional organizations issuing qualifications and certifications maintain similar responsibilities to educational institutions, with additional focus on professional standards.

#### Core responsibilities

Professional bodies maintain specific obligations:

- They verify professional qualifications and continuing education requirements before issuing credentials. This verification ensures credentials reflect current professional standing.
- They maintain current records of professional credentials and status information. These records support verification of professional qualifications.
- They manage credential status changes based on professional standing and conduct. This management ensures credentials accurately reflect current professional status.

#### Industry alignment

Professional bodies must maintain alignment with industry requirements:

- They ensure credentials reflect current professional standards and requirements. This alignment maintains credential value for professional practice.
- They coordinate with industry stakeholders to maintain relevant credentialing standards. This coordination ensures credentials serve professional needs.
- They adapt credentialing practices to evolving professional requirements. This adaptation maintains credential utility over time.

### *4.3.4 Regulatory authorities*

Regulatory bodies at national and European levels provide essential oversight and coordination.

#### European level

European authorities maintain framework oversight:

- They establish and maintain framework standards that ensure consistent implementation across jurisdictions. These standards support cross-border credential recognition.
- They monitor framework operation to ensure it serves European mobility objectives. This monitoring supports continuous improvement.
- They coordinate with national authorities to maintain framework alignment. This coordination ensures consistent framework operation.

#### National level

National authorities provide crucial coordination within their jurisdictions:

- They maintain registries of authorized credential issuers within their territory. These registries support reliable verification of issuer authority.
- They ensure alignment between framework implementation and national regulations. This alignment prevents regulatory conflicts.
- They support national institutions in framework adoption and operation. This support facilitates effective implementation.

### *4.3.5 Credential holders*

Individuals holding credentials maintain specific rights and responsibilities within the framework.

#### Rights management

Credential holders maintain important rights:

- They control access to their credential information, determining when and how to share credentials. This control protects individual privacy while enabling legitimate credential use.
- They receive clear information about how their credentials function within the framework. This information enables informed credential management.
- They maintain the ability to present their credentials for verification throughout Europe. This capability supports educational and professional mobility.

#### Responsibilities

Credential holders must meet certain obligations:

- They maintain the security of their credential access mechanisms. This security prevents unauthorized credential use.
- They report any suspected unauthorized credential use promptly. This reporting helps maintain system integrity.
- They use their credentials in accordance with framework policies. This compliance supports proper framework operation.

### *4.3.6 Verifying parties*

Organizations verifying credentials must operate within framework requirements.

#### Verification procedures

Verifiers follow established procedures:

- They confirm issuer authority through official registries before accepting credentials. This verification ensures reliance on authorized credentials.

- They check current credential status during verification. This checking prevents reliance on invalid credentials.
- They protect privacy during verification processes. This protection prevents unauthorized tracking of credential use.

#### Data protection

Verifiers maintain privacy protections:

- They collect only necessary information during verification processes. This minimization protects individual privacy.
- They maintain appropriate security for any retained verification records. This security protects sensitive information.
- They follow data retention policies that protect individual privacy. These policies prevent unnecessary data accumulation.

### *4.3.7 Technology providers*

Organizations providing technical solutions must support framework requirements while maintaining security and privacy.

#### System requirements

Providers ensure their solutions:

- Support all required framework functions while maintaining security and privacy. This support enables effective framework operation.
- Implement privacy-protecting features that prevent unauthorized tracking. These features protect individual rights.
- Maintain compatibility with framework standards that ensure interoperability. This compatibility supports system-wide operation.

#### Service management

Providers maintain operational excellence:

- They ensure system reliability and availability that supports framework operation. This reliability maintains system utility.
- They provide necessary technical support to framework participants. This support enables effective system use.
- They maintain security measures that protect framework operation. These measures prevent system compromise.

### *4.3.8 Collaborative responsibilities*

All participants share certain responsibilities:

#### Framework support

Shared obligations include:

- Contributing to framework improvement through feedback and suggestions. This contribution supports continuous enhancement.
- Reporting security or operational issues promptly. This reporting enables quick problem resolution.
- Maintaining awareness of framework updates and requirements. This awareness ensures continued effective operation.

### Privacy protection

All parties must:

- Implement required privacy protection measures. These measures protect individual rights.
- Follow data minimization principles in their operations. This practice prevents unnecessary data collection.
- Maintain appropriate security for framework-related information. This security protects system integrity.

Through clear definition and execution of these roles and responsibilities, the framework maintains efficient operation while protecting all participants' interests. This clarity supports effective credential management while enabling educational and professional mobility across Europe.

## 4.4 Compliance and monitoring framework

### *4.4.1 Overview*

The compliance and monitoring framework ensures the integrity, security, and effectiveness of credential management across Europe. Operating within the non-delegated trust model, this framework establishes mechanisms for maintaining high standards while respecting institutional autonomy and protecting individual privacy.

### *4.4.2 Regulatory compliance*

#### European level requirements

The framework ensures alignment with key European regulations:

- eIDAS Regulation requirements shape credential trust services and electronic identification. This alignment ensures legal recognition of credentials across member states and establishes clear requirements for qualified and non-qualified trust services in educational credentialing.
- General Data Protection Regulation (GDPR) principles govern all personal data handling within the framework. Educational institutions and professional bodies must implement privacy by design, maintain clear legal bases for data processing, and ensure individual rights protection throughout the credential lifecycle.
- Single Digital Gateway Regulation supports efficient cross-border credential recognition. The framework enables once-only submission of credentials while maintaining privacy and security requirements.

#### National level requirements

Framework implementation must accommodate national regulations:

- National education laws and professional qualification requirements guide credential issuance and recognition. This alignment ensures credentials meet local legal and regulatory standards.
- Data protection regulations at national level complement European requirements. Implementation must satisfy both European and national privacy protection standards.

- Professional practice regulations influence credential management for regulated professions. The framework supports specific requirements for professional credential verification and status management.

### *4.4.3 Standards compliance*

#### Operational standards

The framework establishes clear operational requirements:

- Quality assurance standards ensure consistent credential management across institutions. These standards cover issuance, verification, and status management processes.
- Security standards protect credential integrity and system operation. These requirements ensure appropriate protection for credential information and operations.
- Privacy standards maintain individual rights protection throughout credential processes. These standards ensure privacy-preserving operation at all stages.

#### Implementation standards

Participating organizations must meet specific standards:

- Technical infrastructure requirements ensure reliable system operation. These standards support secure, efficient credential management.
- Process requirements establish consistent operational practices. These standards ensure reliable credential handling across organizations.
- Staff qualification requirements ensure proper system operation. These standards maintain operational quality through appropriate training.

### *4.4.4 Monitoring framework*

#### Continuous monitoring

Regular monitoring ensures framework effectiveness:

- Regular system checks ensure smooth operations. These checks help identify and resolve potential problems before they impact service delivery.
- Regular compliance checks verify adherence to framework requirements. These checks maintain high operational standards across participating organizations.
- Performance metrics track framework effectiveness. These measurements support continuous improvement efforts.

#### Audit programs

Comprehensive auditing ensures framework integrity:

- Regular internal audits verify organizational compliance. These reviews ensure consistent adherence to framework requirements.
- External audits provide independent verification of framework operation. These assessments validate framework effectiveness.
- Specialized audits address specific aspects of framework operation. These reviews ensure thorough evaluation of critical functions.

### *4.4.5 Quality management*

#### Process management

Quality management ensures consistent, reliable operation:

- Documented procedures guide all framework operations. These procedures ensure consistent handling of credentials and related processes.
- Change management processes control system evolution. These processes ensure orderly implementation of necessary changes.
- Incident management procedures address operational issues. These procedures ensure appropriate handling of any problems.

#### Performance management

Regular assessment maintains operational excellence:

- Performance indicators track system effectiveness. These metrics enable objective evaluation of framework operation.
- User satisfaction monitoring ensures framework utility. This feedback helps identify improvement opportunities.
- Operational efficiency assessment supports optimization. These evaluations help enhance framework operation.

### *4.4.6 Risk management*

#### Risk Assessment

Continuous risk evaluation protects framework operation:

- Regular risk assessments identify potential threats. These evaluations ensure comprehensive risk awareness.
- Impact analysis determines potential consequence severity. This analysis supports appropriate risk mitigation.
- Mitigation planning addresses identified risks. These plans ensure appropriate risk management.

#### Security management

Comprehensive security measures protect framework operation:

- Access control systems protect credential operations. These controls prevent unauthorized system access.
- Encryption protects credential information. These measures ensure data confidentiality.
- Security monitoring identifies potential threats. This surveillance enables quick response to security issues.

### *4.4.7 Incident management*

#### Response procedures

Clear procedures guide incident handling:

- Incident classification determines appropriate responses. This classification ensures proper handling of different issue types.
- Response protocols guide incident management. These protocols ensure appropriate incident handling.
- Escalation procedures address serious issues. These procedures ensure proper handling of significant problems.

#### Recovery processes

Framework resilience requires robust recovery capabilities:

- Business continuity plans ensure continued operation. These plans maintain essential services during disruptions.
- Disaster recovery procedures address serious incidents. These procedures enable system recovery after significant issues.
- Service restoration priorities guide recovery efforts. These priorities ensure appropriate focus during system restoration.

#### *4.4.8 Improvement framework*

##### Continuous improvement

Regular enhancement maintains framework effectiveness:

- Performance analysis identifies improvement opportunities. This analysis supports systematic enhancement.
- Stakeholder feedback informs improvement efforts. This input ensures changes address actual needs.
- Implementation planning guides enhancement efforts. These plans ensure effective improvement implementation.

##### Innovation management

Framework evolution requires managed innovation:

- Technology assessment evaluates new capabilities. This evaluation identifies valuable innovations.
- Pilot programs test new features. These tests ensure proper operation before full implementation.
- Staged rollout manages implementation risk. This approach ensures controlled introduction of changes.

#### *4.4.9 Reporting framework*

##### Regular Reporting

Systematic reporting maintains transparency:

- Performance reports track system operation. These reports provide clear operational visibility.
- Compliance reports verify requirement adherence. These reports document framework compliance.
- Incident reports document operational issues. These reports ensure proper incident documentation.

##### Stakeholder communication

Clear communication supports framework operation:

- Status updates inform stakeholders of system operation. These updates maintain operational awareness.
- Change notifications announce system modifications. These notifications ensure stakeholder awareness of changes.
- Issue alerts communicate operational problems. These alerts ensure appropriate awareness of issues.

This comprehensive compliance and monitoring framework ensures reliable, efficient credential management while protecting all participants' interests. Through systematic

oversight and continuous improvement, the framework maintains high operational standards while supporting educational and professional mobility across Europe.

## 4.5 Infrastructure requirements

### *4.5.1 Overview*

The infrastructure supporting educational and professional credentials must provide secure, reliable, and efficient operations while protecting privacy and supporting institutional autonomy. These requirements define the essential capabilities needed to support the trust framework's operations without prescribing specific technical implementations.

### *4.5.2 Core infrastructure components*

#### Trust list infrastructure

The framework requires authoritative information about participating organizations:

- A list of authorized credential issuers must maintain current information about educational institutions and professional bodies authorized to issue credentials. This list enables reliable verification of issuer authority while supporting institutional autonomy.
- Status information for authorized issuers must remain current and readily accessible. This availability ensures verifiers can confirm issuer authority during credential verification.
- Regular updates must maintain list accuracy as institutional status changes. This maintenance ensures reliable issuer verification throughout the framework.

#### Credential management infrastructure

Institutions require robust systems for credential operations:

- Credential issuance capabilities must support secure creation and delivery of credentials to recipients. These capabilities ensure reliable credential distribution while maintaining security.
- Status management systems must enable immediate updates to credential validity information. This immediacy ensures current information availability for verification processes.
- Revocation mechanisms must support immediate invalidation of credentials when necessary. This capability ensures proper control over credential validity.

#### Privacy protection infrastructure

Privacy protection requires specific capabilities:

- Selective disclosure mechanisms must enable credential holders to share only necessary information. Issuers disclosures' policies shall be considered, as EAA's become legal binding documents issued and to be used under specific scopes. This control protects privacy while enabling legitimate credential use.
- Data minimization tools must support privacy-preserving credential operations. These tools ensure appropriate privacy protection throughout credential processes.

Co-funded by the European Union

- Consent management systems must maintain individual control over credential sharing. These systems protect individual rights while enabling necessary credential verification.

### *4.5.3 Operational requirements*

#### Availability requirements

Infrastructure must maintain reliable operation:

- High availability systems must support continuous credential operations. This reliability ensures framework utility for all participants.
- Disaster recovery capabilities must protect against service interruption. These capabilities ensure framework resilience.
- Load management systems must handle peak processing requirements. This capacity ensures reliable operation under all conditions.

#### Performance requirements

Infrastructure must maintain efficient operation:

- Response time requirements ensure quick system operation. This performance supports efficient credential processes.
- Throughput capabilities must handle expected transaction volumes. This capacity ensures reliable framework operation.
- Scalability features must accommodate growing system usage. This flexibility supports framework evolution.

#### Security requirements

Infrastructure must protect framework operation:

- Security measures ensure only authorized users can access the system. These measures protect the credibility of all credentials issued.
- The system keeps detailed records of all activities. These records help maintain transparency and accountability.
- Encryption must protect credential information throughout its lifecycle. This protection ensures data confidentiality.

### *4.5.4 Integration requirements*

#### Internal integration

Systems must support institutional operations:

- Integration with academic management systems must support efficient credential issuance. This integration streamlines institutional processes.
- Connection to professional qualification systems must enable efficient credential management. This capability supports professional credentialing processes.
- Links to administrative systems must support operational management. These connections enable efficient framework operation.

#### External integration

Systems must support cross-border operations:

- Integration with European-level systems must support credential recognition. These connections enable cross-border mobility.
- Links to national systems must support local operations. These connections enable framework operation within national contexts.
- Professional body connections must support qualification verification. These links enable professional credential verification.

### *4.5.5 Data management requirements*

#### Data storage

Infrastructure must support appropriate data management:

- Storage systems must maintain credential information securely. This security protects sensitive data.
- Archive capabilities must preserve historical information appropriately. These capabilities support long-term credential validity.
- Backup systems must protect against data loss. This protection ensures operational continuity.

#### Data protection

Infrastructure must ensure appropriate data security:

- Access controls must protect stored information. These controls prevent unauthorized data access.
- Encryption must protect sensitive information. This protection ensures data confidentiality.
- Monitoring must identify potential security issues. This surveillance enables quick response to threats.

### *4.5.6 Support requirements*

#### Operational support

Infrastructure must include support capabilities:

- Help desk systems must support framework participants. This support ensures effective framework use.
- Problem management capabilities must address operational issues. These capabilities ensure reliable framework operation.
- Change management systems must control framework evolution. These systems ensure orderly implementation of changes.

#### User support

Infrastructure must support framework participants:

- User assistance systems must help credential holders manage their credentials. This support ensures effective credential use.
- Verifier support must enable efficient credential verification. This assistance ensures proper credential verification.
- Issuer support must enable effective credential management. This support ensures proper credential handling.

### *4.5.7 Quality assurance requirements*

#### Monitoring capabilities

Infrastructure must support quality management:

- Performance monitoring must track system operation. This monitoring ensures framework effectiveness.
- Compliance checking must verify framework adherence. These checks maintain operational standards.
- Security monitoring must identify potential threats. This surveillance protects framework operation.

#### Testing capabilities

Infrastructure must support quality maintenance:

- Test environments must support feature validation. These environments ensure proper system operation.
- Integration testing must verify system interactions. These tests ensure reliable framework operation.
- Security testing must verify protection measures. These tests ensure appropriate security maintenance.

### *4.5.8 Evolution requirements*

#### Adaptability

Infrastructure must support framework evolution:

- Flexible architecture must accommodate changing requirements. This flexibility ensures framework sustainability.
- Modular design must enable component updates. This modularity supports framework evolution.
- Extensible capabilities must support new features. This extensibility enables framework enhancement.

#### Innovation support

Infrastructure must enable framework advancement:

- Pilot program support must enable new feature testing. This capability ensures proper feature validation.
- Evaluation environments must support innovation assessment. These environments enable feature testing.
- Staged deployment capabilities must support controlled implementation. These capabilities ensure orderly framework evolution.

These requirements align with the technical framework detailed in Chapter 8 and support the use cases presented in Chapter 7.

This infrastructure framework establishes essential capabilities while maintaining implementation flexibility. By focusing on required capabilities rather than specific technologies, it enables effective credential management while supporting framework evolution and institutional autonomy.

Co-funded by the European Union

## 4.6 Benefits of the operational model

### *4.6.1 Overview*

The operational model offers significant advantages for the European education and professional qualification landscape. These benefits are derived from the non-delegated trust model, an inclusive governance structure, and a privacy-respecting approach to credential management. By addressing the challenges of fragmented systems and cross-border recognition, the model supports seamless mobility and trust within the EU. This section outlines the benefits tailored to different stakeholder groups and the alignment with European objectives for educational and professional mobility.

### *4.6.2 Strategic value*

1. Enhanced trust in qualifications
    - Secure, verifiable credentials that ensure authenticity across EU borders.
    - Standardised digital verification provides a reliable framework for recognising qualifications, reducing confusion and disputes.
    - Verification directly from authorised institutions eliminates the need for third-party intermediaries, simplifying processes and ensuring accuracy.
    - Cryptographic security safeguards credentials from tampering, reinforcing the trustworthiness of educational and professional records. For example, universities issuing digitally verifiable diplomas can assure employers of their legitimacy.
2. Improved Educational and Professional mobility
    - Streamlined qualification recognition ensures that students and professionals can easily present and have their credentials recognised throughout EU member states.
    - Accelerated verification processes support faster admissions, job applications, and licensing, enhancing opportunities for individuals.
    - Lower barriers to cross-border education and employment foster an environment where skills and knowledge transfer seamlessly.
    - Enhanced portability of qualifications and certifications simplifies transitions, such as a nurse from Spain being able to quickly present verified credentials when applying to work in Germany.
3. Support for lifelong learning
    - Digital records that include both traditional and non-traditional credentials create a comprehensive, accessible repository for lifelong learning achievements.
    - Integration of micro-credentials allows for recognition of smaller, modular learning experiences that contribute to professional growth.
    - Recognising informal learning and additional certifications helps individuals maintain continuous career development and adaptability in changing job markets.

Co-funded by the European Union

- For example, professionals who earn new skills through workshops or online courses can have these micro-credentials verified alongside formal education.

### *4.6.3 Operational excellence*

1. Administrative efficiency
   - Significant reduction in manual verification processes frees up resources and reduces processing times, enabling institutions to focus on strategic tasks.
   - Automated credential validation and issuance lead to more streamlined workflows and reduced risk of errors.
   - Digital processes lower operational costs by eliminating redundant paperwork and manual record-keeping.
   - For example, universities can streamline admissions by automating the validation of incoming students' credentials, reducing administrative workloads.
2. Enhanced security and fraud prevention
   - Cryptographically secured credentials ensure tamper-proof records, building trust in the validity of shared information.
   - Clear audit trails for all credential actions provide transparency and accountability.
   - Immediate status verification capabilities enable quick identification of suspended or revoked credentials, preventing fraudulent use.
   - Selective disclosure ensures individuals share only necessary information, protecting personal data and enhancing privacy.
3. Optimised resource utilisation
   - Reduced time spent on routine verification tasks allows staff to focus on core educational missions and strategic initiatives.
   - Improved allocation of resources results in better service delivery and enhanced data management capabilities.
   - Digital systems facilitate comprehensive data analytics, supporting informed decision-making and policy planning.
   - Compliance and reporting processes become more straightforward, saving institutions time and effort.

### *4.6.4 Stakeholder benefits*

1. Educational institutions
   - Institutional autonomy: Full control over credential issuance and management aligns with existing practices, enabling customisation according to institutional policies. The ability to implement the model according to unique needs preserves the institution's identity and credibility.
   - Operational efficiency: Automated processes reduce administrative overhead, allowing staff to allocate more resources to student-focused services. Improved data management supports efficient and secure handling of academic records.

- Enhanced service quality: Faster credential processing ensures better service for students and external partners. Institutions can foster better international collaboration by ensuring that their issued credentials are easily verifiable and recognisable abroad.

2. Professional Bodies
   - Enhanced oversight: Reliable systems allow professional bodies to monitor and verify the credentials of their members, ensuring adherence to quality standards. Enhanced tracking of ongoing professional development maintains a high level of competency within regulated fields.
   - Efficient operations: Automation in verification processes reduces administrative tasks, streamlining membership and licensing. Cost-effective operations support long-term sustainability.
   - International recognition: Simplified cross-border recognition processes enhance professional mobility, making it easier for professionals to practise in different EU countries. For example, an engineer certified in Italy can seamlessly present credentials for recognition in other member states.
3. Individuals
   - Enhanced control: Individuals manage their personal credentials securely and share them as needed, protecting their privacy through selective data disclosure. The model ensures that users remain in charge of their data, with the flexibility to present credentials in various contexts.
   - Simplified processes: Easy access and sharing of verified credentials reduce time spent on application procedures. Faster application and enrolment processes enable students and professionals to focus on their growth without bureaucratic delays.
   - Improved opportunities: Broader access to education and employment opportunities is facilitated by the ease of verifying credentials across borders. Clearer career development paths encourage lifelong learning and professional advancement.
4. Society
   - Increased access to education: Lower barriers make education more accessible, supporting inclusion and lifelong learning. Efficient qualification recognition promotes a fairer system where skills and knowledge are valued consistently.
   - Workforce mobility: Simplified professional qualification verification supports free movement, allowing talent to flow where it is needed most. Skills recognition boosts employability and matches labour market demands.
   - Economic efficiency: Cost savings through streamlined verification processes benefit not only institutions but the broader economy. Better skills matching ensures more effective workforce development, driving economic growth.

### *4.6.5 Implementation Benefits*

1. Technical integration
   - Seamless integration with existing digital infrastructure reduces the burden of adoption.

- Standardised interfaces make connecting systems simpler, facilitating interoperability.
- Flexible implementation options allow stakeholders to adapt the model to their specific needs.
- Future-proof architecture ensures compatibility with new technological advancements, supporting continuous improvement.

2. Compliance and governance
   - Adherence to EU regulatory standards ensures alignment with legal and privacy obligations.
   - Strong data protection measures maintain user trust.
   - Transparent governance models foster accountability, providing clear mechanisms for oversight and trust.
3. Support for evolution
   - Adaptability to emerging credential types and evolving requirements ensures that the system can grow with new educational trends.
   - Continuous improvement frameworks encourage ongoing innovation and system optimisation.
   - For example, as new types of digital learning experiences develop, the system can accommodate and certify these credentials efficiently.

The operational model, with its well-defined benefits for all stakeholders, advances the EU's objectives for educational and professional mobility, while upholding high standards of privacy and security. By maintaining context and illustrating practical applications, stakeholders can better appreciate the value this model brings in supporting trust, efficiency, and transparency.

Co-funded by the European Union

# Chapter 5: Natural persons and legal entities onboarding process

This chapter describes the onboarding process for integrating individuals - students and professionals - and legal entities into the digital credential ecosystem. Covering both educational and professional pathways, the chapter highlights the streamlined approach to verifying user identity and credential eligibility. Effective onboarding is essential for ensuring security, user control over personal data, and seamless credential issuance, setting a reliable foundation for lifelong credential portability within the European Union.

## 5.1 Educational onboarding process

### *Overview*

This chapter describes the student onboarding process within an educational institution. The process is divided into three distinct phases: admission, enrolment, and credential issuance. Each phase involves a series of actions, decision points, and interactions between various actors and systems. The following sections outline the key steps in each phase, the actors involved, and the systems required to execute the process.

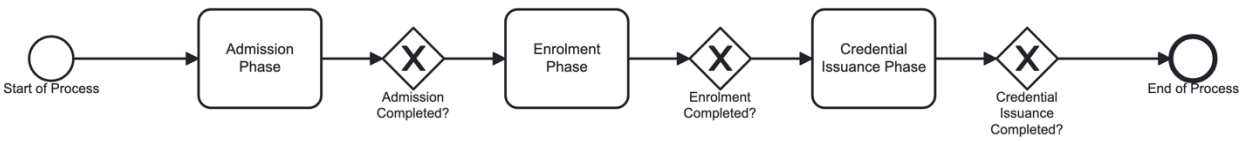
### *Process description*

The student onboarding process ensures that a prospective student progresses from initial application to full enrolment and finally receives their digital credential. Each phase is interconnected and relies on the successful completion of the previous phase. The credential issuance process follows standardized formats based on the W3C Verifiable Credentials Data Model and European Learning Model, ensuring that credentials are both human and machine-readable while maintaining compatibility with European-wide systems.

### *Overall process flow*

Once admission, enrolment and first credential issuance phases are completed, the student is fully onboarded into the institution, with their admission approved, enrolment confirmed, and credential issued.

BPMN Diagram




### *Phases of the onboarding process*

The student onboarding process is structured into three main phases:

1. Admission Phase
2. Enrolment Phase

3. Credential Issuance Phase

Each phase includes specific tasks, interactions, and decision points, which are detailed below.

### Phase 1: Admission

The admission phase is the first stage of the onboarding process. Prospective students begin by submitting their personal and academic details for review. Depending on the method chosen, this data can be submitted directly by the student, or by an authorised institution acting on their behalf.

Actors

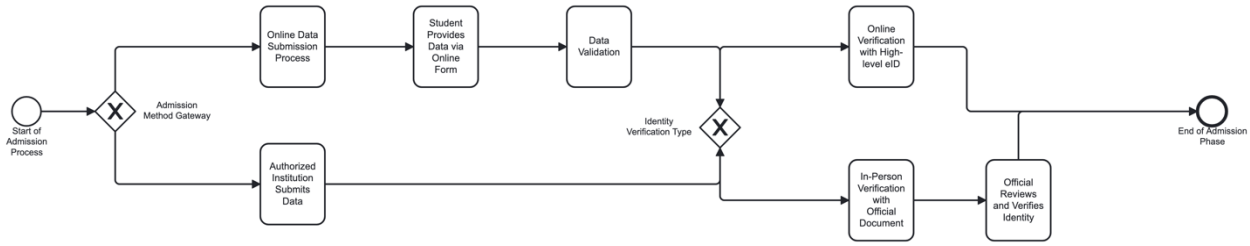
- Student: Provides personal details.
- Educational Institution Official: Reviews the application and verifies identity.
- Authorised Institution Official: Submits data on behalf of the student (if applicable).

Process description

- Data submission: The student can submit their data through the institution's online admission portal.
- Identity verification: Once the data is submitted, the institution uses an identity verification system to confirm the applicant's identity.
- Data validation: Following identity verification, the data is validated to ensure its accuracy and compliance with institutional requirements.
- Alternate submission: If an authorised institution submits the data, the same validation and identity verification steps apply.

The admission phase concludes once the data is successfully validated.

BPMN Diagram Placeholder




### Phase 2: Enrolment

The enrolment phase begins once the admission process has been completed. During this phase, the student authenticates their identity, selects courses, and completes any necessary payments.

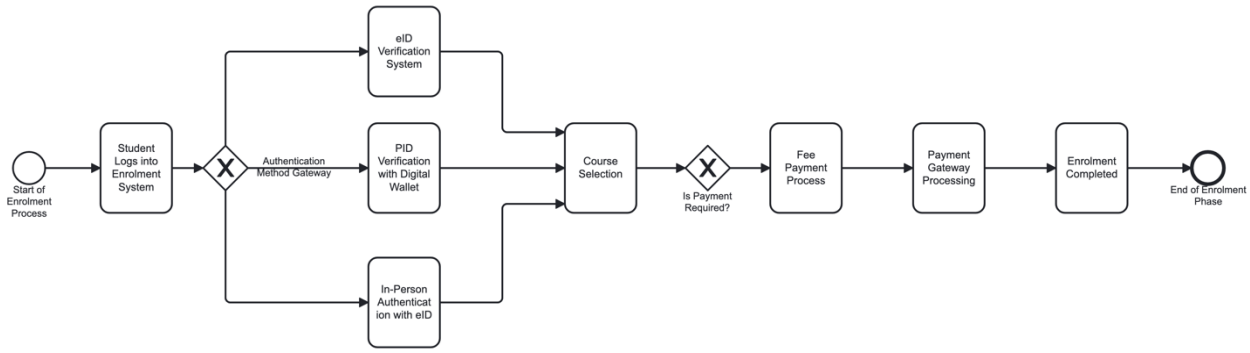
Actors

- Student: Logs into the system, selects courses, and makes payments (if required).
- Enrolment Management System: Manages the enrolment process and course selection.
- Authentication System: Verifies the student's identity (via eID, EUDI wallet, or in-person).
- Payment System Provider: Processes payments for course enrolment.

Process Description

- Authentication: The student logs into the enrolment management system and is prompted to authenticate their identity using a national eID, a EUDI wallet with personal identity data (PID), or in-person verification.
- Course selection: Once authenticated, the student gains access to the course catalogue and selects their courses.
- Payment: If payment is required for the chosen programme, the system directs the student to a secure payment gateway.
- Enrolment completion: Upon completing the course selection and payment, the student's enrolment is confirmed, and they can proceed to the next phase.

BPMN Diagram




## Phase 3: Credential Issuance

The credential issuance phase involves providing the student with a digital credential (EducationalID), which grants them access to institutional services.

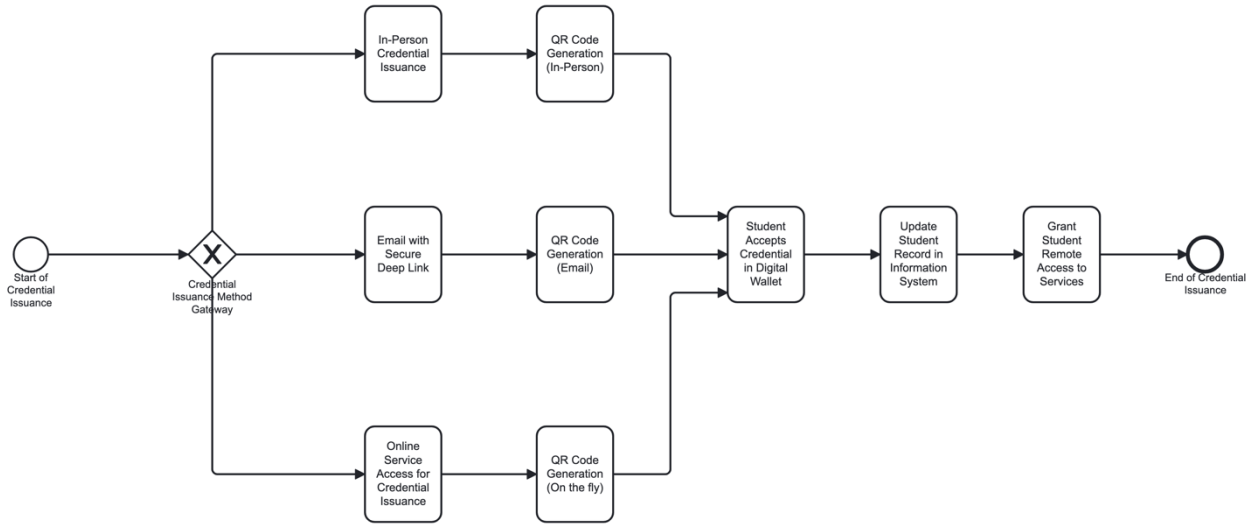
Actors

- Student: Receives the digital credential and accepts it into their EUDI wallet.
- Credential Issuance System: Manages the creation and issuance of the digital credential.
- QR Code Generation System: Generates a QR code for the credential.
- Student Information System: Updates the student's record.
- Remote Access System: Grants the student access to the institution's remote services.

Process Description

- Credential issuance options: The student has three options to receive their credential:
  - In-person: The student visits the academic secretary's office, where an official generates a QR code, which the student scans with their EUDI wallet.
  - Email: The student receives an email containing a secure deep link that directs them to a QR code, which they scan to accept the credential.
  - Online: The student logs into an online portal, authenticates, and scans the QR code to receive the credential.
- Credential acceptance: After scanning the QR code, the student accepts the credential into their EUDI wallet.
- Student information update: The system updates the student's record to reflect the successful issuance of the credential.
- Remote access: Once the credential is issued, the student is granted access to the institution's remote services.

BPMN Diagram




*Actors and Systems Overview*

| Actor/System | Role |
|---|---|
| **Student** | Initiates the admission process, enrols in courses, and receives the digital credential. |
| **Educational Institution Official** | Reviews applications and verifies student identity. |
| **Authorised Institution Official** | Submits data on behalf of the student (if applicable). |
| **Online Admission Portal** | Receives student data and forwards it for validation and review. |

| | |
|---|---|
| **Identity Verification System** | Verifies the identity of the student through online or in-person methods. |
| **Data Validation System** | Confirms the accuracy of the student‚Äôs application data. |
| **Enrolment Management System** | Manages student enrolment, including authentication and course selection. |
| **Authentication System** | Provides identity verification for the student during the enrolment process. |
| **Payment Gateway** | Processes payments for course enrolment, interacting with the payment system provider. |
| **Payment System Provider** | Handles secure payments and confirms payment transactions. |
| **Credential Issuance System** | Manages the creation and issuance of the student‚Äôs digital credential. |
| **QR Code Generation System** | Generates QR codes used for credential acceptance. |
| **Student Information System** | Updates the student‚Äôs record after credential issuance. |
| **Remote Access System** | Provides access to the institution's remote services after credential issuance. |

## 5.2 Professional qualifications onboarding process

### *Overview*

This chapter describes the professional qualifications onboarding process within authorized professional bodies and associations. The process is divided into three distinct phases: request, enrolment, and credential issuance. Each phase involves a series of actions, decision points, and interactions between various actors and systems. The following sections outline the key steps in each phase, the actors involved, and the systems required to execute the process.

### *Process description*

The professional qualifications onboarding process ensures that a professional progresses from initial request to full enrolment and finally receives their digital credentials. Each phase is interconnected and relies on the successful completion of the previous phase.

### *Overall process flow*

Once request, enrolment and credential issuance phases are completed, the professional is fully onboarded into the system, with their request approved, enrolment confirmed, and credentials issued.

### *Phases of the onboarding process*

The professional qualifications onboarding process is structured into three main phases:

1. Request Phase
2. Enrolment Phase
3. Credential Issuance Phase

Each phase includes specific tasks, interactions, and decision points, which are detailed below.

### Phase 1: Request

The request phase is the first stage of the onboarding process. Professionals begin by logging into their association's platform and submitting their personal and professional details for review.

Actors

- Professional: Provides personal and professional details

- Professional Association Official: Reviews the application and verifies identity
- Identity Verification Service Provider: Validates the professional's identity

Process description

- Platform Access: The professional logs into the association's platform using existing credentials
- Identity verification: The professional's identity is verified through online or in-person methods
- Data validation: Following identity verification, the data is validated to ensure its accuracy and compliance with professional requirements

The request phase concludes once the data is successfully validated.

### Phase 2: Enrolment

The enrolment phase begins once the request process has been completed. During this phase, the professional authenticates their identity, selects required credentials, and completes any necessary payments.

Actors

- Professional: Authenticates identity and selects credentials
- Professional Association Official: Oversees the enrolment process
- Authentication System: Verifies the professional's identity
- Payment System Provider: Processes payments if required

Process Description

- Authentication: The professional authenticates their identity using a national eID, a EUDI wallet with personal identity data (PID), or in-person verification
- Credential Selection: Once authenticated, the professional selects the required credentials
- Payment: If payment is required, the system directs the professional to a secure payment gateway
- Enrolment completion: Upon completing the credential selection and payment, the professional's enrolment is confirmed

### Phase 3: Credential Issuance

The credential issuance phase involves providing the professional with digital credentials that verify their qualifications and enable them to practice their profession.

Actors

- Professional: Receives the digital credentials and accepts them into their EUDI wallet
- Professional Association Official: Manages credential issuance

- Credential Issuance System: Manages the creation and issuance of digital credentials
- QR Code Generation System: Generates QR codes for credential acceptance
- Central Registry System: Updates the professional's record

Process Description

- Credential issuance options: The professional has three options to receive their credentials:
  - In-person: Visit to the association office where an official generates a QR code
  - Email: Receive an email containing a secure deep link to a QR code
  - Online: Log into an online portal, authenticate, and scan the QR code
- Credential acceptance: After scanning the QR code, the professional accepts the credentials into their EUDI wallet
- List update: The system updates the professional's record in the central list
- Access grant: Once credentials are issued, the professional can share them with employers or regulatory bodies as needed

### Actors and Systems Overview

| Actor/System | Role |
|---|---|
| **Professional** | Initiates the request process, completes enrolment, and receives digital credentials |
| **Professional Association Official** | Reviews applications and verifies professional identity |
| **Platform Access System** | Manages professional login and initial data submission |
| **Identity Verification System** | Verifies the identity through online or in-person methods |
| **Data Validation System** | Confirms the accuracy of the professional's application data |
| **Authentication System** | Provides identity verification during the enrolment process |
| **Payment Gateway** | Processes payments when required |
| **Credential Issuance System** | Manages the creation and issuance of digital credentials |
| **QR Code Generation System** | Generates QR codes for credential acceptance |
| **Central Registry System** | Updates the professional's records after credential issuance |
| **Email System** | Delivers secure links for online credential acceptance |
| **Remote Access System** | Enables credential sharing with employers and regulatory bodies |

## 5.3 Legal entities onboarding process

### *5.3.1 Introduction*

Legal entities must join the trust framework through a structured process that maintains quality and trust across the credentialing ecosystem. This chapter explains how organisations become authorised members of the framework.

The inclusion of legal entities in the trust framework represents a critical step in establishing a reliable credential ecosystem. Each organisation's participation adds to the framework's value, creating a network of trusted credential issuers and verifiers across Europe. This process builds upon existing regulatory structures while adding the necessary digital trust layer for modern credential management.

The onboarding process follows the non-delegated trust model from Chapter 4, with each organisation retaining direct control of their credentials within the European framework. This approach respects institutional autonomy while ensuring consistent standards across the network.

#### 5.3.1.1 Participating organisations

The framework's effectiveness depends on the participation of diverse organisations across the education and professional qualification sectors. Each type of organisation brings specific value to the ecosystem, contributing to a comprehensive network of trusted credential issuers and verifiers.

The framework accepts these organisations:

- 1. Educational bodies
  - Universities
  - Higher education institutions
  - Vocational education providers
  - Professional education centres
  - Continuing education organisations

  These institutions form the core of the credential issuance network, providing primary academic and professional qualifications that serve as the foundation for career development and further education.

- 2. Professional organisations
  - Professional associations
  - Industry certification bodies
  - Regulatory bodies

- Quality control agencies

Professional organisations add sector-specific expertise and validation, ensuring credentials meet industry standards and professional requirements.

- 3. Accreditation bodies
  - National accreditors
  - Subject-specific accreditors
  - International accreditors

Accreditation bodies provide quality assurance across the network, validating the standards of both educational and professional credentials.

- 4. Public authorities
  - Education ministries
  - Professional regulators
  - Quality oversight bodies

Public authorities establish the regulatory framework and provide official recognition of credentials at national and European levels.

### *5.3.2 Entry requirements*

The entry requirements establish baseline standards for participation in the trust framework. These requirements balance the need for rigorous verification with practical implementation considerations, ensuring that participating organisations can maintain high standards while operating efficiently.

#### 5.3.2.1 Legal standards

Legal standards protect the integrity of the credential ecosystem and ensure compliance with European and national regulations. These requirements create a foundation of trust through verified legal status and demonstrated compliance with relevant education and professional standards.

Organisations must meet these requirements:

- Legal position
  - Registration in home country
  - Education law compliance
  - Qualification authority
  - Good standing proof
- Rules compliance
  - Education standards met
  - Professional recognition

    - Data protection measures
    - Cross-border permissions
- Quality checks
    - Current accreditation
    - Quality systems
    - External reviews
    - Written procedures

#### 5.3.2.2 Technical standards

Technical standards ensure that participating organisations can interact securely and efficiently within the digital credential ecosystem. These requirements focus on practical capabilities needed for secure credential management while maintaining flexibility in specific implementation approaches.

Organisations need these capabilities:

- Systems
    - Protected IT setup
    - Data safeguards
    - Digital signatures
    - Recovery plans
- Connection methods
    - API readiness
    - Identity systems
    - Credential tools
    - Checking processes
- Work methods
    - File management
    - Record tracking
    - Staff preparation
    - Problem response

### *5.3.3 The joining process*

The joining process addresses three distinct governance types that shape how legal entities participate in the trust framework:

#### 5.3.3.1 Entitlement governance onboarding

This process establishes an organisation's legal authority to act within the education or professional qualifications domain:

- Verification of legal basis

    - National authority confirmation
    - Legal scope definition
    - Cross-border recognition status
    - Regulatory compliance check
- Domain authority establishment
    - Qualification issuing rights
    - Professional recognition scope
    - Geographic coverage
    - Authority limitations
- Framework registration
    - Legal entity identifier assignment
    - Authority scope documentation
    - Public registry inclusion
    - Status publication

#### 5.3.3.2 Quality assurance regime onboarding

This process integrates organisations into the quality assurance framework:

- Quality framework alignment
    - Standards mapping
    - Assessment processes
    - Review cycles
    - Improvement mechanisms
- Audit process establishment
    - Audit schedule setting
    - Assessment criteria
    - Evidence requirements
    - Review procedures
- Accreditation integration
    - Recognition processes
    - Standard alignment
    - Cross-border applicability
    - Renewal procedures

#### 5.3.3.3 Non-foundational identity governance onboarding

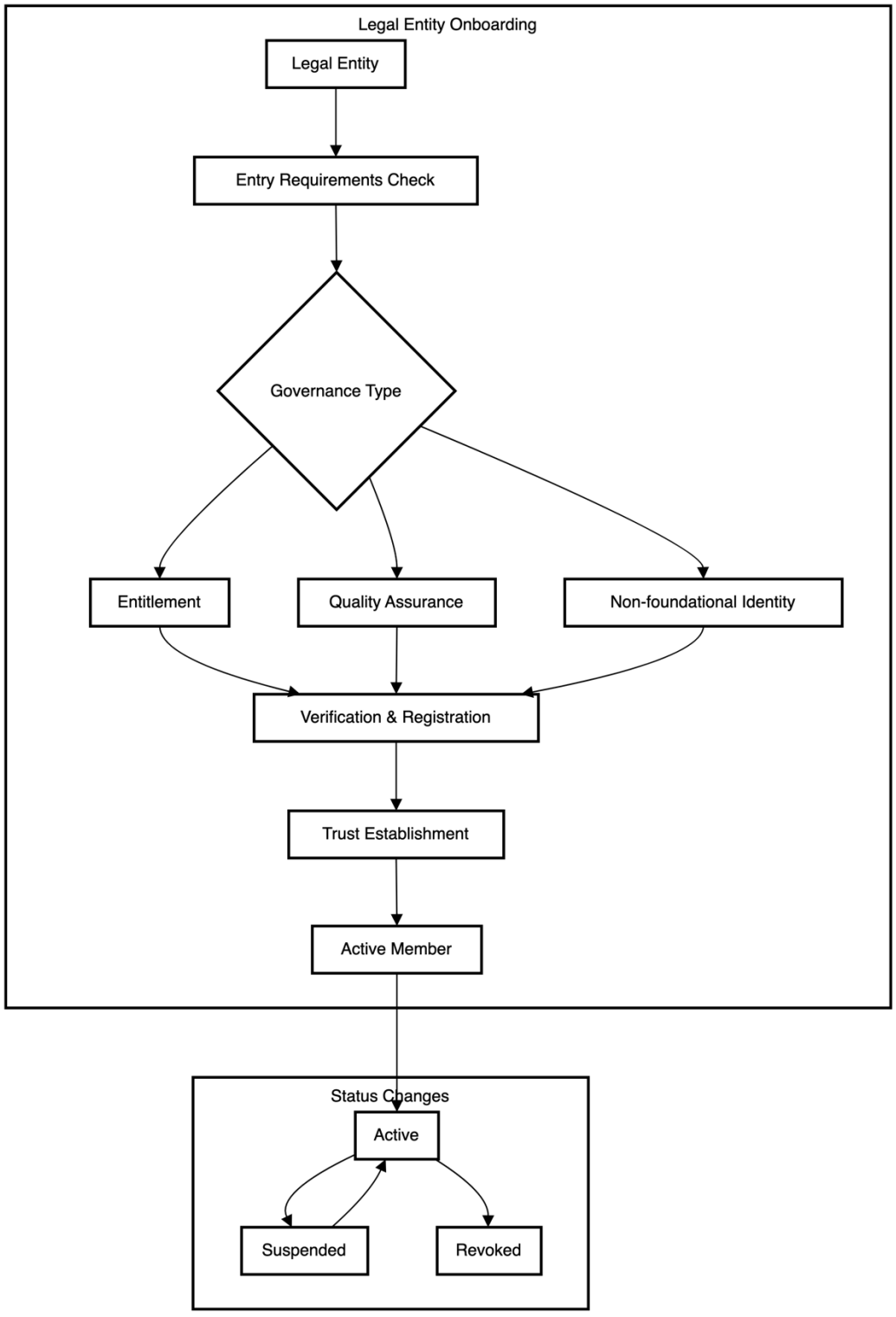
This process enables organisations to participate in non-foundational identity credential issuance (credentials under trust services legal regime, not eID legal regime):

- Identity credential authority
    - Credential type definition
    - Issuance scope
    - Verification mechanisms
    - Privacy safeguards

- Technical integration
  - Identity systems setup
  - Verification infrastructure
  - Privacy controls
  - Security measures
- Operational procedures
  - Identity verification processes
  - Credential lifecycle management
  - Status update mechanisms
  - Privacy protection measures

### *5.3.4 Flow diagram*

The onboarding of legal entities into the trust framework follows a structured process that addresses three distinct governance types: entitlement, quality assurance, and non-foundational identity. Each flow represents a specific aspect of establishing trust and authority within the framework.



# Chapter 6: The education and professional qualifications sectorial rulebook

The education and professional qualifications sectorial rulebook aims to establish a standardised approach for managing digital educational and professional credentials within the European Union. The rulebook sets the foundation for trusted digital credential management, encompassing identity, trust, data models, and operational processes. This framework balances member state sovereignty with European integration needs, creating a unified system that supports educational mobility while respecting national and institutional autonomy.

Each component serves both practical needs and policy goals, creating a system that works for students, institutions, and member states while advancing European educational integration.

The technical implementations always support policy priorities, making the system both practically useful and politically aligned with European goals for education, privacy, and mobility.

The complete system brings together European educational priorities:

- Respects member state sovereignty in education
- Maintains institutional independence
- Protects student privacy
- Supports educational mobility
- Links to quality frameworks
- Creates trusted credentials
- Enables automatic recognition
- Supports lifelong learning
- Records formal and informal learning
- Works across European borders

## 6.1 Natural person's identity

The European Digital Identity wallet serves as a harmonised electronic identification method, introducing personal identification data (PID) as the preferred option when high security is needed. This system respects member state authority over identity while creating a consistent European approach.

This approach streamlines identity verification in educational contexts, particularly in two main processes:

- Registration and enrolment: When students begin their educational journey, requiring secure identification
- Formal degree issuance: When official qualifications are awarded, needing reliable identity confirmation

## 6.2 Legal entity's identity

Educational institutions need reliable digital identification through public key infrastructure (PKI) with X.509v3 digital certificates. This system assigns unique digital identifiers to institutions, linking them with public certificates for seamless identity verification across European systems. The public key infrastructure (PKI) with X.509v3 digital certificates provides this balance, letting institutions participate in European-wide systems while keeping their internal processes intact.

## 6.3 Identity matching

The combination of personal identification data and member state-specific matching rules creates a unified approach to identity verification. The rulebook acknowledges the complexity of European identity systems by combining personal identification data with member state-specific matching rules. This approach respects national sovereignty while creating reliable links between national identities and institutional records, making student identification more accurate across borders.

This system helps educational institutions connect external identities (issued by national authorities) with their internal systems, making student identification more accurate and efficient.

## 6.4 Trusted lists

The system maintains several critical lists to support trust in educational credentials:

- Trusted issuers: Authorised organisations that can issue credentials, ensuring only legitimate institutions can grant qualifications
- Relying parties: Organisations authorised to verify and accept credentials
- Trusted accreditation organisations: Bodies that validate educational institutions, maintaining quality standards
- Data models catalogue: Standardised formats for representing educational credentials
- Trusted schemes: Templates ensuring consistent credential structure

Within the the trust framework, trust lists support European education policy through several interconnected lists:

- Trusted issuers: Maintains academic integrity by authorising legitimate institutions
- Relying parties: Creates clear paths for credential recognition
- Trusted accreditation organisations: Links to European quality frameworks like EQAR
- Data models catalogue: Enables consistent credential representation
- Trusted schemes: Supports automated processing across systems

## 6.5 Lifecycle management

The credential lifecycle system supports educational mobility while protecting credential integrity. This balance enables institutions to manage qualifications independently while ensuring European-wide recognition. The system incorporates privacy-by-design principles, letting institutions update credential status without tracking usage patterns.

Managing educational credentials requires careful tracking from creation through to potential revocation and/or suspension. The system:

- Tracks credential status changes (active, suspended, revoked)
- Maintains verification services that respect privacy
- Provides tools for educational institutions to manage their issued credentials

## 6.6 Data model

The credential data model follows W3C Verifiable Credential standards, structuring educational data in a consistent format. Each credential includes:

- Context definitions for clear interpretation
- A unique identifier
- The credential type
- The issuing authority's identifier
- Issue date
- Information about the credential holder
- Cryptographic proof of authenticity
- Multi-language support

## 6.7 Education and professional qualifications Ontology - European Learning Model (ELM)

The ELM creates a shared understanding of educational achievements across Europe. Supporting and facilitating quality assurance information, links to European and National qualification frameworks and cross-border recognition support, the model covers:

- Achievement records:
  - Qualification titles and descriptions
  - Classification of the achievement
  - European Qualification Framework alignment
  - Issue dates
  - Issuing institution details
- Learning outcomes:
  - Knowledge gained
  - Skills developed

    - Competences achieved
    - Links to European skills frameworks
- Learning activities:
    - Type of education received
    - Duration of study
    - Learning delivery method
- Assessment details:
    - Evaluation methods used
    - Grading systems
    - Assessment authority
- Issuer information:
    - Legal institution name
    - Accreditation status
    - Contact information
    - Digital identification
- Holder details:
    - Personal identification compliant with privacy laws
    - Educational profile linkage
- Recognition elements:
    - Cross-border agreements
    - Framework alignments
    - European Education Area mobility support
- Supporting data:
    - Links to course documentation
    - Language of instruction
    - Geographic context

## 6.8 Issuance

The issuance process varies based on the type of attestation:

- Qualified electronic attestation of attributes (QEAA):
    - Provided by qualified trust service providers
    - Requires citizen consent
    - Needs data validation through member state mechanisms
- Public sector body electronic attestation of attributes (PSBEAA):
    - Issued by public sector bodies
    - Must meet specific regulatory requirements
    - Public sector bodies act as both authentic source and issuer
- Electronic attestation of attributes (EAA) issuance follows these steps:
    1. Secure connection with the European Digital Identity Wallet
    2. Identity verification when required
    3. Identity matching processes
    4. Data gathering from authentic sources
    5. Credential creation using trusted schemas

Co-funded by the European Union

6. Addition of quality assurance information
7. Digital identifier selection
8. Direct or deferred issuance to the wallet

## 6.9 Selective disclosure

The system enables users to share only necessary credential data, meeting privacy requirements through:

- Technical implementations like SD-JWS, SD-JWT and BBS+
- Issuer-defined disclosure policies
- Privacy-preserving verification methods

## 6.10 Sharing mechanisms

The credential sharing framework supports European mobility through:

- Cross-border credential recognition
- Privacy-protected verification
- Quality assurance validation
- Institutional trust verification

The credential sharing system uses OpenID for Verifiable Presentations to:

- Establish secure connections with wallets
- Verify proof of possession
- Check relying party trustworthiness
- Validate information proportionality
- Enable credential combination
- Support selective disclosure policies

## 6.11 Verification

The verification process ensures credential validity while protecting privacy:

- Key characteristics:
  - Distributed system to avoid single points of failure
  - Privacy protection from issuer monitoring
  - Time-based validation linked to credential issuance

- The verification process follows these steps:
  1. Secure wallet connection and proof of possession
  2. Credential request
  3. Integrity verification
  4. Metadata checking (expiration dates)
  5. Issuer verification:
     - Digital identifier validation
     - Educational accreditation checking

- Accreditation issuer verification
- Status verification

6. Identity information analysis
7. Schema compliance checking
8. Quality assurance verification:
   - Issuer entitlement checking
   - Expiration verification
   - Status checking
9. Credential status verification
10. Record keeping for audit purposes

## 6.12 Enforcement policy agent

The wallet's policy enforcement role implements European privacy principles in practical ways:

- Students control their educational records
- Institutions request only necessary data
- Systems prevent excessive data collection
- Privacy protection becomes automatic
- Cross-border rights remain protected

Digital wallets act as policy enforcers by:

- Detecting disproportionate information requests
- Warning users about excessive data sharing
- Blocking unauthorised information access
- Maintaining user control over personal data

To fully respect individual's rights, "Blocking" won't be applied at sectorial level.

## 6.13 Supporting infrastructure

The underlying system requires:

- Multi-domain and sector support
- Distributed architecture
- Pan-European coverage
- Privacy-enhanced verification
- Data protection compliance
- Security audit mechanisms
- Verification record keeping
- Service discovery tools
- Cross-country legal entity mandatory recognition

This infrastructure supports the entire credential ecosystem while maintaining security, privacy, and usability across European educational systems.

Co-funded by the European Union

# Chapter 7: Use Cases and implementation scenarios

To illustrate the practical applications of the trust framework, this chapter presents a series of use cases and scenarios that demonstrate its functionality in educational and professional contexts. These examples provide insights into how digital credentials can be issued, verified, and shared across borders, addressing key challenges such as identity verification, fraud prevention, and data privacy. By showcasing real-world applications, this chapter aims to clarify the benefits of a unified credentialing approach for institutions, individuals, and employers within the EU.

## 7.1 Introduction to Use Cases in the Trust Framework

The implementation of a trust framework for educational and professional credentials across Europe represents a significant shift in how qualifications are issued, managed, shared and verified. This chapter aims to provide an overview of the types of use cases that demonstrate the practical application and benefits of this framework. While specific use cases will be developed later, this section will outline the general categories and importance of these use cases in illustrating the framework's value.

These use cases demonstrate how the implementation of standards such as W3C Verifiable Credentials and the European Learning Model enables secure, verifiable, and interoperable credential management across different scenarios and stakeholder needs.

Use cases serve several critical functions in the context of the trust framework:

- Demonstration of practical benefits: They show how the framework solves real-world problems in credential management.
- Stakeholder engagement: Use cases help different stakeholders understand how the framework applies to their specific needs and contexts.
- Implementation guidance: They provide concrete examples that can guide the implementation process for various institutions and organisations.
- Gap analysis: By mapping current processes against future scenarios, use cases help identify areas needing development or adjustment.

These use cases demonstrate the practical implementation of:

- The operational model detailed in Chapter 4
- The technical framework specified in Chapter 8
- The trust model outlined in Section 4.1

## 7.2 Categories of Use Cases

The trust framework's use cases can be broadly categorised into several key areas:

1. Credential Issuance:

- This category includes scenarios related to how educational institutions and professional bodies issue digital credentials.
- It covers the process from the completion of educational and professional requirements to the secure issuance of a digital credential.
- These use cases will demonstrate how the framework ensures the authenticity and integrity of newly issued credentials.

2. Credential Verification:
- These use cases focus on how employers, educational institutions, and other authorised parties can verify credentials.
- They will showcase the efficiency and reliability of the verification process compared to traditional methods.
- Scenarios in this category will address both domestic and cross-border verification challenges.

3. Learner Empowerment:
- Use cases in this area will illustrate how learners can manage and share their credentials.
- They will demonstrate the increased control and privacy that learners have over their educational data.
- Scenarios will include how learners can compile and present their qualifications for various purposes.

4. Lifelong Learning Support:
- These use cases will show how the framework supports the accumulation and recognition of diverse learning experiences.
- They will cover scenarios involving micro-credentials, non-formal learning, and continuous professional development.
- The focus will be on how the framework facilitates a comprehensive view of an individual's learning journey.

5. Cross-Border Mobility:
- This category will include scenarios that demonstrate how the framework facilitates studying or working in different EU countries.
- Use cases will show how the framework simplifies the recognition of qualifications across borders.
- They will address challenges related to different educational and professional systems and qualification frameworks.

6. Fraud Prevention and Detection:
- These use cases will illustrate how the framework prevents credential fraud and detects fraudulent activities.
- They will demonstrate the security features of the system and how they protect the integrity of credentials.
- Scenarios will include how the system handles credential revocation and updates.

7. Institutional Integration:
- Use cases in this category will show how educational institutions can integrate the framework into their existing systems.
- They will cover scenarios of migration from traditional to digital credential systems.
- These use cases will address challenges and solutions in adopting the new framework.

8. Employer and Recruitment Scenarios:
- These will focus on how the framework streamlines recruitment processes for employers.
- Use cases will demonstrate how the system facilitates more efficient and accurate candidate assessment.
- They will show how the framework supports skills-based recruitment and talent mobility.

9. Data Analytics and Policy Making:
- This category will include scenarios showing how the framework can provide insights for educational policy making.
- Use cases will demonstrate how aggregated, anonymised data can inform curriculum development and labour market alignment.
- They will address how the system maintains privacy while providing valuable analytical insights.

10. Continuous Professional Development:
- These use cases will focus on how the framework supports ongoing professional learning and certification.
- They will demonstrate how professional bodies can issue and manage credentials for continuing education.
- Scenarios will include how professionals can showcase their up-to-date qualifications and skills.

## 7.3 Structure of Use Cases

Each use case, when developed, will typically include the following elements:

- Title
- Context: Background information setting the scene for the use case.
- The story
- Actors: The stakeholders involved in the scenario.
- Current Process ("As-Is"): A description of how the process currently works without the trust framework.
- Future Process ("To-Be"): An illustration of how the process would work with the trust framework implemented.

Co-funded by the European Union

- Benefits: A clear articulation of the advantages the new system brings to this specific scenario.
- Challenges: Potential obstacles or considerations in implementing this use case.
- Technical Requirements: Key technical components or standards needed to support this use case.
- Detailed user journey steps

## 7.4 Importance of User Journeys

User journeys will be an integral part of developing these use cases. They will provide a step-by-step walkthrough of how different users interact with the system in various scenarios. These journeys are crucial for:

1. User-centric design: Ensuring the system meets the needs and expectations of its users.
2. Identifying pain points: Highlighting areas where the current system falls short and how the new framework addresses these issues.
3. Demonstrating value: Clearly showing the benefits of the new system from a user's perspective.
4. Guiding implementation: Helping developers and institutions understand the user experience they need to deliver.

## 7.5 Cross-cutting themes

Across all use cases, several themes will be consistently addressed:

- Privacy and data protection: How the framework ensures compliance with GDPR and other privacy regulations.
- Interoperability: Demonstrating how the system works across different platforms and national systems.
- User control: Showcasing how individuals maintain control over their credentials and personal data.
- Trust and security: Illustrating the mechanisms that ensure the authenticity and integrity of credentials.
- Scalability: Showing how the system can handle increasing numbers of users and credentials.
- Accessibility: Ensuring the system is usable for people with diverse needs and backgrounds.

## 7.6 Stakeholder engagement in Use Case development

Co-funded by the European Union

The development of these use cases will involve engagement with various stakeholders, including:

- Educational institutions
- Employers and industry representatives
- Government agencies and policy makers
- Students and lifelong learners
- Professional bodies and accreditation agencies
- Technology providers and developers

This multi-stakeholder approach ensures that the use cases reflect real-world needs and scenarios, making them more relevant and applicable.

## 7.7 Use cases

### 7.7.1 Non-foundational identity

#### *7.7.1.1 Enhancing student mobility through verifiable digital credentials in European University Alliances*

Context

European universities are forming alliances to improve student mobility and collaboration, aligning with European Education Area goals. These alliances aim to create a seamless ecosystem for student mobility across European higher education institutions. This system builds upon and enhances existing identification methods such as MyAcademicID and the European Student Identifier (ESI), addressing their limitations and providing a more comprehensive solution.

The story

Eva had always dreamed of studying abroad, but the thought of navigating the complex web of university applications across different countries had always seemed daunting. As she sat at her desk, staring at her computer screen, she couldn't help but feel a mix of excitement and nervousness. She was about to embark on a journey that would test the new European University Alliance system, a digital platform designed to make cross-border education more accessible.

With a deep breath, Eva opened her EUDI wallet app. Inside, she found her newly issued EducationalID and MyAllianceID, secure digital credentials provided by her home institution, University A1. These weren't just ordinary digital documents; they were comprehensive identifiers that went beyond the traditional MyAcademicID and European Student ID (ESI). The EducationalID contained all the claims of these previous systems, but with added flexibility and functionality that overcame their limitations.

Eva marvelled at how her EducationalID simplified her identity across different systems. Unlike the ESI, which was tied to specific mobility programmes, or the MyAcademicID with its limited scope, her EducationalID could be used seamlessly across all alliance

institutions. It contained all her relevant academic information, making identity matching between institutions much easier and more reliable.

Eva's first step was to browse the course catalogue of University Duisburg-Essen, another member of the alliance. As she scrolled through the list of available courses, her eyes lit up at the prospect of studying subjects she had always been passionate about but weren't available at her home university. She selected an intriguing course and clicked 'Apply'.

To her surprise, the application process was remarkably smooth. Instead of the usual tedious form-filling and document uploading, Eva was simply prompted to share her EducationalID and MyAllianceID from her EUDI wallet. With a few clicks, her credentials were securely transmitted to University Duisburg-Essen.

Behind the scenes, University Duisburg-Essen's systems were hard at work. They verified Eva's credentials through the alliance portal, checking her student status and academic qualifications. In a matter of minutes, Eva received a notification: her application had been accepted, and she was enrolled in the course.

As Eva applied to University Duisburg-Essen, she realised another advantage of her EducationalID. The receiving institution could easily match her identity across their systems, something that had been a challenge with previous identification methods. This streamlined the entire application process, reducing administrative burden for both Eva and the university.

As the term progressed, Eva found herself thriving in her new academic environment. She attended virtual lectures, participated in online discussions with students from across Europe, and submitted assignments through the alliance's learning management system. The seamless integration of technologies made her feel as if she were studying at her home university, despite being hundreds of miles away.
Weeks flew by, and before she knew it, the course was coming to an end. Eva submitted her final project, feeling a sense of accomplishment. A few days later, she received a notification on her EUDI wallet app. University Duisburg-Essen had issued her a verifiable Transcript of Records, a digital credential certifying her successful completion of the course.

Excited about her achievement, Eva decided to share this new credential with her home university, University Rovira i Virgili. Again, the process was surprisingly simple. She selected the credential in her EUDI wallet and authorised its sharing with University Rovira i Virgili. Within moments, her home university had received and verified the credential, automatically updating her academic record to reflect the credits she had earned.

Encouraged by this positive experience, Eva began to explore more opportunities within the alliance. She discovered a workshop at University A3 that perfectly complemented

her studies. The application process was just as smooth as before, using her alliance credentials to quickly secure a spot.

As Eva reflected on her journey, she marvelled at how technology had transformed her educational experience. Gone were the days of paperwork, long waiting periods, and uncertainty about credit transfers. The European University Alliance had opened up a world of possibilities, allowing her to craft a unique educational path that crossed borders with ease. She also appreciated how her EducationalID had smoothed her path. It had eliminated the need for multiple logins and separate identities for different aspects of her academic life. Whether she was applying for courses, accessing library resources, or sharing her academic achievements, her EducationalID served as a unified, trusted academic identity across the alliance.

Eva's story demonstrates how the European University Alliance system, particularly through the enhanced EducationalID, is revolutionising higher education. By building upon and improving existing systems like MyAcademicID and ESI, it's creating a more integrated, flexible, and user-friendly experience. For students like Eva, it's not just about simplifying processes; it's about having a unified academic identity that works seamlessly across borders, expanding their educational horizons in ways that were once unimaginable .

Actors

- Students (Users of the system who hold EducationalID and MyAllianceID credentials. These credentials incorporate and expand upon the functionality of MyAcademicID and ESI)
- Universities (home and host institutions)
- European University Alliances
- Ministries of Education
- IT service providers

Current Process ("As-Is")

Students navigate multiple systems and provide various documents when applying for courses at different institutions. Verifying credentials is time-consuming and error-prone. Recognition of academic achievements across institutions is often complicated. Current systems like the European Student Identifier (ESI) or MyAcademicID are often tied to specific mobility programmes, limiting their flexibility and usefulness across different academic contexts..

---

Students receive verifiable EducationalID and MyAllianceID credentials directly from their home institution to their EUDI wallet. These digital identities enable:

- Secure sharing of academic credentials: The EducationalID contains all relevant claims from MyAcademicID and ESI, but offers greater flexibility and functionality across all alliance institutions.
- Simplified authentication and access to services across alliance institutions

- Self-sovereign identity, giving students control over their personal data
- Selective disclosure of academic information
- Improved identity matching: The comprehensive nature of the EducationalID facilitates easier and more reliable identity matching between institutions, streamlining administrative processes.

Students use these credentials to apply for courses at any alliance university. Host institutions verify student identities and qualifications quickly. Upon course completion, students receive verifiable credentials directly to their wallet, which they can easily share with their home institution.

Benefits

The implementation of digital credentials in university alliances delivers benefits across three key areas:

1. Enhanced Student Mobility & Experience
   - Seamless cross-border study through simplified application and enrollment
   - Automatic recognition of credits and qualifications across alliance institutions
   - Improved access to diverse educational opportunities across Europe
2. Institutional Excellence
   - Streamlined administrative processes through automated verification
   - Enhanced collaboration through shared resources and joint programs
   - Better data-driven decision making for strategic planning
3. Quality & Innovation
   - Consistent quality assurance across alliance institutions
   - Support for innovative learning models and digital education
   - Improved tracking and validation of student achievements

Challenges

- Ensuring interoperability between different university systems: Universities within alliances often use varied IT systems and databases. Creating a unified system that can communicate seamlessly across these diverse platforms is a significant technical challenge. This interoperability is crucial for the smooth exchange of student data and credentials across institutions.
- Adapting existing processes to accommodate new digital credentials: Universities have established procedures for admissions, credit transfer, and credential verification. Integrating the new digital credential system into these existing processes requires careful planning and may necessitate changes to administrative workflows and staff training.
- Addressing data protection and privacy concerns: The handling of student data across multiple institutions and potentially across borders raises important privacy issues. Ensuring compliance with data protection regulations, such as GDPR, while maintaining the utility of the system is a complex balancing act.
- Gaining buy-in from all stakeholders, including ministries of education: The success of this system depends on widespread adoption. Convincing all parties -

universities, students, and governmental bodies - of the benefits and addressing their concerns is crucial. This may involve navigating different national regulations and education system structures.

- Managing the transition from current systems to the new framework: Implementing a new system while maintaining existing operations can be challenging. Universities need to plan for a transition period where both old and new systems might need to coexist, ensuring that no students are disadvantaged during the change.

Technical Requirements

- Verifiable credentials infrastructure: This forms the backbone of the system, allowing for the creation, issuance, and verification of digital academic credentials. The infrastructure must be robust, secure, and scalable to handle the volume of credentials across alliance institutions.
- Digital wallets for students: These wallets allow students to store and manage their digital credentials securely. The wallet interface should be user-friendly, enabling students to easily share their credentials with relevant parties while maintaining control over their personal data.
- Secure authentication mechanisms: Strong authentication processes are necessary to ensure that only authorised individuals can access and modify credential information. This might involve multi-factor authentication or other advanced security measures.
- Standardised data models for academic credentials: Common data standards that incorporate and expand upon existing models used in MyAcademicID and ESI, ensure that credentials issued by different institutions can be uniformly understood and processed across the alliance. This standardisation is key to enabling seamless student mobility and credit recognition.
- Implementation of W3C Verifiable Credentials and European Learning Model standards for credential issuance and verification
    - Support for selective disclosure capabilities as defined in the W3C Verifiable Credentials Data Model
    - Integration with EDCI for standardized credential templates and formats
- Integration with existing university management systems: The new credential system must work alongside current student information systems, learning management systems, and other university software. This integration is crucial for the practical implementation of the new framework.
- information, schemas, and other metadata associated with the use case. It provides a secure, tamper-proof record of the credential ecosystem without storing personal data on-chain. The actual credentials are issued directly from the issuer to the student's wallet.
- Compliance with data protection regulations: The system must be designed with privacy in mind, incorporating features like data minimisation, user consent mechanisms, and secure data storage and transmission methods to meet legal requirements such as those set out in GDPR.

- The trust infrastructure must provide: distributed verification capabilities, redundant record keeping, independent verification pathways, protection against single points of failure. This technology stores the governance and key elements of the trust framework

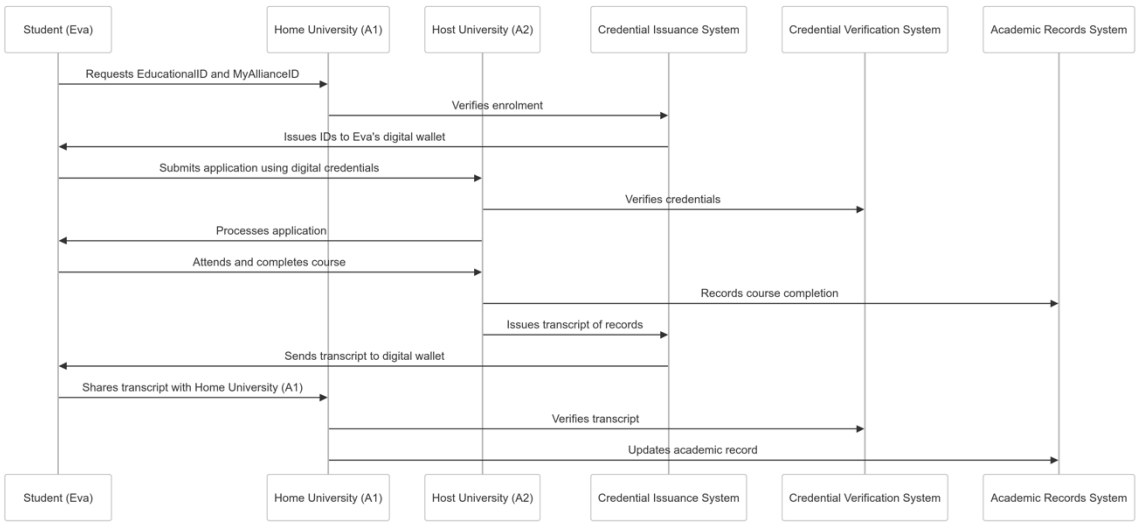
User Journey

1. Student obtains verifiable credentials
2. Student applies for a course at an alliance university
3. Student completes the course
4. Student receives a verifiable credential for course completion
5. Student shares credentials with home university

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Student obtains verifiable credentials | Student (Eva) | Requests EducationalID and MyAllianceID | Home University (Rovira i Virgili) issues credentials directly to Eva's EUDI wallet |
| | Home University (Rovira i Virgili) | Verifies Eva's enrolment status | University Student Information System |
| | Home University (Rovira i Virgili) | Issues EducationalID and MyAllianceID | Credential Issuance System |
| 2. Student applies for a course at an alliance university | Student (Eva) | Selects course at University Duisburg-Essen | Alliance Portal |
| | Student (Eva) | Submits application using digital credentials | Eva's Digital Wallet |
| | Host University (Duisburg-Essen) | Verifies Eva's credentials | Credential Verification System |
| | Host University (Duisburg-Essen) | Processes application | University Admissions System |
| 3. Student completes the course | Student (Eva) | Attends and completes course | Learning Management System at University Duisburg-Essen |
| | Host University | Records course completion | University Academic Records System |

| | | | |
|---|---|---|---|
| | (Duisburg-Essen) | | |
| 4. Student receives a verifiable credential for course completion | Host University (Duisburg-Essen)<br><br>Student (Eva) | Issues verifiable Transcript of Records<br><br>Receives credential in EUDI wallet | Credential Issuance System<br><br>Eva's Digital Wallet |
| 5. Student shares credentials with home university | Student (Eva)<br>Home University (Rovira i Virgili)<br>Home University (Rovira i Virgili) | Selects and shares new credential<br>Verifies received credential<br>Updates Eva's academic record | Eva's Digital Wallet<br>Credential Verification System<br>University Academic Records System |




This user journey demonstrates how verifiable credentials and digital identities can simplify studying across alliance institutions, reducing administrative burden and enhancing the student experience.

## 7.7.2 Learning achievements

### *7.7.2.1 Formal accreditation*

Context

European universities aim to simplify the application process for students who hold degrees from one country and wish to pursue further education in another. This aligns with the broader goals of enhancing student mobility and promoting cross-border education within Europe.

The story

Anna's fingers hovered over her keyboard as she took a deep breath. She had just completed her bachelor's degree at the University of Athens, and now, sitting in her small flat in Greece, she was about to take the first step towards her dream of pursuing a master's degree in Switzerland. The prospect was both thrilling and intimidating.
She navigated to the eDiplomas platform, a digital gateway to her academic achievements. As the login page appeared, Anna reached for her phone and opened her national ID app. With a quick scan of the QR code on her screen, she was authenticated and granted access to the platform.

The interface was clean and intuitive. Anna saw a list of her academic credentials, each represented by a small digital icon. She carefully selected her bachelor's degree and transcript of records, the digital keys she needed to unlock her future studies.
As she confirmed her selection, Anna's phone buzzed. She picked it up to find a notification from her EUDI wallet app, requesting permission to receive new credentials. With a swipe and a tap, she accepted, and watched as her bachelor's degree and transcript materialised as secure, verifiable digital documents in her wallet.
Anna couldn't help but smile, remembering the stories her older sister had told her about applying for international studies just a few years ago - the stacks of papers, the costly translations, the anxiety of sending original documents through the post. How times had changed.

With her credentials safely stored, Anna turned her attention to the University of Lausanne's website. She navigated to the application page for the master's programme she had been eyeing for months. As she began to fill out the form, she came to a section requesting her academic qualifications.

Instead of the dreaded "upload documents" button, Anna was pleasantly surprised to see an option to share digital credentials. She clicked it, which prompted her EUDI wallet app to open. With a few taps, she selected her bachelor's degree and transcript, then authorised their sharing with the University of Lausanne.

In the background, unseen by Anna, a complex dance of digital verification was taking place. The University of Lausanne's systems were communicating with the underlaying

trust framework, verifying the authenticity of Anna's credentials, checking that they were issued by an accredited institution, and had not been tampered with or revoked.

Within moments, Anna's screen updated, showing that her credentials had been successfully received and verified. She couldn't help but let out a small cheer, drawing a curious look from her cat lounging nearby.

Encouraged by the smooth process, Anna completed the rest of the application form with renewed confidence. She carefully reviewed her personal statement one last time, then, with a mix of excitement and nervousness, clicked the submit button.

Almost immediately, a confirmation appeared on her screen. The University of Lausanne had received her application, complete with her verified digital credentials. Anna sat back in her chair, a sense of accomplishment washing over her. The first step of her international academic journey was complete, and it had been far easier than she had ever imagined.

Over the next few weeks, as Anna waited for a response from the university, she marvelled at how technology had transformed the application process. She thought about the broader implications - how this system could open doors for students across Europe, making cross-border education more accessible than ever before.

When the day finally came, and Anna received an email from the University of Lausanne, her heart raced as she opened it. The message congratulated her on her acceptance to the master's programme, citing her strong academic credentials - the very same digital credentials she had so easily shared.

As Anna celebrated her acceptance, she reflected on the journey that had brought her to this point. From the moment she logged into the eDiplomas platform to the instant she received her acceptance, the process had been streamlined, secure, and surprisingly stress-free.

This experience was more than just a personal victory for Anna. It represented a new era in European higher education - one where borders were becoming less of a barrier, where academic achievements could be securely shared and verified in an instant, and where students like her could pursue their dreams with greater ease than ever before.

As she began to plan her move to Switzerland, Anna felt a profound sense of gratitude for the invisible digital infrastructure that had made this possible. The formal accreditation system, with its verifiable credentials and cross-border trust framework, had not just simplified an application process - it had opened up a world of opportunities.

Anna's journey from Athens to Lausanne was just beginning, but thanks to the power of digital credentials and the vision of a more connected European education system, that journey had started on the right foot. As she looked to the future, Anna couldn't help but

feel excited about the possibilities that lay ahead, not just for her, but for students across Europe who would follow in her digital footsteps.

Actors

- Students (graduates holding a bachelor's degree)
- Issuer universities (e.g., University of Athens)
- Verifier universities (e.g., University of Lausanne)
- Greek Universities Network (GUNet) - eDiplomas platform
- Greek Ministry of Education (Root TAO)
- Swiss Accreditation Council (Root TAO)

Current Process ("As-Is")

Students applying to universities in other countries must provide various documents, including diplomas and transcripts. These often need to be translated, notarised, and manually verified by the receiving institution. This process is time-consuming, prone to errors, and can be a barrier to cross-border education.

Future Process ("To-Be")

Students receive verifiable credentials for their bachelor's degree and transcript directly from their alma mater. They can then use these digital credentials to apply to master's programmes at universities in other European countries. The receiving universities can quickly and reliably verify these credentials, streamlining the application process.

Benefits

The formal accreditation process delivers three key benefit areas:

1. Enhanced trust & recognition
   - Secure, tamper-proof verification of academic credentials
   - Clear qualification status and standards across borders
   - Reliable authentication of issuing institutions
2. Streamlined operations
   - Automated verification reducing processing time and costs
   - Simplified enrollment and credit transfer processes
   - Efficient resource allocation through digital workflows
3. Educational opportunity & career growth
   - Improved access to international study opportunities
   - Better alignment between qualifications and market needs
   - Enhanced career mobility through trusted credentials

Challenges

- Establishing a trusted accreditation chain: The system relies on a network of trust between different national education authorities, accreditation bodies, and universities. Establishing and maintaining this trust framework across borders can be complex.

Co-funded by the European Union

- Ensuring interoperability: Different countries and institutions may use varying systems and standards. Ensuring that all these systems can communicate and interpret credentials consistently is a significant technical challenge.
- Data protection and privacy: Handling sensitive educational data across borders raises important privacy concerns. The system must comply with regulations like GDPR while maintaining functionality.
- Adoption and change management: Universities and national authorities need to adapt their processes to incorporate the new digital credential system. This requires investment in technology, training, and potentially changes to regulations.
- Maintaining credential validity: There needs to be a system for updating or revoking credentials if necessary, ensuring that the information remains current and accurate over time.

Technical Requirements

- Verifiable credentials infrastructure: A robust system for creating, issuing, and verifying digital academic credentials that can be trusted across borders.
- Digital wallets for students: Secure and user-friendly applications that allow students to store and manage their digital credentials.
- Standardised data models: Common formats for representing academic qualifications that can be understood by systems in different countries.
- Trusted ledger or distributed ledger technology: To store the trust framework and credential metadata, ensuring a tamper-proof record of the credential ecosystem.
- Integration with existing university systems: The new credential system must work alongside current student information systems and admissions platforms.
- Strong authentication mechanisms: To ensure that only authorised parties can issue or verify credentials.
- Compliance with data protection regulations: The system must incorporate privacy-by-design principles and comply with GDPR and other relevant regulations.

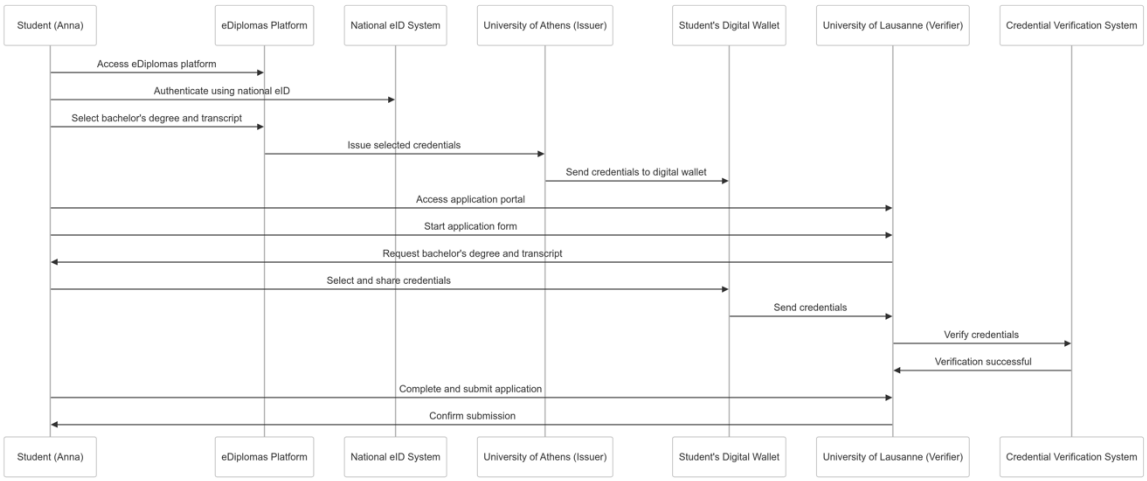
User Journey

1. Obtaining credentials:
    a. Anna, a graduate from the University of Athens, logs into the eDiplomas platform.
    b. She authenticates using her national verifiable ID.
    c. Anna selects her bachelor's degree and transcript of records from the available credentials.
    d. The credentials are issued directly to Anna's EUDI wallet.
2. Applying for a master's degree:
    a. Anna visits the University of Lausanne website to apply for a master's programme.
    b. She fills in the application form, which requests her bachelor's degree and transcript

c. Anna uses her EUDI wallet to share the requested verifiable credentials.
d. The University of Lausanne's system automatically verifies the credentials.
e. Anna completes the rest of the application and submits it.
f. She receives confirmation that her application, including verified credentials, has been successfully submitted.

This user journey demonstrates how verifiable credentials can simplify the process of applying for further education across borders, reducing administrative burdens and enhancing trust in the submitted qualifications.

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Obtaining credentials | | | |
| 1a. Access eDiplomas platform | Anna (Student) | Visits the eDiplomas platform | eDiplomas web interface |
| 1b. Authenticate | Anna (Student) | Logs in using national eID means | National eID authentication system |
| 1c. Select credentials | Anna (Student) | Chooses bachelor's degree and transcript of records | eDiplomas credential selection interface |
| 1d. Issue credentials | University of Athens (Issuer) | Issues selected credentials | Credential Issuance System |
| 1e. Receive credentials | Anna (Student) | Receives credentials in EUDI wallet | Student's Digital Wallet |
| 2. Applying for a master's degree | | | |
| 2a. Access application portal | Anna (Student) | Visits University of Lausanne website | University of Lausanne web interface |
| 2b. Start application | Anna (Student) | Begins filling in the application form | University of Lausanne application system |
| 2c. Request credentials | University of Lausanne (Verifier) | Prompts for bachelor's degree and transcript | Application form interface |
| 2d. Share credentials | Anna (Student) | Selects and shares requested credentials | Student's Digital Wallet |
| 2e. Verify credentials | University of Lausanne (Verifier) | Automatically verifies shared credentials | Credential Verification System |
| 2f. Complete application | Anna (Student) | Fills in remaining application details | University of Lausanne application system |
| 2g. Submit application | Anna (Student) | Submits completed application | University of Lausanne application system |
| 2h. Confirm submission | University of Lausanne (Verifier) | Sends confirmation of successful submission | University of Lausanne notification system |




This detailed user journey illustrates the step-by-step process of obtaining and using verifiable credentials for cross-border university applications. It shows the interactions between the student (Anna), the issuing university (University of Athens), and the verifying university (University of Lausanne), as well as the various systems involved in the process. This journey demonstrates how verifiable credentials can simplify and streamline the application process for international higher education programmes.

## 7.7.3 Professional qualifications

### *7.7.3.1 Issuance of an electronic Certificate of Professional Suitability (eCIP) for collegiate doctors*

Context

European regulations aim to digitise the process of issuing and verifying professional qualifications. This use case concerns the issuance of an electronic Certificate of Professional Suitability (eCIP) to collegiate doctors, streamlining the process of obtaining and sharing professional credentials across borders within Europe. The eCIP confirms that a doctor is qualified and eligible to practice.

Actors

- Collegiate doctor (Anna): A doctor who is a member of a professional body, seeking the issuance of an eCIP.
- COM (Doctors' Official College): The professional body the doctor belongs to, responsible for processing the application.
- CGCOM (General Council of Official Medical Colleges): The Trusted Issuer responsible for issuing the eCIP.
- CGCOM Central Registry: The authentic source of information regarding the doctor's credentials.
- EUDI Wallet: A EUDI wallet that the doctor uses to receive and store their eCIP.

Current process ("As-Is")

Doctors currently request a Certificate of Professional Suitability through a manual process involving physical paperwork or email communication. The Doctors' Official

College (COM) processes the request, verifies the doctor's credentials, and issues the certificate. This process can be time-consuming and requires manual intervention for each step, with limited integration between systems for verification and issuance.

Future process ("To-Be")

The new digital process transforms how collegiate doctors obtain their eCIP. Doctors now request their certificate through a secure online platform provided by their local COM. The system automatically verifies the doctor's collegiate status and professional standing by querying the CGCOM Central Registry. Once verified, CGCOM issues the eCIP directly to the doctor's EUDI Wallet. This digital certificate is cryptographically signed, ensuring its authenticity and integrity. Doctors can then easily share their eCIP with employers or regulatory bodies as needed, who can instantly verify its validity through the CGCOM platform. This streamlined process significantly reduces administrative burden and enhances the security and portability of professional credentials.

Benefits

Streamlined certificate issuance: The new system allows collegiate doctors to Professional qualification management delivers benefits across three strategic areas:

1. Enhanced Professional Mobility & Recognition
    - Seamless cross-border qualification recognition through standardized digital credentials
    - Instant verification of professional standing and competencies
    - Simplified registration and licensing across EU member states
2. Operational Excellence
    - Significant reduction in administrative costs and processing time through automation
    - Enhanced fraud prevention through secure digital verification
    - Improved resource allocation with streamlined workflows
3. Career Development & Quality Assurance
    - Clear pathways for professional development and skill advancement
    - Better tracking and validation of continuing education
    - Strengthened public protection through improved oversight

Challenges

- System integration complexity: Integrating the new eCIP system with existing databases and IT infrastructure of various medical colleges and regulatory bodies may prove technically challenging.
- User adoption: Some doctors, particularly those less comfortable with digital technologies, might resist adopting the new system, necessitating comprehensive training and support.
- Data privacy concerns: Handling sensitive professional information digitally raises data protection issues that must be carefully addressed to comply with GDPR and maintain public trust.

- Cross-border standardisation: Ensuring that the eCIP is recognised and accepted uniformly across different EU countries may require extensive coordination and potential legal adjustments.

Technical requirements

- Secure EUDI wallet: The EUDI Wallet must provide robust security features to protect sensitive professional credentials.
- Interoperable systems: The CGCOM platform needs to interface seamlessly with various medical colleges' systems and the EUDI Wallet.
- The trust infrastructure that must provide distributed verification capabilities, redundant record keeping, independent verification pathways, protection against single points of failure; to ensure the immutability and traceability of credential issuance and verification.
- Strong authentication mechanisms: Multi-factor authentication for doctors accessing the system to request or share their eCIP.
- API development: Creation of secure APIs to enable communication between different components of the system.

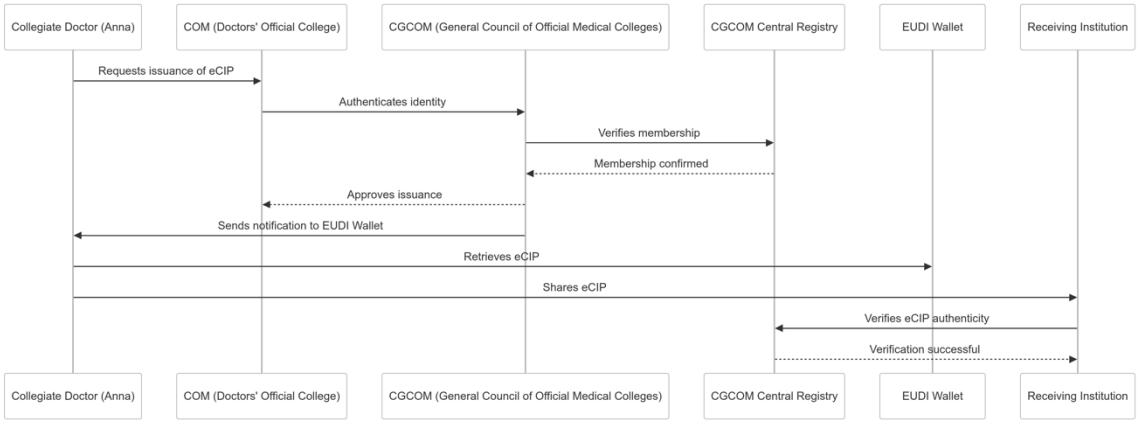
User journey

1. Collegiate doctor requests eCIP through COM
2. CGCOM verifies doctor's credentials
3. CGCOM issues eCIP
4. Doctor receives eCIP in EUDI Wallet
5. Doctor shares eCIP with relevant organisations

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Request eCIP | Anna (Collegiate doctor) | Accesses COM's platform and submits eCIP request | COM digital platform; Doctor selects eCIP request option and provides identification |
| | COM administrative staff | Receive request and authenticate on CGCOM platform | COM staff access CGCOM platform and authenticate |
| 2. Verify credentials | CGCOM | Verifies Anna's credentials | CGCOM platform queries Central Registry to check registration and disqualifications |
| 3. Issue eCIP | CGCOM | Approves request and issues eCIP | CGCOM administrative platform generates and stores eCIP |
| | CGCOM administrative staff | Confirm details and trigger eCIP release | Staff access issuance system, review details, and release eCIP |

| | | | |
|---|---|---|---|
| 4. Provide eCIP | CGCOM<br>Anna (Collegiate doctor) | Notifies Anna that eCIP is ready<br>Receives notification and retrieves eCIP | CGCOM system sends notification to Anna's EUDI Wallet<br>EUDI Wallet app; Doctor authenticates and receives eCIP |
| 5. Share eCIP | Anna (Collegiate doctor)<br>Receiving institution (e.g., foreign regulatory body) | Shares eCIP when required<br>Receives and verifies eCIP | EUDI Wallet app; Doctor selects and sends eCIP<br>Institution's system verifies eCIP through CGCOM Central Registry |




This user journey demonstrates the step-by-step process of obtaining and using an eCIP for a collegiate doctor, from the initial request to sharing with relevant organisations. It shows the interactions between the collegiate doctor (Anna), the COM (Colegio Oficial de Médicos), CGCOM (Consejo General de Colegios Oficiales de Médicos), and the verifying organisations, as well as the various systems involved in the process.

#### *7.7.3.2 Issuance of an electronic Certificate of Professional Suitability (eCIP) for non-collegiate doctors*

Context

For non-collegiate doctors, the process of obtaining a Certificate of Professional Suitability (eCIP) has traditionally been burdensome, involving multiple steps, physical paperwork, and verification processes that took significant time and effort. In this evolving digital landscape, the issuance of an eCIP is streamlined, reducing the administrative load and allowing doctors who are not members of a professional body to prove their qualifications electronically. This digitised process, integrated with the European Digital Identity (EUDI) Wallet, ensures efficiency and security.

The Story

Dr. James, a recently graduated medical professional, stands at the cusp of new opportunities. Although not a member of a professional body, he needs a Certificate of Professional Suitability (eCIP) to present to a prospective employer in a foreign country.

The days of paperwork and notarised copies are behind him, replaced by a digital process that promises efficiency and security.

With a few clicks, Dr. James accesses the CGCOM platform from the comfort of his home. The interface is straightforward and guides him through the necessary steps. He submits his request for an eCIP, and the system immediately verifies his identity using his EUDI Wallet. In the background, a series of checks begin.

First, the system queries the Spanish Official Degree Data Verification Service, retrieving confirmation of his academic qualifications. Dr. James remembers the long wait he once experienced when applying for his degree certificate, but now the system does it all instantly. The response is clear—his degree is valid, and there are no issues.
Next, the platform automatically reaches out to the Spanish Consultation Service for Criminal Records. Dr. James is confident, knowing that his background is clear. Within moments, the platform confirms that there are no criminal records tied to his name that would impede the issuance of his certificate.

The final step comes quickly. The CGCOM system generates Dr. James' electronic Certificate of Professional Suitability. He receives a notification on his phone, and, opening his EUDI Wallet, he sees the certificate waiting for him—no long queues, no emails back and forth. It's all there, secure and ready.

Dr. James feels relieved. A few weeks later, the foreign medical institution requests his professional credentials. With a few taps on his phone, he selects his eCIP from the EUDI Wallet and shares it with the institution. The institution, thousands of miles away, verifies the certificate instantly, querying the CGCOM Central Registry to confirm its validity. Within minutes, the institution acknowledges receipt and confirms that Dr. James' qualifications are in order. His path forward is clear, and the process that once felt burdensome is now a seamless part of his professional life.

Actors

- Non-collegiate doctor (Dr. James): A medical doctor not affiliated with a specific professional body but seeking a Certificate of Professional Suitability to prove his qualifications.
- CGCOM (General Council of Official Medical Colleges): The Trusted Issuer responsible for issuing the eCIP.
- Spanish Official Degree Data Verification Service: Responsible for verifying Dr. James' academic qualifications.
- Spanish Consultation Service for Criminal Records: Ensures there are no disqualifying criminal records.
- EUDI Wallet: Used by Dr. James to receive and store his eCIP.

Current process ("As-Is")

Non-collegiate doctors, such as those recently graduated or not associated with a specific professional body, face a cumbersome process when obtaining a Certificate of Professional Suitability. They are required to submit physical documents, which must be

authenticated manually, including degree certificates and criminal record clearances. The issuing body, CGCOM, must then manually check with various government databases to validate the information, which adds delays to the process.

Future process ("To-Be")

The digitised eCIP issuance process for non-collegiate doctors leverages advanced technology to ensure efficiency and security. Doctors initiate their eCIP request through the CGCOM online platform, authenticating themselves using their EUDI Wallet. The system then automatically verifies the doctor's qualifications by querying the Spanish Official Degree Data Verification Service and checks for any disqualifying records through the Spanish Consultation Service for Criminal Records.

Upon successful verification, CGCOM generates a digitally signed eCIP and sends it directly to the doctor's EUDI Wallet. This digital credential can be easily shared with and verified by potential employers or regulatory bodies across Europe, facilitating professional mobility while maintaining the highest standards of credential integrity.

Benefits

- Accelerated credential verification: The automated checks with official services significantly reduce the time required to verify a non-collegiate doctor's qualifications and background.
- Improved accessibility: Non-collegiate doctors can easily request and receive their eCIP remotely, without the need to visit physical offices or send documents by post.
- Enhanced data accuracy: Automated verification reduces the risk of human error in the credential checking process, ensuring more reliable eCIP issuance.
- Facilitated professional mobility: The digital eCIP stored in the EUDI Wallet can be easily shared and verified across borders, supporting non-collegiate doctors in pursuing international opportunities.
- Reduced administrative burden: The CGCOM and other relevant bodies can process eCIP requests more efficiently, freeing up resources for other essential tasks.

Challenges

- Complex system integration: Connecting various official verification services (e.g., degree verification, criminal records) with the CGCOM platform and EUDI Wallet requires sophisticated technical integration.
- Varied regulatory landscapes: Accommodating different regulatory requirements for non-collegiate doctors across EU member states within a single system may be challenging.
- Identity verification: Ensuring robust identity verification for non-collegiate doctors who may not have established relationships with professional bodies.
- System reliability: The system must be highly reliable, as any downtime could significantly impact doctors' ability to prove their professional suitability.

Technical requirements

- Real-time verification interfaces: Development of APIs to connect with various official verification services for instant credential checking.

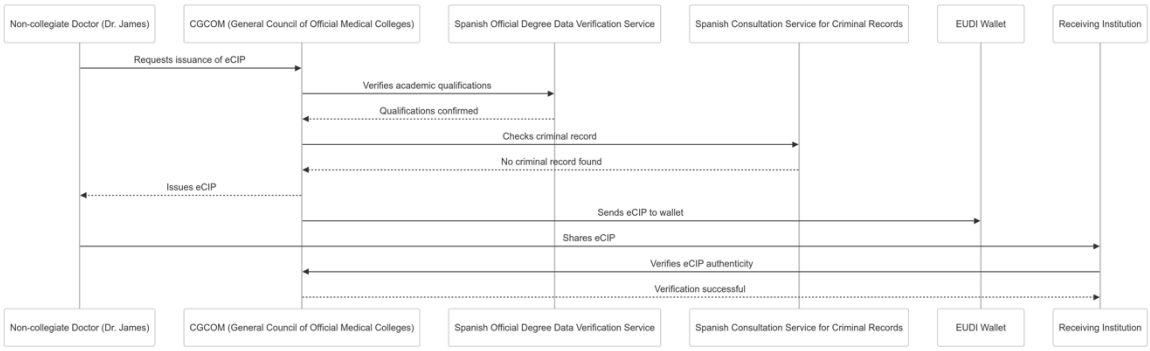
- Scalable infrastructure: The system must be able to handle a large number of concurrent requests from non-collegiate doctors across Europe.
- Data encryption: Implementation of strong encryption for all data transmission and storage to protect sensitive personal and professional information.
- Audit trail functionality: A system to log all credential verifications and eCIP issuances for accountability and troubleshooting purposes.
- Multi-lingual support: The platform should support multiple languages to cater to non-collegiate doctors across different EU countries.

User journey

1. Training provider submits accreditation request
2. SEAFORMEC verifies provider's credentials
3. SEAFORMEC and UEMS assign assessors
4. Assessors evaluate training activity
5. SEAFORMEC issues accreditation certificate
6. Training provider receives certificate in EUDI Wallet
7. Training provider shares certificate with relevant bodies

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Submit accreditation request | MedEduCo (Training provider) | Accesses SEAFORMEC platform and submits accreditation request | SEAFORMEC platform; Provider fills digital form with training details |
| 2. Verify credentials | SEAFORMEC | Verifies MedEduCo's credentials | Trust infrastructure Registry; System checks provider's registration and authorisation |
| 3. Assign assessors | SEAFORMEC, UEMS | Assigns two assessors to evaluate training materials | SEAFORMEC system assigns assessors from SEAFORMEC and UEMS |
| 4. Evaluate training activity | Assessors | Review content, quality, and pedagogical value of training activity | Assessors use evaluation system to review and approve or request revisions |
| 5. Issue accreditation | SEAFORMEC | Generates accreditation certificate after assessors' approval | SEAFORMEC platform generates and digitally signs certificate |
| 6. Provide accreditation certificate | SEAFORMEC | Sends accreditation certificate to MedEduCo's EUDI Wallet | SEAFORMEC system transfers certificate to provider's EUDI wallet |
| 7. Share accreditation certificate | MedEduCo (Training provider) | Shares accreditation certificate with relevant bodies | EUDI Wallet app; Provider selects and sends certificate |
| | Relevant body/institution | Receives and verifies certificate | Institution's system verifies certificate through SEAFORMEC platform |




This user journey demonstrates the step-by-step process of obtaining and using a SEAFORMEC accreditation certificate, from submitting the initial request to sharing the certificate with relevant organisations. It shows the interactions between the training provider (MedEduCo), SEAFORMEC, UEMS, assessors, and the verifying organisations, as well as the various systems involved in the process

#### *7.7.3.3 Accreditation of Continuous Professional Development/Further Medical Competence training activities via SEAFORMEC*

Context

Continuous Professional Development (CPD) and Further Medical Competence (FMC) training activities are essential for health professionals to maintain and enhance their skills. The accreditation of these activities is handled by SEAFORMEC, which ensures that the training meets the required standards. The process of accrediting a CPD/FMC training activity has been digitised to streamline submissions, evaluations, and accreditation issuance. This use case involves a training provider requesting accreditation for a training activity through SEAFORMEC, which ensures that the activity meets the necessary criteria.

The Story

MedEduCo, a company that has long been involved in the training and development of healthcare professionals, is preparing to launch a new CPD training programme. With a focus on the latest advancements in medical education, the company knows that accreditation from SEAFORMEC will lend credibility and ensure that the programme is recognised internationally.

Sitting in her office, the programme director at MedEduCo opens the SEAFORMEC platform. The process is straightforward. She enters all the necessary details about the programme—the course structure, the instructors' credentials, the sources of funding, and the planned outcomes for attendees. Once completed, she clicks the submit button, and the system immediately starts working.

In the background, SEAFORMEC's platform checks MedEduCo's credentials against the Trust infrastructure Registry. MedEduCo is already registered, and the system confirms that they are authorised to provide accredited training. The request moves forward.

Soon after, SEAFORMEC assigns two assessors to review the application. The assessors, experts in medical education, meticulously evaluate the programme's content. They agree that the programme meets the high standards required for accreditation. The process moves forward swiftly, without the delays and manual steps that once plagued the accreditation system.

MedEduCo's programme is approved, and a notification pings in the programme director's EUDI Wallet. She opens the wallet and sees the newly issued accreditation certificate. Everything is in place. The certificate is now stored securely in her EUDI wallet, and she can share it with anyone who needs proof of the programme's accreditation.

Not long after, MedEduCo is approached by a large medical institution looking to collaborate on the new CPD programme. The institution requests proof of accreditation. With a few taps, the director selects the certificate from her EUDI Wallet and sends it over. The institution verifies the certificate's authenticity through SEAFORMEC's platform, confirming that everything is in order. MedEduCo's CPD programme is ready to launch, recognised and accredited across the healthcare field.

Actors

- Training provider (MedEduCo): A company or organisation that offers CPD/FMC training and seeks accreditation for its activities.
- SEAFORMEC: The body responsible for accrediting the training activities.
- UEMS: An international accreditation body that collaborates with SEAFORMEC.
- Assessors: Experts who evaluate the training activity's content and quality.
- EUDI Wallet: Used by the training provider to store and share the accreditation certificate.
- Trust infrastructure list(s): A list used to verify the training provider's credentials.

Current process ("As-Is")

Training providers currently apply for accreditation of their CPD/FMC activities through a manual process. This involves submitting detailed descriptions of the activities, including pedagogical content, funding sources, and instructor qualifications. The process can be slow, requiring manual evaluation by assessors and multiple interactions between the provider and SEAFORMEC. Once the activity is accredited, the training provider receives a certificate, typically in a physical format, to confirm accreditation.

Future process ("To-Be")

The new digital accreditation process revolutionises how CPD/FMC training activities are evaluated and certified. Training providers submit their accreditation requests through a dedicated SEAFORMEC online platform.

The system automatically verifies the provider's credentials against the Trust infrastructure Registry. SEAFORMEC and UEMS then assign assessors through the platform, who can access all necessary materials digitally. The assessment process is

conducted entirely online, with assessors providing feedback and evaluations through the system.

Once approved, SEAFORMEC issues a digital accreditation certificate, which is sent directly to the training provider's EUDI Wallet. This digital certificate can be easily shared with and verified by relevant bodies, streamlining the process of recognising accredited training activities across Europe.

Benefits

1. Quality & Trust
   - Standardized assessment ensuring consistent quality
   - Enhanced credential integrity through secure digital verification
   - Transparent evaluation processes
2. Operational Efficiency
   - Streamlined accreditation workflow
   - Simplified certificate sharing and verification
   - Efficient handling of complex applications
3. Compliance & Security
   - Strong privacy protection controls
   - Interoperability with existing systems
   - Maintained compliance with professional standards

Challenges

- Assessor adaptation: SEAFORMEC and UEMS assessors may need to adapt to new digital evaluation tools and processes, which could require significant training and change management.
- Technical interoperability: Ensuring seamless integration between the SEAFORMEC platform, UEMS systems, and the EUDI Wallet across different countries and institutions.
- Maintaining assessment quality: The digital system must be designed to support, not replace, the expert judgement of assessors in evaluating training activities.
- Handling complex applications: The system needs to accommodate a wide range of CPD/FMC activities, some of which may not fit easily into standardised digital forms.

Technical requirements

- Collaborative assessment platform: A secure online environment where SEAFORMEC and UEMS assessors can review applications and provide feedback.
- Document management system: A robust system to handle the upload, storage, and retrieval of training materials and supporting documents.
- Workflow automation: Implementation of automated workflows to guide applications through the various stages of the accreditation process.
- Integration with Trust infrastructure Registry: Secure connection to the Trust infrastructure Registry for verification of training provider credentials and recording of accreditation decisions.

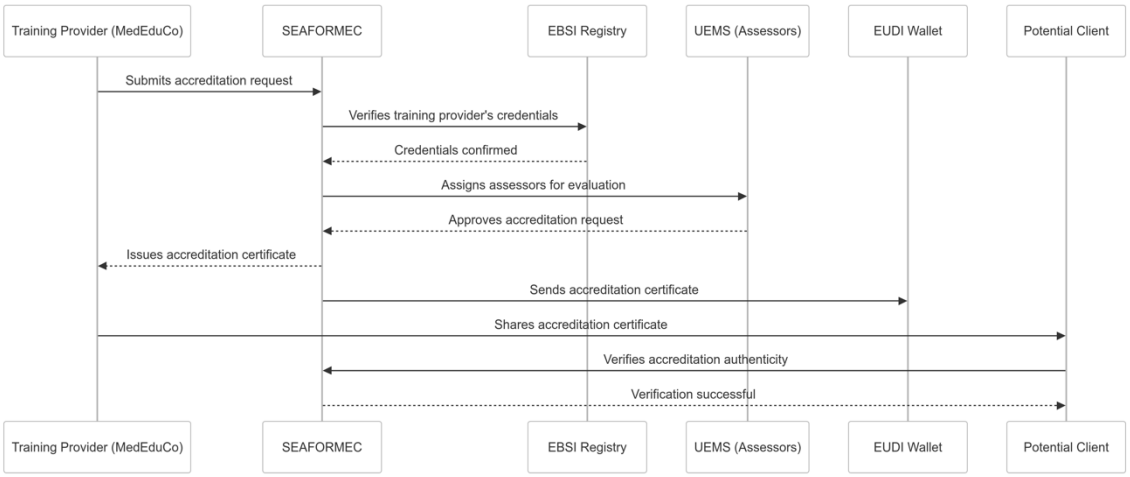
- Digital certificate generation: Capability to create and issue tamper-proof digital accreditation certificates.

User journey

1. Training provider submits accreditation request
2. SEAFORMEC verifies provider's credentials
3. SEAFORMEC and UEMS assign assessors
4. Assessors evaluate training activity
5. SEAFORMEC issues accreditation certificate
6. Training provider receives certificate in EUDI Wallet
7. Training provider shares certificate with relevant bodies

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Submit accreditation request | MedEduCo (Training provider) | Accesses SEAFORMEC platform and submits accreditation request | SEAFORMEC platform; Provider fills digital form with training details |
| 2. Verify credentials | SEAFORMEC | Verifies MedEduCo's credentials | Trust infrastructure Registry; System checks provider's registration and authorisation |
| 3. Assign assessors | SEAFORMEC, UEMS | Assigns two assessors to evaluate training materials | SEAFORMEC system assigns assessors from SEAFORMEC and UEMS |
| 4. Evaluate training activity | Assessors | Review content, quality, and pedagogical value of training activity | Assessors use evaluation system to review and approve or request revisions |
| 5. Issue accreditation | SEAFORMEC | Generates accreditation certificate after assessors' approval | SEAFORMEC platform generates and digitally signs certificate |
| 6. Provide accreditation certificate | SEAFORMEC | Sends accreditation certificate to MedEduCo's EUDI Wallet | SEAFORMEC system transfers certificate to provider's EUDI wallet |
| 7. Share accreditation certificate | MedEduCo (Training provider) | Shares accreditation certificate with relevant bodies | EUDI Wallet app; Provider selects and sends certificate |
| | Relevant body/institution | Receives and verifies certificate | Institution's system verifies certificate through SEAFORMEC platform |




This user journey demonstrates the step-by-step process of obtaining and using a SEAFORMEC accreditation certificate, from submitting the initial request to sharing the certificate with relevant organisations. It shows the interactions between the training provider (MedEduCo), SEAFORMEC, UEMS, assessors, and the verifying organisations, as well as the various systems involved in the process.

#### *7.7.3.4 Issuance of Basic Quality Management training certificates*

Context

The **BQM certificate** is issued to certify that a healthcare professional has successfully completed a SEAFORMEC-accredited training session. This certificate allows healthcare professionals to prove their continuous education efforts, which are critical for maintaining and updating their qualifications. The digitisation of the issuance process for BQM certificates allows professionals to request, receive, and share their certificates easily through the **EUDI Wallet**. This use case outlines how a healthcare professional requests and receives a BQM certificate after completing a training session.

The Story

Dr. Sofia, a diligent healthcare professional, has been working tirelessly to stay up-to-date with the latest developments in her field. She has just enrolled in a SEAFORMEC-accredited training session hosted by the Foundation, aimed at enhancing her knowledge of new medical technologies. Sitting at her desk, she logs into the Foundation's Virtual Campus, reviews the available training options, and registers for the one that best fits her needs.

Over the next few weeks, Dr. Sofia dedicates time to completing the training. The sessions are engaging, and she finishes with a sense of accomplishment, knowing she has expanded her expertise. After completing the final assessment, Dr. Sofia is ready to request her **BQM certificate**, a document that will validate her newly acquired skills and serve as proof of her ongoing professional development.

In the past, this process would have involved manual paperwork, delays, and follow-up emails. But now, it's as simple as a few clicks. From the Virtual Campus, Dr. Sofia

submits her request for the BQM certificate. The system verifies her completion of the training and sends the request to **CGCOM**, the body responsible for issuing the certificate.

Within minutes, CGCOM processes the request, generates a digitally signed certificate, and sends it directly to Dr. Sofia's **EUDI Wallet**. A notification appears on her phone, confirming that her certificate is ready. Dr. Sofia opens the wallet and sees the BQM certificate securely stored. She feels relieved, knowing that she can easily share this certificate with future employers or regulatory bodies whenever necessary.
A few weeks later, Dr. Sofia applies for a new professional position that requires proof of continuous education. With confidence, she selects her BQM certificate from the EUDI Wallet and shares it with the medical institution. The institution verifies the certificate instantly through CGCOM's platform, confirming its validity and Dr. Sofia's credentials. Her application moves forward smoothly, without the delays of manual verification.

Actors

- Healthcare professional (Dr. Sofia): A doctor who completes a SEAFORMEC-accredited training session and requests a BQM certificate.
- Foundation: Manages the training activities and hosts the Virtual Campus for professionals.
- CGCOM (General Council of Official Medical Colleges): The Trusted Issuer responsible for issuing the BQM certificate.
- SEAFORMEC: Accredits the training activity.
- EUDI Wallet: Used by Dr. Sofia to receive and store the BQM certificate.

Current process ("As-Is")
Currently, healthcare professionals who complete accredited training sessions request their BQM certificates manually. The Foundation processes these requests, confirms the completion of the training, and then sends the certificate by email or post. The professional must then keep the physical or digital copy for future use, which may involve additional manual verification steps when presenting it to relevant authorities or organisations.

Future process ("To-Be")
The digitalised BQM certificate issuance process offers a seamless experience for healthcare professionals. Upon completing a SEAFORMEC-accredited training session on the Foundation's Virtual Campus, the system automatically notifies CGCOM. CGCOM then verifies the completion status and generates a digitally signed BQM certificate.

This certificate is immediately sent to the healthcare professional's EUDI Wallet. The professional can then easily manage and share this credential as needed. When shared, the receiving institution can instantly verify the certificate's authenticity through CGCOM's platform.

This digital process eliminates delays, reduces administrative overhead, and ensures the integrity of BQM certifications across the healthcare sector.

Benefits

1. Immediate value & access
   - Instant issuance and verification of training certificates
   - Simplified sharing of professional qualifications
   - Easy management through EUDI wallets
2. Enhanced trust & compliance
   - Secure, verifiable certificates
   - Streamlined compliance tracking
   - Standardized format across institutions
3. Seamless integration
   - Compatible with existing healthcare systems
   - User-friendly interface for healthcare professionals
   - Efficient record management

Challenges

- System reliability: The certificate issuance system must be highly reliable to ensure professionals can receive their certificates without delay after completing training.
- User interface design: Creating an intuitive interface for the Virtual Campus and EUDI Wallet that caters to healthcare professionals of varying technical proficiencies.
- Certificate standardisation: Ensuring that digitally issued BQM certificates are standardised and recognised across different healthcare institutions and regulatory bodies.
- Legacy system integration: Integrating the new digital certificate system with existing training management systems used by the Foundation and CGCOM.

Technical requirements

- Automated certificate generation: A system capable of automatically creating BQM certificates upon verification of training completion.
- Secure API connections: APIs to facilitate secure communication between the Virtual Campus, CGCOM's systems, and the EUDI Wallet.
- Digital signature implementation: Integration of digital signature technology to ensure the authenticity of issued certificates.
- Training completion verification system: An automated system to confirm the successful completion of training before certificate issuance.
- Certificate template management: A flexible system to manage and update BQM certificate templates as requirements evolve.

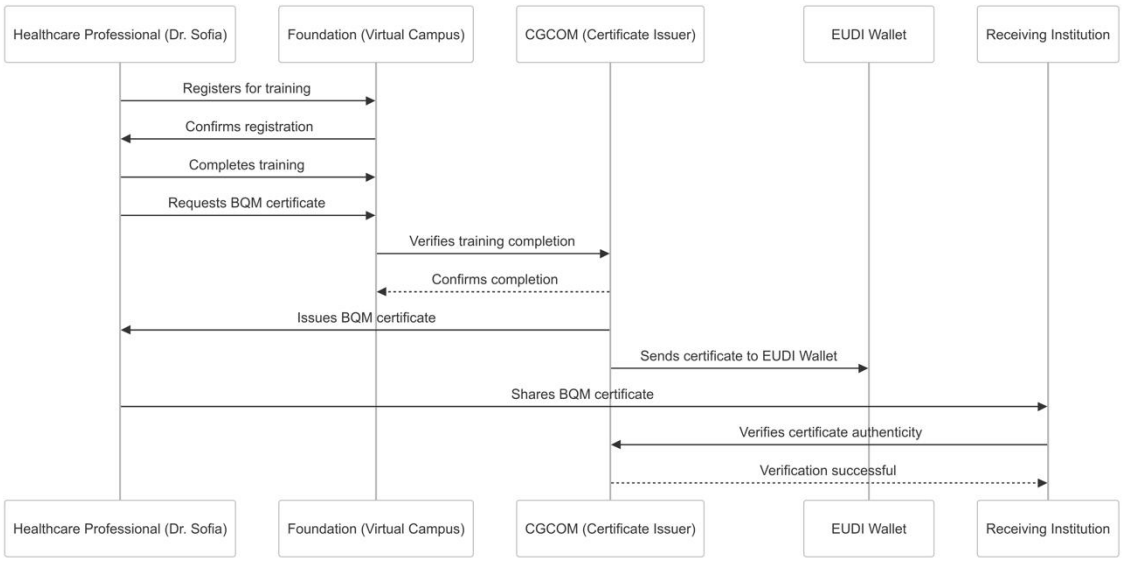
User journey

1. Healthcare professional registers for accredited training
2. Healthcare professional completes training session
3. Healthcare professional requests BQM certificate

4. Professional bodies verify training completion
5. CGCOM issues BQM certificate to EUDI Wallet
6. Healthcare professional shares BQM certificate with relevant organisations

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Register for training | Dr. Sofia (Healthcare professional) | Logs into Foundation's Virtual Campus and registers for SEAFORMEC-accredited training | Virtual Campus; Doctor selects course and provides professional identification details |
| 2. Complete training session | Dr. Sofia (Healthcare professional) | Attends and completes the SEAFORMEC-accredited training session | Virtual Campus records participation and completion |
| 3. Request BQM certificate | Dr. Sofia (Healthcare professional) | Requests issuance of BQM certificate after completing the course | Virtual Campus; Doctor submits request through the platform |
| 4. Verify course completion | Foundation | Verifies Dr. Sofia's completion of the training session | Foundation's system checks completion records |
| | CGCOM | Receives verification from Foundation | CGCOM system receives confirmation from Foundation |
| 5. Issue BQM certificate | CGCOM | Issues BQM certificate and sends to Dr. Sofia's EUDI Wallet | CGCOM system generates, digitally signs, and securely stores certificate in EUDI Wallet |
| 6. Share BQM certificate | Dr. Sofia (Healthcare professional) | Shares BQM certificate when required | EUDI Wallet app; Doctor selects and sends certificate |
| | Relevant organisation/institution | Receives and verifies certificate | Organisation's system verifies certificate through CGCOM platform |




This user journey demonstrates the step-by-step process of obtaining and using a BQM certificate, from registering for training to sharing the certificate with relevant organisations. It shows the interactions between the healthcare professional (Dr. Sofia), the Foundation, CGCOM, and the verifying organisations, as well as the various systems involved in the process

#### *7.7.3.5 Issuance of Validation Professional Competence certificates*

Context

In the healthcare profession, it is crucial to ensure that doctors maintain their qualifications and eligibility to practise medicine. The Validation of Professional Competence (VPC) certificate is issued every six years to verify that doctors are in good standing and meet the necessary requirements for ongoing medical practice. This use case involves the digitisation of the process, allowing registered doctors to request, receive, and share their VPC certificate via the EUDI Wallet.

The Story

Dr. Luis has been practising medicine for over two decades. Every six years, he is required to obtain a Validation of Professional Competence (VPC) certificate to confirm his continued eligibility to practise. In the past, this process involved paperwork and back-and-forth communication with his Doctors' Official College (COM). But now, with the new digitised system, obtaining the certificate is faster and easier than ever.

Dr. Luis logs into his COM's platform and quickly finds the section for requesting a VPC certificate. He submits his application, providing the necessary details to verify his identity. The system takes over from there. Behind the scenes, COM begins the process of verifying Dr. Luis' practice history. Every procedure, consultation, and CPD credit he has accumulated over the last six years is checked. The system also confirms that there are no disciplinary actions on his record.

Once the verification is complete, COM forwards the request to the General Council of Official Medical Colleges (CGCOM). Within minutes, CGCOM issues Dr. Luis' VPC certificate, which is digitally signed and ready for retrieval. A notification pings in Dr. Luis' EUDI Wallet, informing him that the certificate is available.

Dr. Luis opens the EUDI Wallet and sees the VPC certificate securely stored inside. He knows that he no longer needs to worry about physical copies or delayed responses. Whenever the certificate is requested, he can simply share it digitally.

A few weeks later, a regulatory body requires proof of Dr. Luis' professional competence. Without hesitation, he selects the VPC certificate from his EUDI Wallet and shares it directly. The regulatory body verifies the certificate's authenticity through CGCOM's platform, confirming its validity. The entire process is seamless, allowing Dr. Luis to focus on his medical practice rather than paperwork.

Actors

- Registered doctor (Dr. Luis): A doctor who requires a VPC certificate to confirm his professional standing.
- COM (Doctors' Official College): The professional body responsible for validating Dr. Luis' competence and issuing the VPC certificate.
- CGCOM (General Council of Official Medical Colleges): The Trusted Issuer responsible for issuing the VPC certificate.
- EUDI Wallet: Used by Dr. Luis to receive and store the VPC certificate.
- Trust infrastructure Registry: Used to verify the doctor's credentials.

Current process ("As-Is")

Currently, doctors must manually request their VPC certificate from their respective COM every six years. The process involves submitting physical or digital forms, which are processed by COM administrative staff. Verification of the doctor's practice history is conducted, and the certificate is issued either in paper format or via email. The manual process is prone to delays and requires the doctor to physically present the certificate when requested by regulatory bodies or institutions.

Future process ("To-Be")

The new VPC issuance process harnesses digital technology to enhance efficiency and reliability. Registered doctors initiate their VPC request through their COM's online platform.

The system then automatically verifies the doctor's practice history, CPD credits, and disciplinary record by querying comprehensive digital databases. Once verified, COM forwards the request to CGCOM, which generates a digitally signed VPC certificate. This certificate is then sent directly to the doctor's EUDI Wallet.

Doctors can easily share their VPC with regulatory bodies or healthcare institutions as needed. These organisations can instantly verify the certificate's authenticity through

CGCOM's platform. This streamlined process ensures that doctors' professional competence is regularly validated and easily verifiable, supporting patient safety and professional mobility across Europe.

Benefits

1. Professional Excellence
   - Streamlined verification of ongoing competence
   - Simplified renewal processes
   - Clear professional standing across borders
2. Regulatory Compliance
   - Enhanced oversight capabilities
   - Automated compliance checks
   - Improved transparency
3. Data Security & Control
   - Strong privacy protections
   - Secure data management
   - Individual control over credential sharing

Challenges

- Data consolidation: Aggregating practice history, CPD records, and disciplinary information from various sources into a single system for VPC issuance.
- Periodic system updates: Regularly updating the system to reflect changing professional competence requirements and regulations across different medical specialties.
- Cross-border recognition: Ensuring that the digital VPC is recognised and accepted by regulatory bodies and healthcare institutions across different EU countries.
- Transition management: Managing the transition from the current paper-based or email-based VPC system to the new digital system, ensuring no disruption to doctors' practice.

Technical requirements

- Comprehensive doctor database: A centralised or federated database system to store and manage doctors' professional histories and credentials.
- Automated verification algorithms: Development of algorithms to automatically assess a doctor's eligibility for VPC based on predefined criteria.
- Secure data exchange protocols: Implementation of secure methods for data exchange between COM, CGCOM, and other relevant bodies.
- Certificate revocation system: A mechanism to quickly revoke or update a VPC if a doctor's status changes.
- Analytics dashboard: A system to provide COM and CGCOM with overview statistics on VPC issuance, renewals, and any issues identified in the process.

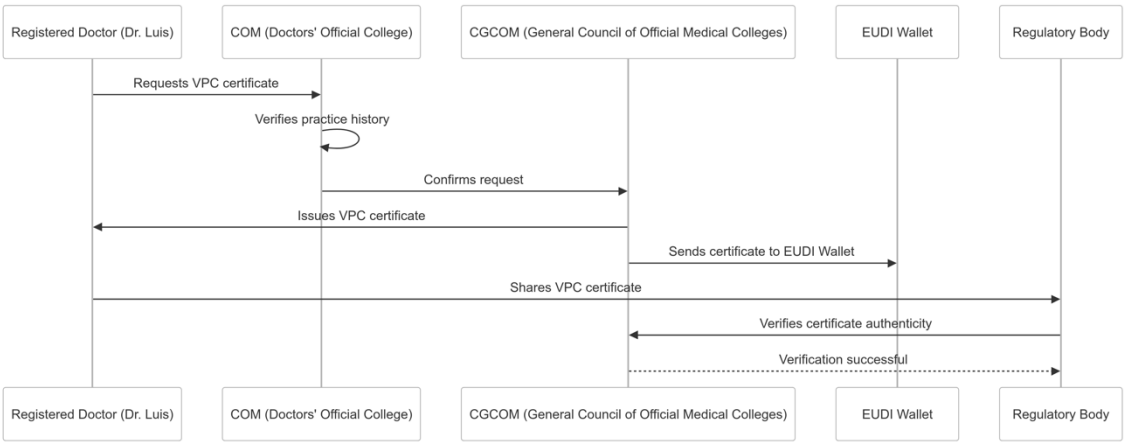
User journey

1. Doctor requests VPC certificate

2. Professional body verifies doctor's practice history
3. Professional body issues VPC certificate
4. Doctor receives VPC certificate in EUDI Wallet
5. Doctor shares VPC certificate with relevant organisations

Detailed user journey:

| User Journey Step | Actor | Action | System Interaction |
|---|---|---|---|
| 1. Request VPC certificate | Dr. Luis (Registered doctor) | Logs into COM's digital platform and submits request for VPC certificate | COM digital platform; Doctor provides professional ID and verifies identity |
| | COM | Receives request and forwards to CGCOM | COM system communicates with CGCOM system |
| 2. Verify practice history | COM | Checks Dr. Luis' practice history | COM database; Automatic check of activity log, disciplinary actions, and CPD credits |
| | CGCOM | Reviews verification results | CGCOM system receives and processes verification data |
| 3. Issue VPC certificate | CGCOM | Generates VPC certificate after successful verification | CGCOM system creates, digitally signs, and securely stores the certificate |
| 4. Provide VPC certificate | CGCOM | Makes certificate available for doctor | CGCOM system sends notification to EUDI Wallet |
| | Dr. Luis (Registered doctor) | Receives notification and retrieves certificate | EUDI Wallet app; Doctor logs in and downloads certificate |
| 5. Share VPC certificate | Dr. Luis (Registered doctor) | Shares VPC certificate when required | EUDI Wallet app; Doctor selects and sends certificate |
| | Regulatory body/Healthcare institution | Receives and verifies certificate | Organisation's system verifies certificate through CGCOM platform |




This user journey demonstrates the step-by-step process of obtaining and using a VPC certificate, from the initial request to sharing with relevant organisations. It shows the interactions between the doctor (Dr. Luis), the COM (Colegio Oficial de Médicos), the CGCOM (Consejo General de Colegios Oficiales de Médicos), and the verifying organisations, as well as the various systems involved in the process. This journey illustrates how digital credentials can streamline the process of maintaining and verifying professional medical qualifications.

## 7.8 Evolving nature of Use Cases

It's important to note that as the trust framework evolves and new technologies emerge, the use cases will need to be regularly reviewed and updated. This ongoing process will ensure that the framework continues to meet the changing needs of the European education and employment landscape.

## 7.9 Conclusion

The use cases, once developed, will serve as a powerful tool for demonstrating the value and functionality of the trust framework. They will provide concrete examples of how the system transforms credential management, enhances educational mobility, and supports lifelong learning and professional qualifications across Europe. By addressing real-world scenarios, these use cases will play a crucial role in gaining buy-in from various stakeholders and guiding the successful implementation of the framework.

Co-funded by the European Union

# Chapter 8: Technical framework and sectorial EAA's catalogue

This chapter details the technical framework and data model that support secure and interoperable digital credentialing across the EU. By defining the core architecture, data structures, and protocols for credential management, this framework underpins the operational model's compliance with EU standards like eIDAS and GDPR. The focus on data security and interoperability ensures that educational and professional credentials can be issued and verified seamlessly across borders, offering a trusted solution for all stakeholders in the credentialing ecosystem.

## 8.1 Introduction

The implementation of trust frameworks for educational and professional credentials requires a robust and flexible technical foundation that can accommodate diverse national requirements while maintaining standardization where needed. This chapter outlines the technical framework and data model that enables the seamless issuance, management, and verification of credentials across Europe.

The framework builds upon established international standards, particularly the W3C Verifiable Credentials Data Model and the European Learning Model, to ensure consistency, interoperability, and trust across implementations while supporting the specific needs of the European education and qualification landscape. It is designed to be both forward-looking and backward compatible, ensuring that institutions can transition at their own pace while maintaining interoperability across the ecosystem

This technical framework implements the operational model detailed in Chapter 4 and supports the use cases presented in Chapter 6.

## 8.2 Core data model architecture

Justification for Data Models

The adoption of the W3C Verifiable Credentials (VC) Data Model and the European Learning Model (ELM) as the core standards for credential issuance and verification is rooted in their proven capabilities for fostering interoperability, ensuring data privacy, and supporting cross-border mobility within the EU. These models align with global digital identity and data standards, making them particularly suited to the objectives outlined in the European Qualifications Framework (EQF) and the Digital Education Action Plan (DEAP).

Key Advantages Include:

- Interoperability: The W3C VC model enables uniform structuring of credential data, allowing educational and professional qualifications to be recognised across all member states without additional modifications.

- Privacy and Security: Features like selective disclosure and cryptographic proofs safeguard personal data, ensuring that credential holders can control what information is shared, in line with GDPR principles.
- Alignment with EU Standards: The use of ELM ensures compatibility with EU-wide initiatives, facilitating seamless integration with services such as Europass and the European Digital Credentials Infrastructure (EDCI).

These aspects underscore why the W3C VC and ELM were selected as the foundational data models for this framework, promoting a unified and secure approach to credentialing across Europe.

The choice of the W3C Verifiable Credentials Data Model and the European Learning Model (ELM) as the standards for credentialing is also rooted in their strong support for interoperability, privacy-preserving features, and alignment with EU digital education policies. These models enable uniformity in the structure of educational credentials, ensuring that digital documents can be securely verified and understood across all EU Member States, enhancing cross-border mobility.

The selected data model incorporates established Bologna Process tools like:

- ECTS credits for measuring student workload
- Degree cycle indicators (Bachelor's, Master's, Doctorate)
- Qualification framework levels
- Quality assurance status

This ensures compatibility with existing European higher education standards while enabling new digital capabilities.

This model enables the credential lifecycle management described in Section 4.2 and supports the implementation roadmap outlined in Chapter 8.

### *8.2.1 Design Philosophy*

The implementation of the European Learning Model (ELM) alongside the W3C Verifiable Credentials framework directly addresses the challenges of interoperability and cross-border recognition. By leveraging these models, institutions can ensure that issued credentials maintain a standardised format that is both machine-readable and verifiable across different systems. This approach mitigates issues related to varying national data standards and supports a coherent digital education ecosystem throughout the EU.

The technical framework is built on two complementary principles that ensure both consistency and adaptability:

1. Standardization through a mandatory core structure:
   - Ensures essential information is consistently captured and presented
   - Facilitates international recognition and comparison of qualifications

- Provides a foundation that cannot be modified, guaranteeing data integrity
- Enables interoperability across different systems and countries

2. Flexibility through country-specific extensions:
   - Allows individual countries to add their unique requirements
   - Enables incorporation of local educational standards
   - Supports country-specific grading systems
   - Maintains compatibility with the international framework

This dual approach ensures that while credentials remain internationally recognizable and verifiable, they can also accommodate the specific needs and requirements of different educational systems and professional bodies.

The technical framework implements the W3C Verifiable Credentials Data Model as its foundation, extended by the European Learning Model to address education-specific requirements. This standards-based approach ensures:

- Consistent credential structure across implementations
- Built-in support for privacy-preserving features like selective disclosure
- Compatibility with existing and future European digital identity initiatives
- Clear separation between core credential attributes and extension fields

The integration of the European Learning Model (ELM) provides a practical solution to the challenges of cross-border credential recognition by ensuring data consistency and standardization. This is critical for member states that need seamless interoperability for educational and professional credentialing. The framework supports the objectives set by the European Qualifications Framework (EQF) and promotes transparency across diverse national systems.

How this benefits stakeholders:

- Educational Institutions: Simplifies the process of credential issuance and verification by using a model that is compatible with EU systems and frameworks.
- Employers and Professional bodies: Facilitates the recognition of professional qualifications and reduces the need for manual validation processes.
- Credential holders: Provides a user-centric approach that prioritises privacy and ease of use, empowering individuals to share their qualifications confidently across borders.

This context further ensures alignment with EU strategies such as the European Education Area (EEA) and the Single Digital Gateway (SDG), which promote cross-border digital services and the Once-Only Principle (OOP).

Co-funded by the European Union

### *8.2.2 Language Requirements*

A critical aspect of the framework is its approach to language management, which balances international accessibility with local compliance:

1. English as mandatory generation language:
   - All core documentation must be generated in English
   - Ensures international accessibility
   - Maintains consistency in terminology across implementations
   - Serves as the reference version for verification

2. Additional official languages through extensions:
   - Countries can add their official languages
   - Multiple language support through standardized extension mechanisms
   - Preserves local identity while ensuring international accessibility

This approach ensures that credentials can be understood internationally while meeting local language requirements, supporting both mobility and local compliance needs.

### *8.2.3* Practical Examples and Use Cases

To illustrate the practical applications of the chosen data models, the following use cases demonstrate their impact:

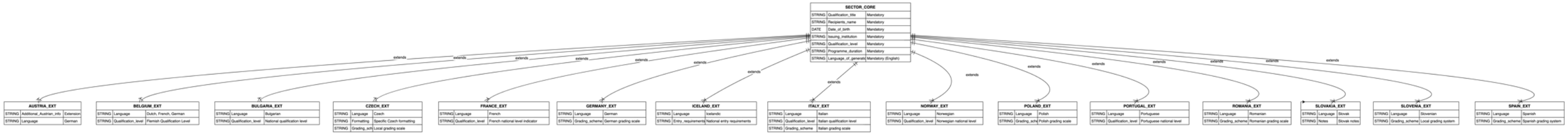
1. Cross-Border academic recognition: A student in Germany graduates with a digitally issued diploma based on the W3C VC and ELM standards. When applying for a master's programme in Spain, the receiving university can instantly verify the diploma's authenticity and details using cryptographic proofs embedded in the credential. This streamlines admissions processes, reduces administrative burdens, and ensures data privacy.
2. Employer verification of Professional qualifications: A professional from France moves to Italy and presents their verifiable professional certification to a potential employer. The certification, structured according to the W3C VC model and containing ELM-compliant data fields, allows the employer to quickly verify the credential through an interoperable verification system. This facilitates faster hiring processes and enhances trust.
3. Lifelong Learning and Micro-Credential recognition: An individual participates in an online training course provided by a Finnish institution, earning a micro-credential formatted according to the ELM and W3C VC standards. This credential is stored in their EUDI wallet and presented to a Swedish employer as part of their application. The standardised format ensures the employer can verify the credential's validity, supporting better skills matching and career progression.

## 8.3 Model structure

Co-funded by the European Union

The framework implements a two-layer approach that forms the backbone of the credential ecosystem. This structure allows for both standardization and flexibility, addressing the diverse needs of educational institutions and professional bodies across Europe.

Co-funded by the European Union



### *8.3.1 Core layer (Sector-wide)*

The core layer establishes the fundamental structure that ensures consistency across all implementations. It consists of carefully selected mandatory and optional fields:

#### Mandatory Fields:

1. Qualification title
   - Official name in English
   - Standardized naming conventions
   - Clear identification of level and field

2. Recipient's name
   - Full legal name
   - International format standards
   - Provisions for different naming conventions

3. Date of birth
   - Standardized date format
   - Additional identifier
   - Prevents confusion with similar names

4. Issuing institution
   - Official name
   - Standardized identifiers
   - Links to institutional databases
   - Qualification level

5.Qualification level

   - Alignment with international qualification frameworks
   - Clear indication of academic or professional level
   - Facilitates qualification comparison across borders

6. Programme duration

   - Standardized format for expressing study duration
   - Includes both time period and credit points
   - Enables accurate comparison of study intensity

7. Language of generation (English)

   - Mandatory English version of all content
   - Ensures international accessibility
   - Serves as the reference version

Co-funded by the European Union

8. Field of study

- Standardized classification of academic/professional field
- Aligned with international classification systems
- Enables accurate field-specific comparison

Optional Fields:

1. Grading scheme
   - Assessment methods
   - Grade calculations
   - International comparison tables

2. Access requirements
   - Program prerequisites
   - Previous qualifications
   - Special conditions

3. Additional notes
   - Supplementary information
   - Program-specific details
   - Special achievements

### *8.3.2 Country Extensions*

The extension layer provides the flexibility needed to accommodate national requirements while maintaining the integrity of the core model. These extensions enable:

1. Additional official language support:
   - Implementation of national language requirements
   - Maintenance of local language versions
   - Correlation with English core content

2. Country-specific qualification frameworks:
   - Integration with national systems
   - Mapping to local standards
   - Alignment with regional frameworks

3. Local educational standards compliance:
   - Adherence to national regulations
   - Local formatting requirements
   - Country-specific educational elements

Co-funded by the European Union

| Field | Sector-wide (Core) | Austria | Belgium | Bulgaria | Czech Republic | France | Germany | Iceland | Italy | Norway | Poland | Portugal | Romania | Slovakia | Slovenia | Spain |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Qualification title | Mandatory | No extension | No extension | No extension | No extension | Specific qualification variant | No extension | No extension | Specific title variants | No extension | Local terminology | No extension | Specific titles | No extension | No extension | No extension |
| Recipient's name | Mandatory | No extension | No extension | No extension | Specific Czech formatting | No extension | No extension | No extension | No extension | No extension | Specific local formatting | No extension | No extension | No extension | No extension | No extension |
| Date of birth | Mandatory | No extension | No extension | No extension | No extension | Optional formatting | No extension | No extension | No extension | No extension | No extension | No extension | Optional formatting | No extension | Optional formatting | No extension |
| Issuing institution | Mandatory | Translation of institution | Inclusion of local language | Local official name | Name in Czech | Name in original and French | No extension | No extension | No extension | No extension | No extension | No extension | No extension | No extension | No extension | No extension |
| Qualification level | Mandatory | EQF level notation | Flemish Qualification Level | National qualification level | ISCED classification | French national level indicator | German national level indicator | EQF inclusion | Italian qualification level | Norwegian national level | Polish national level | Portuguese national level | Romanian national level | National level indicator | National level indicator | Spanish national level |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Programme duration** | Mandatory | No extension | ECTS and local credits | No extension | ECTS | No extension | Duration notation by credit type | Duration in ECTS | No extension | Duration in local credits | Duration notation | Duration notation by ECTS | ECTS notation | Duration notation by credit type | ECTS notation | Duration notation by credits |
| **Language of generation** | Mandatory (English) | German as extension | Dutch, French, German as extension | Bulgarian as extension | Czech as extension | French as extension | German as extension | Icelandic as extension | Italian as extension | Norwegian as extension | Polish as extension | Portuguese as extension | Romanian as extension | Slovak as extension | Slovenian as extension | Spanish as extension |
| **Field of study** | Mandatory | ISCED field notation | Flemish qualification field | ISCED field | Specific Czech field | Field descriptor in French | No extension | No extension | Specific Italian field descriptor | Specific field notation | Specific field notation | ISCED field notation | ISCED notation | ISCED notation | ISCED notation | National field notation |
| **Grading scheme** | Optional | Austrian grading scale | Grading with percentile | Bulgarian grading scale | Local grading scale | French grading with descriptors | German grading scale | Local grading scale | Italian grading scale | Norwegian grading scale | Polish grading scale | Portuguese grading system | Romanian grading scale | Local grading scheme | Local grading system | Spanish grading system |
| **Access requirements** | Optional | Entry requirement field | Access and prerequisites | Local entry requirements | Specific local prerequisites | Local entry requirements | Access criteria | National entry requirements | Italian entry requirements | Norwegian entry criteria | Polish access requirements | Portuguese access requirements | Romanian entry requirements | Access requirements | Local entry criteria | Spanish entry criteria |
| **Additional notes** | Optional | Additional Austrian | No extension | National requirements for reco | Specific notes for Cze | French legal notes | German additional | Icelandic local notes | Local cultural details | Norwegian regula | National qualification | Portuguese legal notes | Romanian notes | Slovak notes | Slovenian legal | National legal notes |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | inf o | | gniti on | ch use | | det ails | | | tio ns | spe cific s | | | | no tes | |

### *7.3.3 Standards and Specifications*

The technical framework implements internationally recognized standards to ensure interoperability, security, and wide adoption across the European education and professional qualification landscape:

#### Core Standards

1. W3C Verifiable Credentials Data Model
The W3C Verifiable Credentials Data Model serves as the foundational standard for our framework, providing a robust and internationally recognized approach to digital credentials. This standard was developed through extensive collaboration within the World Wide Web Consortium (W3C), representing a global consensus on how digital credentials should be structured and verified.

The standard addresses several critical challenges in digital credentialing. First, it ensures that credentials can be cryptographically verified, meaning that any attempt to tamper with or forge a credential can be detected. This is particularly crucial in education and professional qualifications, where the authenticity of credentials directly impacts employment opportunities and further education prospects.

The model's structure directly supports our core layer requirements by providing standardized ways to represent essential credential information. For example, when a university issues a degree certificate, the standard ensures that all crucial elements - from the graduate's name to the qualification level - are represented in a consistent, machine-readable format while remaining human-understandable.

One of the model's key strengths is its support for privacy-preserving features, particularly selective disclosure. This means that credential holders can choose to share only specific parts of their credentials while maintaining the verifiability of that information. For instance, a professional might choose to share their qualification title and date of issuance without revealing their date of birth, even though all this information is contained in the same credential.

The standard also includes robust mechanisms for managing the lifecycle of credentials, including issuance, verification, and potential revocation. This ensures that institutions can maintain control over their credentials even after they've been issued, for instance, being able to revoke a professional certification if necessary.

2. Decentralized Identifiers (DIDs)

Complementing the Verifiable Credentials Data Model, Decentralized Identifiers provide the critical infrastructure for managing digital identity within our framework. DIDs represent a paradigm shift from traditional centralized identity systems, offering a more resilient and flexible approach to identity management in educational and professional contexts.

DIDs solve several fundamental challenges in credential management. They provide a way for educational institutions, professional bodies, and other organizations to establish persistent, verifiable digital identities that don't depend on any single centralized system. This is particularly important in the European context, where we need to support autonomous operation of numerous educational institutions while maintaining interoperability.

The standard enables educational institutions to maintain their autonomy while participating in the broader credential ecosystem. Each institution can create and manage its own identifiers while still being part of the trusted network. This balances the need for institutional independence with the requirements for system-wide trust and verifiability.

For example, when a university issues a digital diploma, its Digital identifier serves as a verifiable digital signature that can be checked independently by any party, without needing to contact the university directly. This significantly streamlines the verification process while maintaining security.

DIDs also support the various authentication methods needed by different types of institutions. A large university might implement sophisticated key management systems, while a smaller professional body could use simpler authentication methods - all while maintaining compatibility with the broader framework.

The standard's flexibility in supporting different authentication methods and service endpoints means that institutions can evolve their technical infrastructure over time without breaking existing credentials. This future-proofing is essential for a system that needs to remain operational for decades, as educational credentials often do.

The combination of these core standards provides several key benefits for our framework:

1. Trust and Security
    - Cryptographic verification ensures credential authenticity
    - Tamper-evident credential structure
    - Secure, verifiable issuer identities
    - Protected credential revocation mechanisms
2. Privacy and Control
    - Granular control over information sharing
    - Privacy-preserving verification processes
    - Support for data minimization principles
    - Compliance with GDPR requirements

Co-funded by the European Union

3. Interoperability and Scalability
   - Standardized credential formats
   - Vendor-independent implementations
   - Cross-border credential recognition
   - Future-proof technical foundation
4. Institutional Autonomy
   - Independent identity management
   - Flexible implementation options
   - Maintained institutional control
   - Supported local requirements

### Complementary Specifications

The core standards provide a solid foundation for digital credentials, but education and professional qualifications have unique requirements that need additional standardization. Two key specifications have been developed to address these sector-specific needs, building upon the core standards while adding crucial education-specific functionality.

1. European Learning Model (ELM)

The European Learning Model represents a significant advancement in standardizing educational credentials across Europe. While the W3C Verifiable Credentials Data Model provides the basic structure for digital credentials, ELM extends this foundation with detailed specifications for representing educational achievements, qualifications, and learning outcomes in a way that meets the specific needs of European education systems.

ELM was developed through extensive collaboration between educational institutions, government bodies, and technical experts across Europe. This collaborative development ensures that the model addresses real-world requirements while maintaining compatibility with existing educational processes and systems.

The model's strength lies in its comprehensive approach to representing educational credentials. It defines standardized ways to express complex educational concepts such as:

- Learning outcomes and achievements
- Credit systems and workload measurements
- Assessment methods and grading schemes
- Professional competencies and skills
- Quality assurance information

For example, when a university needs to issue a transcript of records for a student participating in the Erasmus program, ELM ensures that course credits, grades, and learning outcomes are represented in a way that can be correctly interpreted by institutions across different countries. This standardization significantly reduces the administrative burden of student mobility and credit recognition.

Co-funded by the European Union

ELM also addresses the challenge of representing qualifications that combine multiple elements, such as joint degrees or professional certifications with multiple specializations. Its structured approach ensures that complex credentials remain machine-readable and verifiable while preserving all necessary context and detail.

2. Europass Digital Credentials Infrastructure (EDCI)
The Europass Digital Credentials Infrastructure provides the practical implementation framework for digital credentials in European education. EDCI translates the theoretical models of W3C Verifiable Credentials and ELM into a concrete, operational system that educational institutions can implement.

EDCI was developed by the European Commission as part of the broader Europass initiative, ensuring alignment with EU policies and objectives for education and employment. It provides a comprehensive set of tools, specifications, and services that enable educational institutions to issue, manage, and verify digital credentials in a standardized way.

The infrastructure addresses several critical needs in the European education sector:

1. Standardized Credential Templates EDCI provides ready-to-use templates for common educational credentials, from university degrees to professional certifications. These templates ensure consistency while remaining flexible enough to accommodate institutional and national requirements. For instance, a diploma template can include both standardized European elements and institution-specific features, maintaining both interoperability and institutional identity.
2. Integration Support The infrastructure includes detailed specifications for integrating with existing educational management systems. This is crucial for practical adoption, as it allows institutions to maintain their current workflows while adding digital credential capabilities. A university can continue using its student information system while leveraging EDCI to issue verifiable digital credentials.
3. Quality Assurance EDCI incorporates mechanisms for representing accreditation and quality assurance information within credentials. This enables automatic verification of not just the credential itself, but also the accreditation status of the issuing institution and the quality assurance framework under which the credential was issued.
4. Multi-stakeholder Support The infrastructure supports various stakeholders in the educational ecosystem:
    - Educational institutions can issue standardized digital credentials
    - Students can receive and manage their credentials securely
    - Employers can verify credentials efficiently
    - Quality assurance bodies can integrate their assessments
    - Professional bodies can link qualifications to competency frameworks

The combination of ELM and EDCI provides several key benefits for European education:

1. Enhanced Mobility

- Standardized representation of educational achievements
- Automated recognition of qualifications
- Simplified credit transfer processes
- Reduced administrative barriers

2. Quality and Trust
   - Integrated quality assurance information
   - Verified institutional accreditation
   - Transparent qualification frameworks
   - Maintained educational standards
3. Operational Efficiency
   - Streamlined administrative processes
   - Reduced manual verification needs
   - Automated credential processing
   - Improved data accuracy
4. Future Readiness
   - Support for emerging credential types
   - Adaptability to educational innovations
   - Sustainable technical infrastructure
   - Evolving credential ecosystem

### Alignment with European Frameworks

While technical standards provide the foundation for digital credentials, and education-specific specifications add sector functionality, alignment with established European frameworks is crucial for ensuring that digital credentials serve their ultimate purpose: supporting education and professional mobility across Europe. Two key frameworks provide the structured context needed for meaningful credential recognition and comparison.

1. European Qualifications Framework (EQF)
The European Qualifications Framework represents one of the most significant achievements in European educational cooperation, providing a common reference system that makes qualifications comparable across national borders. In the context of digital credentials, EQF integration is essential for ensuring that qualifications can be automatically understood and evaluated across different national contexts.
The EQF's eight-level structure provides a sophisticated yet practical approach to comparing qualifications. Each level is defined through learning outcomes – what a person knows, understands, and can do – rather than focusing on formal educational pathways. This outcomes-based approach is particularly valuable for digital credentials because it enables:

1. Automated Level Mapping When credentials are issued digitally, they can include structured EQF level information that allows automatic comparison of qualifications. For example, when a graduate with a Bachelor's degree from Spain applies for a Master's program in Germany, the receiving institution can

automatically verify that the qualification meets their entry requirements through EQF level mapping.

2. National Framework Integration The EQF acts as a translation device between different national qualification frameworks. Digital credentials can simultaneously express qualifications in terms of national levels and their corresponding EQF levels, maintaining both national specificity and European comparability. This is crucial for countries that maintain their own qualification frameworks while participating in the European educational space.
3. Learning Outcomes Verification Digital credentials structured according to EQF principles can include detailed learning outcomes information in a standardized format. This enables more precise matching of qualifications to requirements, whether for further education or employment purposes. For instance, an employer in Sweden can understand exactly what skills and knowledge a qualification from Romania represents.

2.ESCO (European Skills, Competences, Qualifications and Occupations)
ESCO provides the crucial link between education and the labor market by offering a standardized, multilingual classification of skills, competences, qualifications, and occupations. Its integration into digital credentials creates a powerful tool for matching educational achievements with professional opportunities across Europe.
ESCO's value in digital credentialing comes from several key features:

1. Standardized Terminology ESCO provides a common language for describing skills and competencies across all European languages. This standardization is essential for digital credentials because it enables:
   - Automatic translation of qualifications between languages
   - Precise matching of skills to job requirements
   - Consistent interpretation of competencies across borders
   - Clear communication between education and employment sectors
2. Skills-Based Mapping The framework allows digital credentials to express educational achievements in terms of specific skills and competencies. This granular approach offers several benefits:
   - More precise matching of qualifications to job requirements
   - Better support for recognition of partial qualifications
   - Clearer pathways for professional development
   - Enhanced support for lifelong learning
3. Labor Market Intelligence By using ESCO's structured vocabulary, digital credentials can be automatically analyzed to:
   - Identify emerging skill needs
   - Track qualification trends
   - Support career guidance
   - Inform curriculum development

The integration of these frameworks with digital credentials provides several crucial benefits:

1. Enhanced Mobility and Recognition
   - Automatic qualification level comparison

Co-funded by the European Union

- Consistent skills interpretation across borders
- Simplified recognition procedures
- Reduced barriers to professional mobility

2. Improved Educational Planning
   - Better alignment with labor market needs
   - Evidence-based curriculum development
   - Clear progression pathways
   - Support for lifelong learning
3. Employment Market Efficiency
   - Precise matching of qualifications to jobs
   - Reduced skills mismatches
   - Better career guidance
   - Enhanced workforce development
4. System-wide Intelligence
   - Improved qualification transparency
   - Better understanding of skill needs
   - Enhanced policy development
   - Evidence-based decision making

The alignment with these European frameworks transforms digital credentials from simple digital documents into powerful tools for educational and professional mobility. By embedding EQF levels and ESCO classifications within standardized digital credentials, we create a comprehensive system that:

- Makes qualifications truly comparable across borders
- Connects education directly to employment opportunities
- Supports evidence-based policy making
- Facilitates lifelong learning and professional development

This framework alignment ensures that digital credentials not only carry verified information about educational achievements but also provide structured, meaningful data that supports real-world mobility and opportunity across Europe. The combination of technical standards, educational specifications, and framework alignment creates a robust ecosystem that serves the needs of learners, educational institutions, employers, and policy makers while advancing European educational and professional mobility objectives.

## 8.4 Country-specific implementations

The framework supports various implementation approaches across different regions, reflecting the diverse educational landscapes while maintaining interoperability.

### *8.4.1 Western European Extensions*

Western European implementations reflect sophisticated educational traditions and cross-border cooperation:

Co-funded by the European Union

- Austria
  - German language extension: Implements full documentation in German while maintaining English core
  - EQF level notation: Integrates European Qualification Framework references with national qualifications
  - Additional Austrian info: Includes specific information about Austrian higher education characteristics
- Belgium
  - Multi-language support: Implements three official languages (Dutch, French, German) reflecting the country's linguistic diversity
  - Flemish Qualification Level: Incorporates specific qualification framework used in the Flemish region
  - Special considerations for regional variations in educational systems
- France
  - French language extension: Complete documentation in French parallel to English core
  - National level indicators: Integration with French qualification framework
  - Specific qualification variants: Accommodates unique French degree titles and specializations
- Germany
  - German language extension: Full German translation maintaining technical precision
  - Specific duration notation: Detailed semester and credit point system
  - German grading scale: Integration of the numerical grading system with descriptors
- Spain
  - Spanish language extension: Complete Spanish translation with technical terminology
  - National field notation: Specific classification of academic disciplines
  - Integration with European educational initiatives

### *8.4.2 Eastern European Extensions*

Eastern European implementations reflect educational reforms and EU alignment:

- Bulgaria
  - Bulgarian language extension: Complete documentation in Bulgarian
  - National qualification level: Integration with reformed qualification framework

    - Local entry requirements: Specific prerequisites aligned with national standards
- Czech Republic
    - Czech language extension: Full Czech translation with technical accuracy
    - Specific formatting requirements: Adherence to national documentation standards
    - Local grading scale: Integration of Czech evaluation system
- Poland
    - Polish language extension: Complete Polish translation
    - Local terminology: Specific academic and professional terms
    - National qualification specifics: Integration with Polish qualification framework
- Romania
    - Romanian language extension: Full Romanian translation
    - Optional formatting: Flexibility in document presentation
    - Romanian grading scale: Integration of national evaluation system
- Slovakia
    - Slovak language extension: Complete Slovak translation
    - Credit type notation: Specific credit system implementation
    - Local qualification recognition requirements

### *8.4.3 Nordic Extensions*

Nordic implementations emphasize international compatibility while maintaining regional educational traditions:

- Iceland
    - Icelandic language extension: Full documentation in Icelandic
    - ECTS inclusion: Strong integration with European Credit Transfer System
    - National entry requirements: Specific prerequisites for Icelandic institutions
- Norway
    - Norwegian language extension: Complete Norwegian translation
    - Local credits system: Integration with Norwegian credit framework
    - Specific field notation: Alignment with Norwegian academic classifications

### *8.4.4 Southern European Extensions*

Southern European implementations reflect regional educational practices while ensuring international recognition:

- Italy
  - Italian language extension: Complete Italian translation
  - Specific title variants: Accommodation of traditional degree titles
  - Local cultural details: Integration of specific academic traditions
- Portugal
  - Portuguese language extension: Full Portuguese translation
  - ECTS notation: Detailed credit system implementation
  - Portuguese legal notes: Compliance with national regulations
- Slovenia
  - Slovenian language extension: Complete Slovenian translation
  - Local grading system: Integration of national evaluation methods
  - Slovenian legal notes: Specific regulatory requirements

## 8.5 Implementation guidelines

The successful deployment of this framework requires careful attention to both technical and organizational considerations.

### *8.5.1 Core Model Implementation*

Key steps for implementing the fundamental structure include:

1. Establishing mandatory fields:
   - Define data types and relationships
   - Implement validation rules
   - Create standardized templates

2. Implementing English as default:
   - Set up primary language controls
   - Establish translation frameworks
   - Define language-specific validation

3. Configuring data formats:
   - Implement standardized formatting
   - Define character set requirements
   - Establish field parameters

### *8.5.2 Extension Implementation*

Guidelines for adding country-specific features include:

1. Creating extension modules:
   - Develop modular framework
   - Implement inheritance from core
   - Establish extension boundaries

2. Configuring language additions:
   - Set up multi-language support
   - Implement translation management
   - Create language-specific validation

3. Implement local formatting rules

   - Define country-specific formats
   - Create regional templates
   - Establish formatting validation

4. Add national qualification frameworks

   - Implement local qualification systems
   - Create mapping to international standards
   - Establish qualification validation

5. Set up regional grading schemes

   - Implement local grading systems
   - Create grade conversion tools
   - Establish grade validation rules

## 8.6 Maintenance and updates

To ensure the long-term success of the framework, regular maintenance and updates are essential:

### *8.6.1 Core model updates*

Ensuring ongoing effectiveness of the core structure:

- Regular review of mandatory fields
  - Scheduled assessment periods
  - Change impact analysis
  - Update implementation procedures
- Standardization compliance checks
  - Regular compliance audits
  - Standard evolution monitoring

    - Adjustment procedures
- International compatibility verification
    - Cross-border testing
    - Compatibility assessments
    - Update validation

### *8.6.2 Extension updates*

Managing country-specific components:

- Country-specific regulation monitoring
    - Legislative change tracking
    - Regulatory compliance assessment
    - Update planning
- Local requirement implementations
    - Requirement analysis
    - Implementation planning
    - Testing procedures
- Regional format updates
    - Format change assessment
    - Update implementation
    - Validation procedures

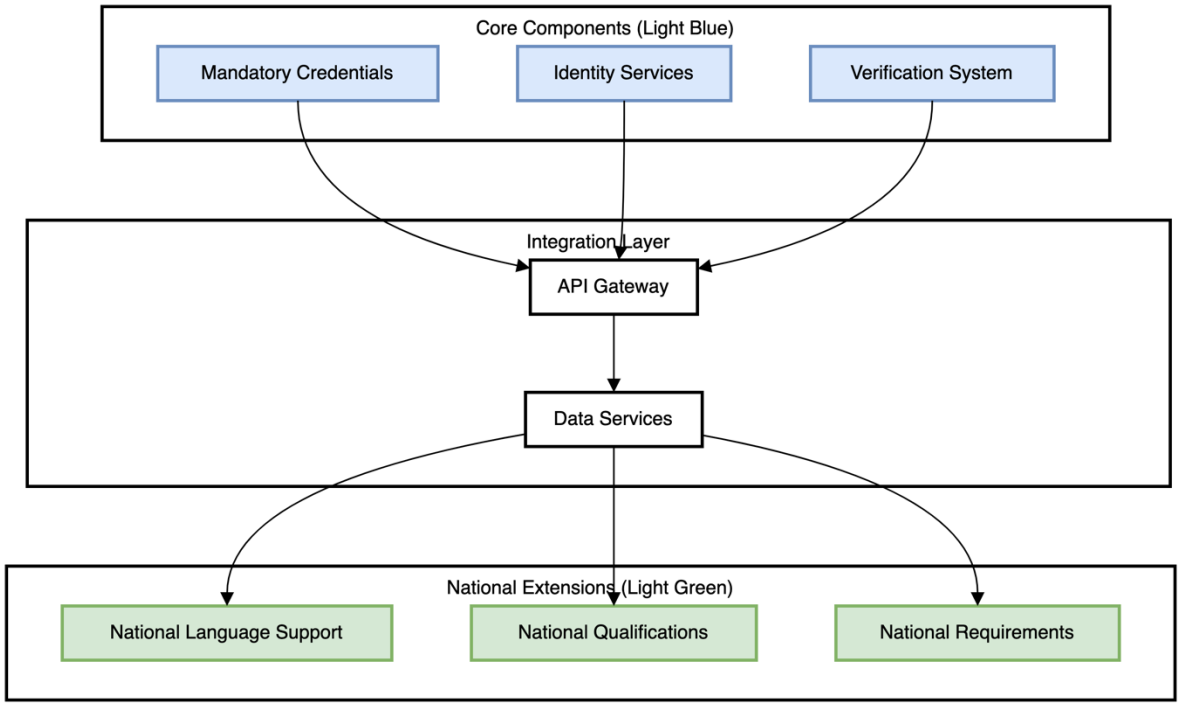
## 8.7 Model visualization and business architecture

### *8.7.1 Overview*

Visual representations of the framework's architecture help stakeholders understand how different components interact and support business processes. These visualizations bridge the gap between technical implementation and business requirements, ensuring alignment across all levels of the organization.

### *8.7.2 Core architecture components*

Co-funded by the European Union




The diagram above illustrates:

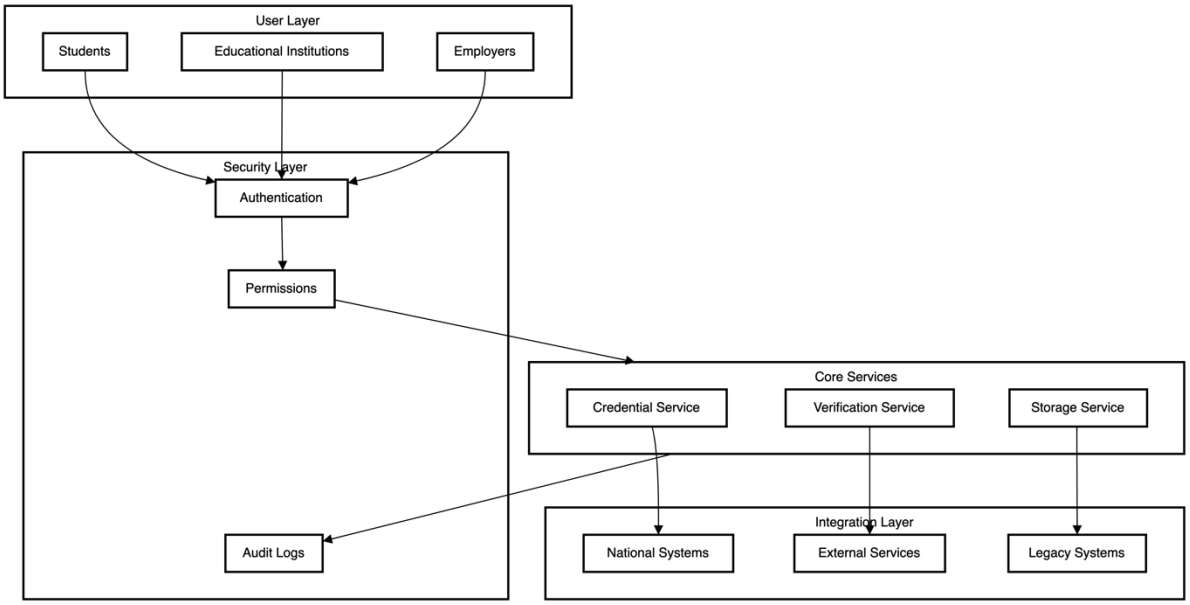
- Core components (light blue) representing mandatory elements
- Extension components (light green) showing country-specific additions
- Relationships between different elements of the framework
- Integration points with existing systems

Key business implications:

- Standardized core enables cross-border recognition
- Flexible extensions support national requirements
- Clear separation of concerns allows phased implementation
- Modular design supports future adaptability

### *8.7.3 Implementation architecture*

Co-funded by the European Union




This visualization shows:

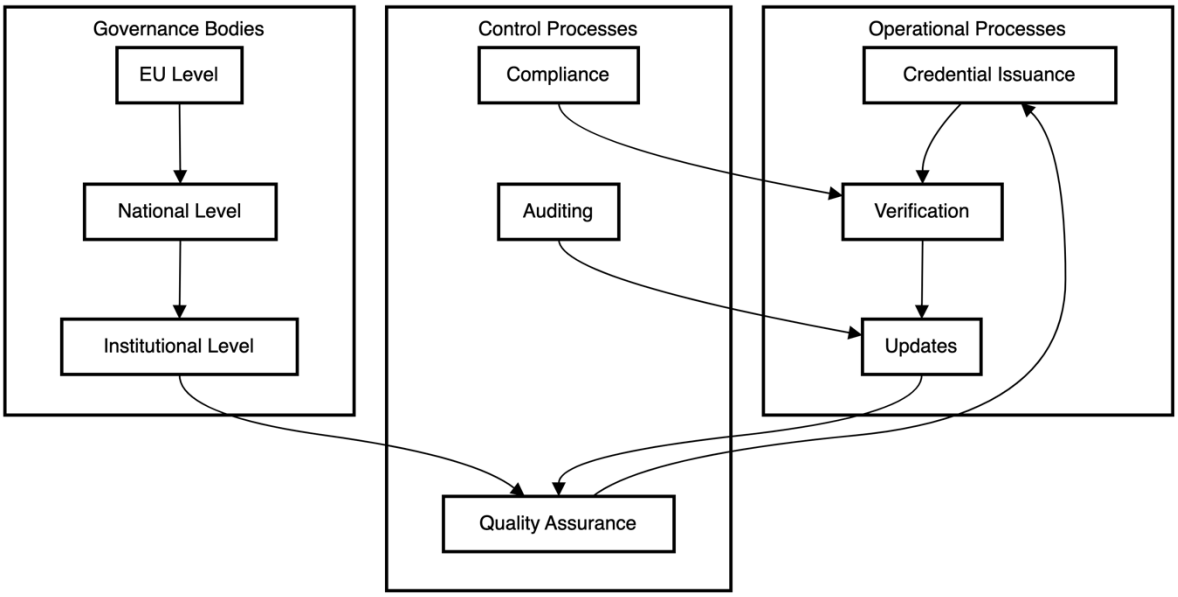
- How different stakeholders interact with the system
- Major data flows between components
- Integration points with existing infrastructure
- Security and privacy boundaries

Business benefits:

- Clear understanding of process flows
- Identified integration requirements
- Visible security and privacy controls
- Streamlined stakeholder interactions

### *8.7.4 Governance and control flow*

Co-funded by the European Union



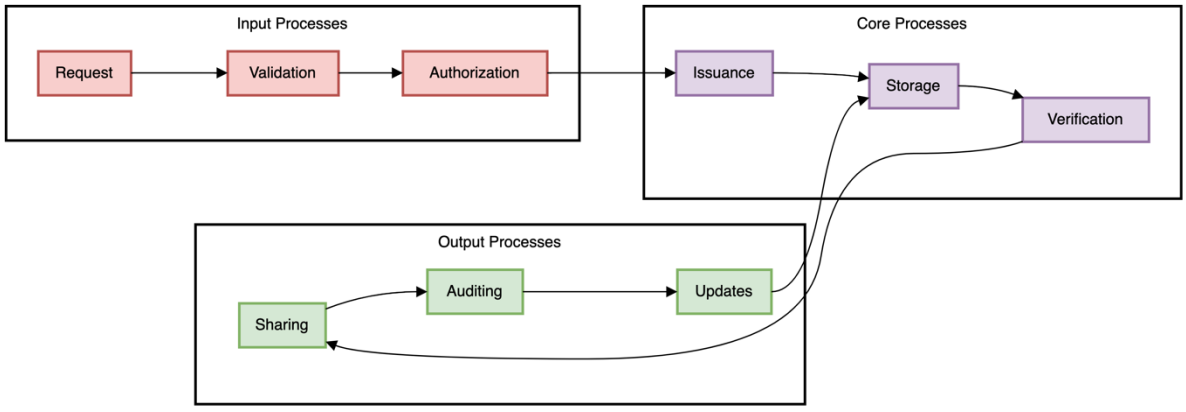

This representation illustrates:

- Decision-making hierarchies
- Quality control processes
- Audit and compliance workflows
- Stakeholder responsibilities

Important considerations:

- Clear lines of authority
- Defined escalation paths
- Compliance checkpoints
- Quality assurance mechanisms

### *8.7.5 Business Process Integration*




This diagram demonstrates:

- How the framework supports key business processes

Co-funded by the European Union

- Integration with existing workflows
- Data exchange patterns
- User interaction points

Operational benefits:

- Streamlined workflows
- Reduced manual intervention
- Clear process ownership
- Enhanced efficiency

#### *8.7.6 Maintenance and Evolution*

The visualizations provided in this section should be regularly updated to reflect:

- Changes in business requirements
- New technological capabilities
- Evolving regulatory requirements
- Stakeholder feedback

This ensures that the framework continues to align with business needs while maintaining technical integrity.

## 8.8 Conclusion

The technical framework for sectorial EAA's catalogue and data model presented in this chapter provide the foundation for a robust and flexible credential management system across Europe. By balancing standardization with flexibility, and international accessibility with local compliance, the framework enables the successful implementation of trust frameworks while accommodating the diverse needs of educational and professional institutions across Europe.

This technical infrastructure supports the use cases presented in previous chapters and enables the continuous evolution of credential management practices. As technology and educational needs continue to evolve, the framework's modular design ensures it can adapt while maintaining the integrity and interoperability of credentials across the European education and professional qualification landscape.

Co-funded by the European Union

# Chapter 9: Data models

Proposed data models form part of the European Union's strategy to digitise educational credentials and streamline student mobility across Europe. They represent different layers of digital identity management in the educational context, from institutional identification to cross-border mobility and comprehensive learning records.

Each model serves distinct yet complementary purposes:

- Managing institutional identities
- Supporting cross-border student mobility
- Enabling university alliance collaboration
- Recording comprehensive learning achievements
- Creating verifiable digital credentials

These schemas align with European standards for digital credentials and support the broader goals of the European Education Area by enabling seamless educational experiences across borders.

## 9.1 EducationalID

This data model which represents a verifiable educational ID schema for individuals in educational settings. This model serves educational institutions by providing a standardised way to issue verifiable digital credentials that can be trusted across the European education sector while maintaining privacy and security standards.

The schema defines a structure for educational identification credentials that follows the json-schema.org draft 2020-12 standard.

The main component of this schema is the credentialSubject object, which contains personal and educational information about an individual. Let's examine the key fields:

Core identification elements:

- "id": A unique identifier using DID:Key format, generated by the user's wallet
- "identifier": A persistent global identifier linked to the person's eduPersonPrincipalName
- "schacHomeOrganization": The educational institution where the person belongs

Personal information:

- "familyName" and "firstName": The person's current legal names
- "displayName": The preferred name for directory listings
- "dateOfBirth": Birth date in yyyyMMdd format
- "commonName": Birth names of the person
- "mail": Primary institutional email address

Educational affiliations:

Co-funded by the European Union

- "eduPersonPrincipalName": A persistent identifier within the institution
- "eduPersonPrimaryAffiliation": Main role at the institution
- "eduPersonAffiliation": List of all roles (student, staff, etc.)
- "eduPersonScopedAffiliation": Roles with institutional context
- "eduPersonAssurance": Identity assurance levels meeting REFEDS framework standards

The schema includes support for profile images through a MediaObject type definition, which can handle various media formats with proper content type and encoding specifications.

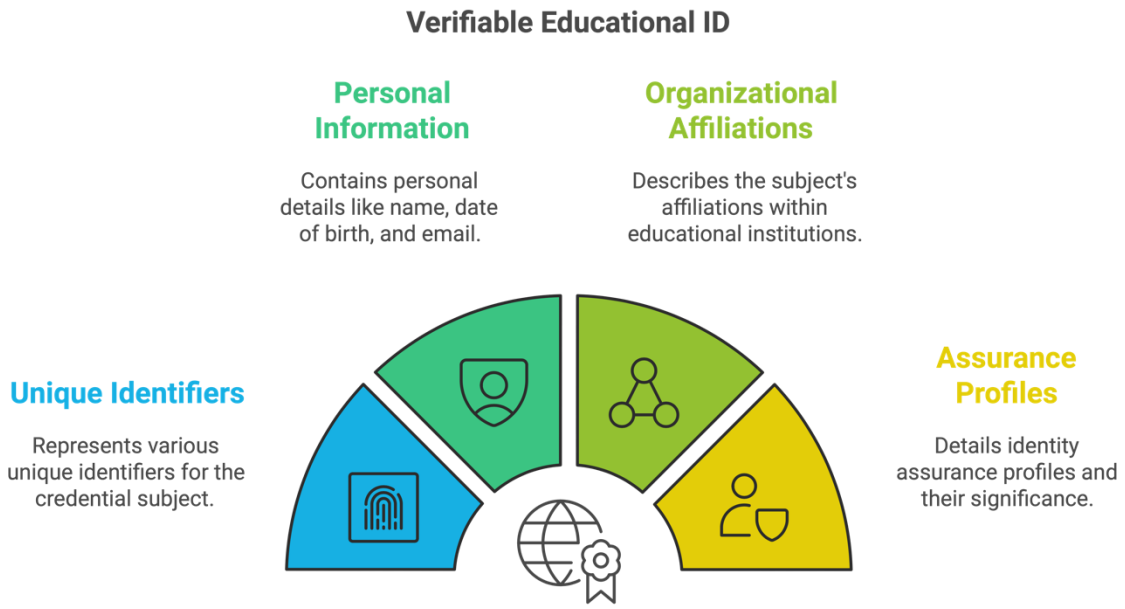
Three mandatory fields exist:

- id
- identifier
- eduPersonScopedAffiliation

The schema supports internationalisation through language codes and includes strict validation rules for URIs and other standardised identifiers. Tis model represents an institutional view, where the focus lies on:

- Recording formal relationships between a person and their educational institution
- Capturing multiple roles within the institution (student, staff, faculty)
- Managing institutional email and identification systems
- Recording specific institutional affiliations through schacHomeOrganization

Co-funded by the European Union




JSON serialisation

See annex C

## 9.2 MyAcademicID

This schema defines the MyAcademicId credential structure, which represents a standardised digital identity for academic and research communities in mobility across Europe. The schema enables educational institutions to issue standardised digital credentials that support academic mobility while maintaining proper identity management practices.

Core identification fields:

- "id": A unique identifier using DID format
- "communityUserIdentifier": A permanent identifier following eduPersonUniqueId format, scoped to erasmus.eduteams.org
- "europeanStudentIdentifier": An array of ESI values supporting student mobility across institutions

Personal information:

- "displayName": The person's full name in a format suitable for complex naming structures
- "givenName": First names or given names
- "familyName": Surname following RFC4519 standards
- "emailAddress": Email contact with proper format validation
- "organization": The person's affiliated organisation

Co-funded by the European Union

Affiliation and rights:

- "externalAffiliation": Array of relationships with academic institutions using eduPersonScopedAffiliation format
- "entitlements": Array of rights and capabilities granted to the person
- "assurance": Identity verification levels meeting REFEDS Assurance Framework standards

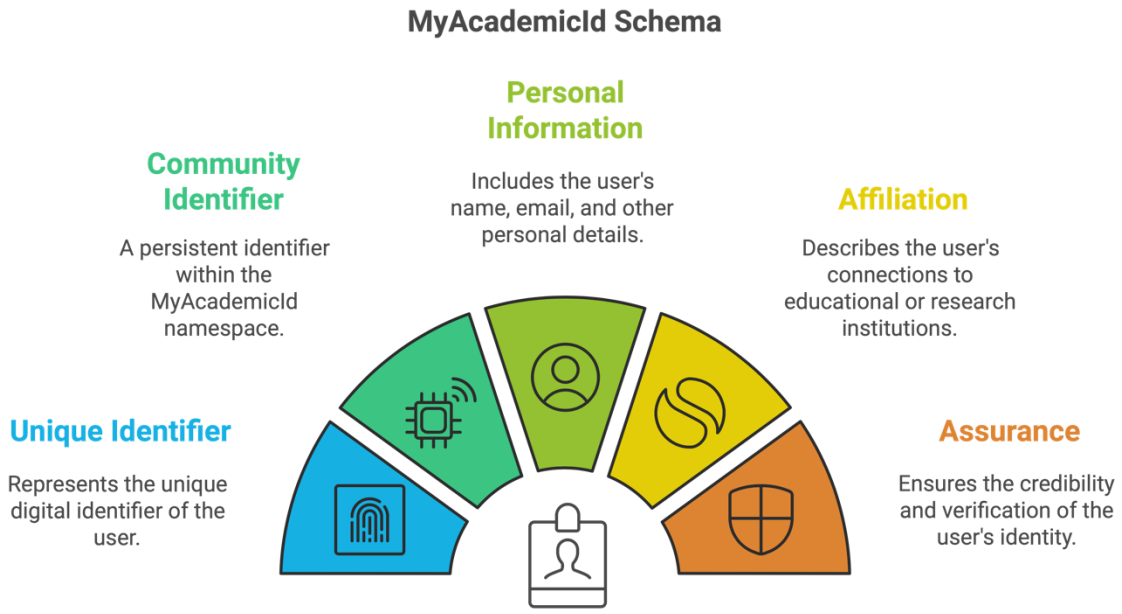
The schema requires seven mandatory fields:

- id
- communityUserIdentifier
- displayName
- givenName
- familyName
- emailAddress
- assurance

Each field links to official standards through Object Identifiers (OIDs) and follows established educational sector specifications from REFEDS and related frameworks.

This model supports the European academic community by:

- Creating persistent identifiers that work across institutions
- Supporting student mobility through standardised European Student Identifiers
- Maintaining compatibility with existing educational directory services
- Providing clear identity assurance levels
- Supporting cross-border academic services



JSON seralisation

See annex C

## 9.3 Europass Digital Credentials (European Learning Model v3.2 )

This schema defines the structure for Europass Digital Credentials (EDC), which is built on the European Learning Model (ELM) version 3.2. The schema represents a comprehensive framework for digital educational credentials in Europe.

The EDC schema represents a comprehensive data model developed by the European Commission to standardise educational data exchange across Europe.

Core structure and principles:

- Built on W3C Verifiable Credential data model standards
- Available in 31 Europass languages
- Maps to other European standards (ELMO, EBSI, EQF, ESCO)
- Enables authentic, tamper-evident digital credentials

The main body of the schema comprises several key components:

Core credential structure:

- "EuropeanDigitalCredentialType": The primary credential object
- Contains mandatory fields like issuer, subject, validity dates, and credential schema
- Supports multiple credential profiles and display parameters

Learning-related entities:

- "LearningAchievement": Records completed educational accomplishments
- "LearningActivity": Describes educational activities undertaken
- "LearningAssessment": Documents evaluation methods and results
- "LearningEntitlement": Specifies rights or permissions granted through education

Supporting elements:

- "Organization": Represents educational institutions with legal identifiers
- "Person": Contains detailed information about credential holders
- "Location": Provides standardised geographical information
- "MediaObject": Handles credential attachments and visual elements
- "Evidence": Supports verification of claims and achievements

Administrative components:

- "AwardingProcess": Records how credentials are granted
- "VerificationCheck": Manages credential verification
- "CredentialStatus": Tracks the current state of credentials

Co-funded by the European Union

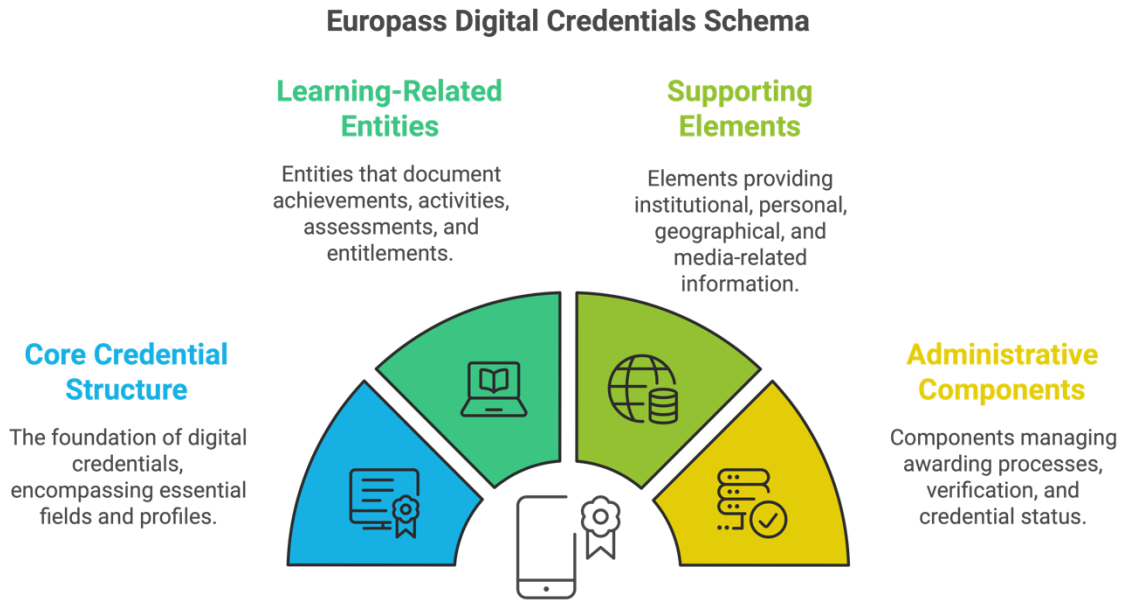
- "DisplayParameter": Controls how credentials are presented

The schema includes extensive multilingual support through "LangStringType" and incorporates standardised reference data using "ConceptType". This enables consistent interpretation across European education systems.

The model links with external standards and frameworks:

- Uses standard identifiers (URIs) for concepts
- Integrates with education-specific standards
- Supports grading schemes and credit systems
- Enables credential verification through proof mechanisms

Each component maintains strict validation requirements while offering flexibility to accommodate different educational contexts across Europe.




The European Learning Model (ELM) can be used to issue credentials (referred to as Electronic Attestations of Attributes . EAAs), for a wide range of education and training levels and contexts. This includes tertiary, secondary, primary, and adult education, as well as formal, non-formal, and informal learning achievements. The model is highly adaptable and built on principles that support various types of learning outcomes, making it suitable for diverse use cases.

Examples of credentials supported by ELM:

- Formal Education:
  - Tertiary: VET, Master's and Bachelor's degrees, Diplomas, Doctorates.

    - Secondary and Primary: VET, Certificates of Completion, High School Diplomas.
- Non-Formal Education:
    - Micro-credentials: Short learning programmes, skill certifications.
    - Adult education achievements: Continuing education courses, vocational training certificates.
- Informal Education:
    - Certificates of participation or completion in workshops or training programmes.
    - Records of learning achievements gained through informal means, such as MOOCs or self-paced learning platforms.

Features making ELM suitable for various education types:

- Versatility: ELM's data model allows for the encoding of information relevant to different educational settings and levels, including qualification descriptions, learning outcomes, accreditation details, and the context of the learning process.
- Interoperability: The model aligns with standards like the W3C Verifiable Credentials Data Model and integrates with other European frameworks such as ESCO (skills and competences) and the EQF (qualification levels), ensuring compatibility across systems.
- Customisation: The ELM can be tailored to different credentialing needs, whether for formal degrees or less structured recognitions like participation in community learning or professional upskilling initiatives.
- Recognition of All Learning Types: By incorporating attributes relevant to both structured and unstructured learning experiences, the model ensures that credentials for non-formal and informal learning are as verifiable and trustworthy as those from formal education.

Supporting EU strategies:

- Micro-Credentials Framework: Supports the Council Recommendation on micro-credentials by standardising their issuance, enhancing transparency, and fostering portability.
- Digital Education Action Plan: Facilitates digital credentialing processes to support lifelong learning and seamless mobility within the European Education Area.
- EBSI and eIDAS Integration: Credentials issued using ELM can be anchored in the European Blockchain Services Infrastructure (EBSI) and comply with eIDAS standards for verifiability and trust.

Practical applications:

- Issuing a Master's Degree: A university issues a Master’s degree credential in ELM format, ensuring its compatibility with EQF levels and enabling cross-border recognition.
- Micro-Credentials for Upskilling: An online training provider issues skill-specific micro-credentials that can be verified and added to an EUDI Wallet.

- Transcript of Records: An Erasmus+ participant receives a digital transcript of records, encoded in ELM, to ensure seamless credit transfer between institutions.

The ELM's flexibility and alignment with European and global standards make it an effective framework for issuing and verifying credentials across all types of education, facilitating recognition and mobility for learners and professionals.

JSON serialisation

See annex C

## 9.4 AllianceID

This schema defines the structure for a verifiable University Alliance ID. It's designed to identify members of European university alliances. The schema represents a minimalist but effective approach to identity management within university alliances, requiring only essential identification elements while maintaining the verifiable nature of the credential.

The schema contains two main sections:

Core credential subject fields:

- "id": A unique identifier for the individual
- "identifier": A structured object containing alliance-specific details

The identifier object includes:

- "schemeID": The identification scheme being used
- "value": The actual identification value
- "id": A URI format identifier

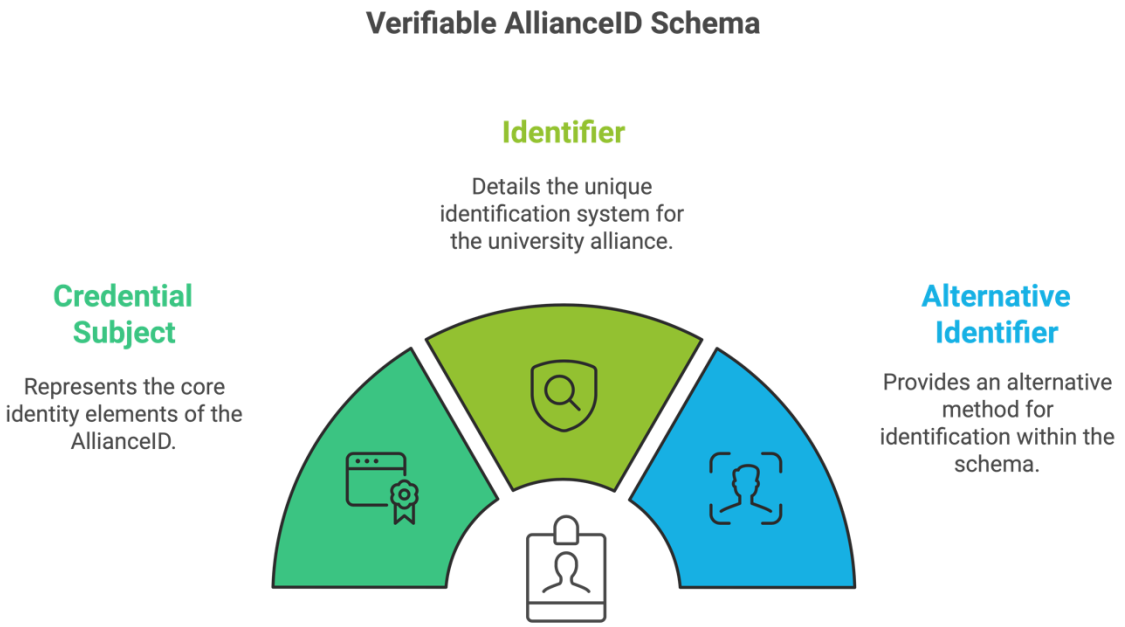
The schema uses a specific format for alliance identification:
`urn:schac:europeanUniversityAllianceCode:int:euai:<sHO>:<code>`
where:

- sHO: The schacHomeOrganization of the issuing alliance
- code: The specific university alliance code

This model serves university alliances by:

- Creating standardised identifiers for alliance members
- Maintaining compatibility with EBSI standards
- Supporting verifiable credentials
- Enabling cross-alliance recognition

Co-funded by the European Union




JSON serialisation

See Annex C

# Chapter 10: Implementation roadmap

## 10.1 Introduction

This chapter provides a structured, step-by-step guide for the adoption and deployment of the educational credential management framework across EU member states (DC4EU related ones). The roadmap will outline the main phases of implementation: preparation and assessment, pilot implementation, full-scale rollout, and ongoing management and improvement. This roadmap is designed to ensure compliance with EU regulations, alignment with European initiatives, and successful integration into national systems.

This roadmap guides the implementation of:

- The operational model detailed in Chapter 4
- The technical framework specified in Chapter 8
- The use cases demonstrated in Chapter 6"

## 10.2 Phase 1: Preparation and assessment

The preparation phase is crucial for setting the foundation for a successful implementation. This stage involves strategic planning, stakeholder engagement, and initial assessments.

- Strategic Planning: Define project objectives and align them with national and EU-level digital education strategies, such as the European Education Area (EEA), the European Skills Agenda, and the Digital Education Action Plan.
- Stakeholder Identification and Engagement: Identify key stakeholders, including educational institutions, accreditation bodies, government authorities, and technology providers. Engage stakeholders early to ensure commitment and gather feedback.
- Regulatory and Legal Compliance: Assess the alignment with relevant EU regulations, such as eIDAS, GDPR, and the Single Digital Gateway, to identify necessary legal and policy adjustments.
- Governance Identification: Collaborate with WP5 partners, leveraging existing regulations and publications from relevant authorities to identify the following key governance types:
    - Entitlement Governance: The governance model that identifies a legal entity as a relevant actor in the education and/or professional qualifications domain and defines its scope of activity within that domain.
    - Quality Assurance Regimes: The governance model related to educational quality assurance, involving periodic audit processes and accreditation of institutions and/or programs that meet quality requirements.
    - Non-foundational Identity: The governance model(s) linked to non-foundational identity credentials (regulated under trust services, not the legal eID regime), such as EducationalID, MyProfessionalID, MyAcademicID, MyAllianceID, etc.

Co-funded by the European Union

- Infrastructure Readiness: Review current IT infrastructure to determine gaps and needs for technical upgrades or integrations.
- Partner Ecosystem Mapping: Identify all WP5 partners and their roles or connections within the educational sector (e.g., education providers, accreditation issuers, technology providers). This step helps outline the WP5 ecosystem within DC4EU, fostering collaboration synergies and recognizing potential actors for cross-border user journey implementation (e.g., governance actors, service providers, implementers).
- User Journey Mapping: Collect and analyse current user journeys to understand the existing processes and pain points that will be addressed by the new system.

This phase must ensure alignment with:

- The trust model requirements outlined in Section 4.1
- The technical specifications detailed in Section 7.2
- The compliance framework described in Section 4.4

## 10.3 Phase 2: Pilot implementation preparation

The pilot phase tests the framework in a controlled environment to identify potential challenges and refine processes before a full-scale rollout.

- Selection of Piloting Agents: Choose pilot institutions and regions that represent diverse educational and regulatory environments.
- Pilot scope definition: Establish the specific use cases to be tested, such as credential issuance, verification, and the onboarding of educational institutions and users.
- Proposing standardized schemes and data Models: Develop and propose standardized data models and a sectoral catalogue of Electronic Attestations of Attributes for education and professional qualifications.
- Deployment of Governance: Deploy the identified governance structures from Phase 1 onto the existing infrastructure. This step ensures that all necessary governance components are in place before advancing to the development and implementation of user journeys in Phase 3.
- Technical integrations preparation: Identify necessary technical integrations, including credential lifecycle management systems, issuers, verifiers, and local databases.
- Gap reporting and coordination: If gaps are identified between the proposed standardization efforts (e.g., data models, schemes) and the existing infrastructure, these gaps must be reported to the responsible infrastructure teams to ensure necessary adjustments are made.
- Training and support preparation: Develop and deliver training materials for stakeholders involved in the pilot phase. Ensure support mechanisms, such as a helpdesk, are in place.
- Monitoring and KPI tracking preparation: Define and monitor key performance indicators (KPIs) to evaluate the pilot's success, such as user adoption rates, verification times, and system reliability.

Co-funded by the European Union

- Feedback loop preparation: Gather feedback from pilot participants to inform adjustments and improvements. Regular meetings and reporting will support iterative refinement.

Pilot implementations should follow the patterns demonstrated in the use cases in Sections 6.3.1 through 6.3.3, whilst adhering to the technical requirements specified in Chapter 8.

## 10.4 Phase 3: Full-scale rollout

Following successful pilot testing, the full-scale rollout extends the implementation to a broader set of institutions and regions.

- Deployment plan: Develop a phased deployment schedule, starting with early adopters and scaling to additional institutions in subsequent waves.
- Capacity building: Expand training and support programs to include all participating institutions and stakeholders. This includes workshops and online training resources.
- System enhancements: Address any technical or operational issues identified during the pilot phase. Ensure that all systems meet interoperability standards and align with EU-level frameworks.
- Single point of contact establishment: Deploy a single point of contact for educational institutions to streamline communication, support, and problem resolution.
- User Journey rollout: Implement the updated user journeys, ensuring alignment with eIDAS, the European Digital Identity Wallet (EUDIW), and other relevant frameworks.

## 10.5 Phase 4: Ongoing management and improvement

To maintain the effectiveness and relevance of the credential management system, continuous management and iterative improvements are essential.

- Monitoring and reporting: Implement ongoing monitoring tools to track system performance and user satisfaction. Regular reports should be submitted to stakeholders, detailing key metrics and any operational challenges.
- Quality assurance: Establish quality assurance procedures to ensure the system's compliance with EU standards and the consistent performance of credential management processes.
- Feedback mechanisms: Maintain open channels for feedback from institutions, users, and regulatory bodies to facilitate continuous improvement.
- Periodic reviews and updates: Conduct periodic reviews to adapt to new regulations, technological advances, and feedback. Updates to the system should be implemented to align with changes in EU directives and educational requirements.

Co-funded by the European Union

- Risk management: Implement a risk management framework to identify, assess, and mitigate potential risks, ensuring that the system remains robust against new challenges.

## 10.6 Success metrics and evaluation criteria

Success in the implementation of the credential management framework will be measured through a series of key indicators:

- Adoption rates: The number of institutions and users onboarded.
- Verification efficiency: Average time taken for credential verification processes.
- System reliability: Uptime and system performance metrics.
- User satisfaction: Surveys and feedback mechanisms to gauge user experience.
- Compliance: Adherence to EU regulations and national requirements.

This phased approach provides a comprehensive strategy for the successful implementation of the credential management framework, ensuring alignment with European digital transformation goals and addressing stakeholder needs effectively.

Co-funded by the European Union

# Annex A: Glossary of terms

1. CPD (Continuous Professional Development): Ongoing education for professionals to maintain and enhance skills in their fields, often a requirement for professional licensing and career progression.

2. DLT (Distributed Ledger Technology): A technology that uses a decentralised network to store data in a secure, tamper-proof format, supporting blockchain and other applications.

3. EBSI (European Blockchain Services Infrastructure): A European Union blockchain initiative providing secure, cross-border services including verifiable credentials for educational and professional credentials.

4. eIDAS (Electronic Identification, Authentication and Trust Services Regulation): Regulation (EU) No 910/2014, governing digital identification and trust services for electronic transactions within the EU, supporting interoperability and legal recognition of digital credentials.

5. EducationalID: A unique digital identifier assigned to individuals within the education sector, used in digital credentialing systems to manage records securely and efficiently.

6. EHEA (European Higher Education Area): A collaborative network of European countries aiming to ensure comparability of higher education standards and quality to support student mobility.

7. ELM (European Learning Model): A framework inspired by the W3C Verifiable Credentials model, designed to support digital credentialing and interoperability across the EU's education systems.

8. ELMO (European Learner Mobility Ontology): A data model used within the Erasmus Without Papers (EWP) network to facilitate cross-border student data exchanges.

9. EQF (European Qualifications Framework): A reference framework to help compare qualifications across EU countries, supporting transparency and recognition of qualifications.

10. ESCO (European Skills, Competences, Qualifications, and Occupations): A classification system by the European Commission to connect job matching, skill recognition, and labour mobility across the EU.

11. EDSSI (European Digital Student Service Infrastructure): An infrastructure supporting student mobility within the EU, providing services for secure digital credentialing and verification.

Co-funded by the European Union

12. FMC (Further Medical Competence): Advanced qualifications for healthcare professionals to demonstrate specific competencies and advanced skills.

13. GDPR (General Data Protection Regulation): Regulation (EU) 2016/679, the EU's legal framework for data protection and privacy, critical for protecting personal data in digital credentialing.

14. GUNet (Greek Universities Network): A platform supporting eDiplomas and academic credential sharing, aiding in credential verification for Greek universities.

15. ISCED (International Standard Classification of Education): A UNESCO framework that standardises education classification globally, supporting data comparisons and interoperability in education statistics.

16. MyAcademicID: An initiative providing students with a digital identity to support participation in the European Higher Education Area, aiding in secure and seamless access to cross-border educational services.

17. Non-Foundational Identity: An identifier used within specific sectors, such as education, distinct from foundational (e.g., national ID) systems, supporting identity verification while respecting sector-specific needs.

18. OOP (Once-Only Principle): A principle in the EU's digital strategy ensuring that data collected from users is reused across services to prevent repetitive data entry.

19. PID (Personal Identification): Personal data stored securely in digital credentialing systems, supporting identity verification within trusted frameworks.

20. ProfessionalID: A unique digital identifier for managing records and credentials within professional fields, enhancing security and trust in digital credentialing.

21. QR (Quick Response code): A matrix barcode used for easy, secure access to digital information, commonly used in credentialing to validate and share digital documents.

22. SDG (Single Digital Gateway): Regulation (EU) 2018/1724, facilitating online access to information and public services across EU Member States, supporting digitalisation and streamlined administrative processes.

23. SEAFORMEC (Foundation for Medical Education and Training Accreditation): An accrediting organisation for healthcare-related Continuous Professional Development (CPD) and Further Medical Competence (FMC) activities within Europe.

24. StatusList2021: A service for managing and verifying the status of digital credentials, supporting revocation and suspension functions to enhance trust in digital credentialing.

Co-funded by the European Union

25. Trust Framework: A set of rules, protocols, and governance structures that define how digital credentials are managed, issued, and verified within a system, ensuring standardisation and security.

26. UEMS (European Union of Medical Specialists): A professional organisation collaborating with SEAFORMEC to accredit medical education, supporting standardised and recognised CPD for medical specialists across Europe.

27. Verifiable Credential (VC): A digital document issued by a trusted entity that can be cryptographically verified to confirm authenticity and enhance portability across digital systems.

28. W3C-VC (World Wide Web Consortium - Verifiable Credentials): A standard developed by the W3C for creating, issuing, and verifying digital credentials. It enables trusted digital representations of credentials that can be securely shared across systems.

29. W3C-VCDM (W3C Verifiable Credentials Data Model): The data model created by W3C to structure verifiable credentials, supporting interoperability and enabling secure, standardised credential issuance and verification.

30. DID (Decentralized Identifier): A globally unique persistent identifier that does not require a centralized registration authority and enables cryptographic verification of credential ownership and validity. DIDs are critical components of verifiable credentials, supporting secure, decentralized identity management.

31. EDCI (Europass Digital Credentials Infrastructure): A framework developed by the European Commission that implements standardized digital credentials based on the European Learning Model and W3C Verifiable Credentials standards. It provides infrastructure for issuing, storing, and verifying digital credentials across Europe.

32. ESCO (European Skills, Competences, Qualifications and Occupations): A multilingual classification system by the European Commission that identifies and categorizes skills, competencies, qualifications, and occupations relevant for the EU labor market and education/training. It serves as a common reference terminology for digital credentials.

33. European Learning Model (ELM): A data model based on W3C Verifiable Credentials, specifically designed for educational credentials in Europe. It defines the structure and relationships for representing educational achievements, qualifications, and learning outcomes in a standardized format.

34. Selective Disclosure: A privacy-enhancing feature of verifiable credentials that allows credential holders to share only specific parts of their credentials while maintaining verifiability. This enables individuals to control their personal data and share only what is necessary for a specific purpose.

Co-funded by the European Union

35. W3C (World Wide Web Consortium): The main international standards organization for the World Wide Web, responsible for developing protocols and guidelines that ensure the long-term growth and standardization of web technologies, including specifications for verifiable credentials.

36. W3C Verifiable Credentials Data Model: A World Wide Web Consortium standard that provides a mechanism to express credentials on the web in a way that is cryptographically secure, privacy respecting, and machine verifiable. This model serves as the foundation for digital credentialing systems in educational and professional contexts.

Co-funded by the European Union

# Annex B: Technical diagrams and business flows

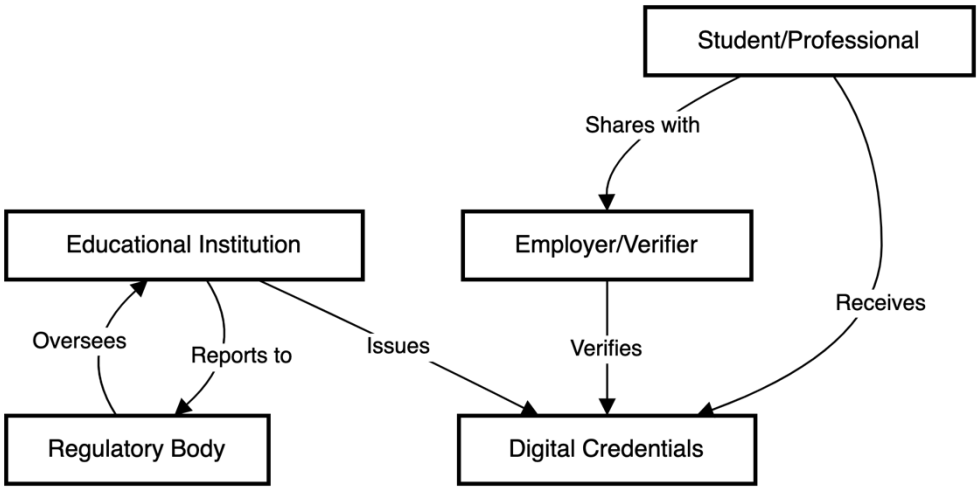
This annex provides visual representations of key business processes and relationships within the European educational credentialing ecosystem. Each diagram emphasizes operational flows and organizational relationships while avoiding technical implementation details.

## 1. Core Ecosystem Components

This diagram provides a visual representation of the core components essential for implementing the DC4EU framework in educational and professional credentialing. It includes foundational elements required for decentralised trust management, and how they interrelate within the broader ecosystem.

### 1.1 Stakeholder Interaction Model

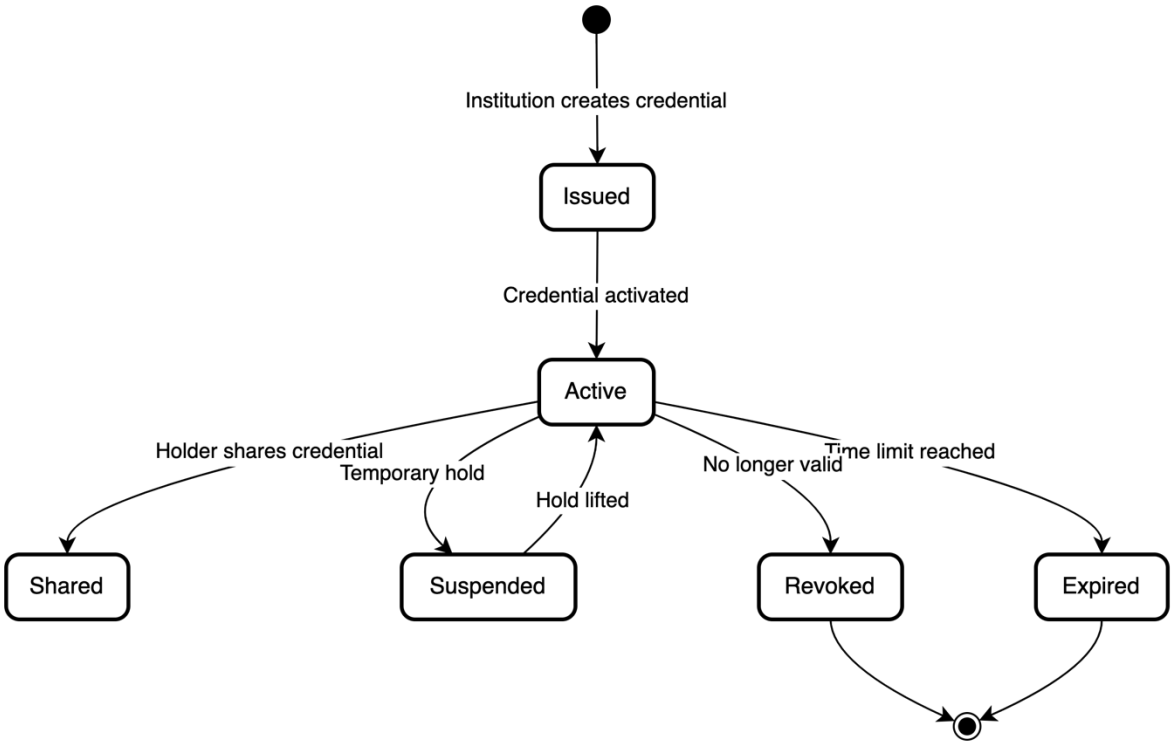
This diagram maps the core interactions between main participants in the digital credentials ecosystem. It demonstrates how credentials flow from educational institutions to students, how these credentials are shared with employers, and how regulatory oversight maintains system integrity. The model emphasizes the bi-directional nature of trust relationships and verification processes. This model serves as a framework for understanding each stakeholder's responsibilities and how they collaborate to maintain the integrity and trustworthiness of digital credentials across the EU. It highlights interaction pathways that support compliance, data privacy, and streamlined user experiences




### 1.2 Credential Lifecycle

This diagram presents the complete lifecycle of a digital credential from issuance through various possible states including active use, suspension, expiration, and revocation. It illustrates all possible status transitions and demonstrates how credentials are managed throughout their lifetime.

Co-funded by the European Union

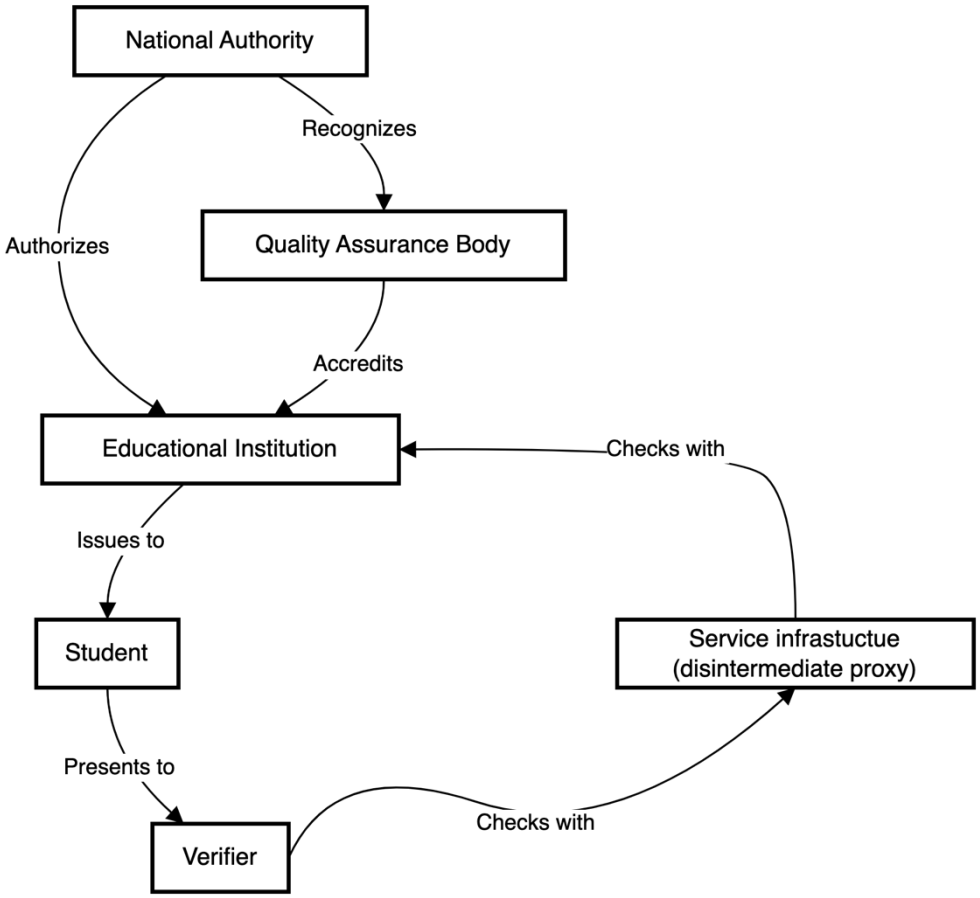



2. Trust Relationships

2.1 Trust Network Structure

This diagram outlines how trust is established and maintained between different organizations. It shows the hierarchical relationships between national authorities, educational institutions, and quality assurance bodies, demonstrating how trust flows enable credential verification and recognition.

Co-funded by the European Union



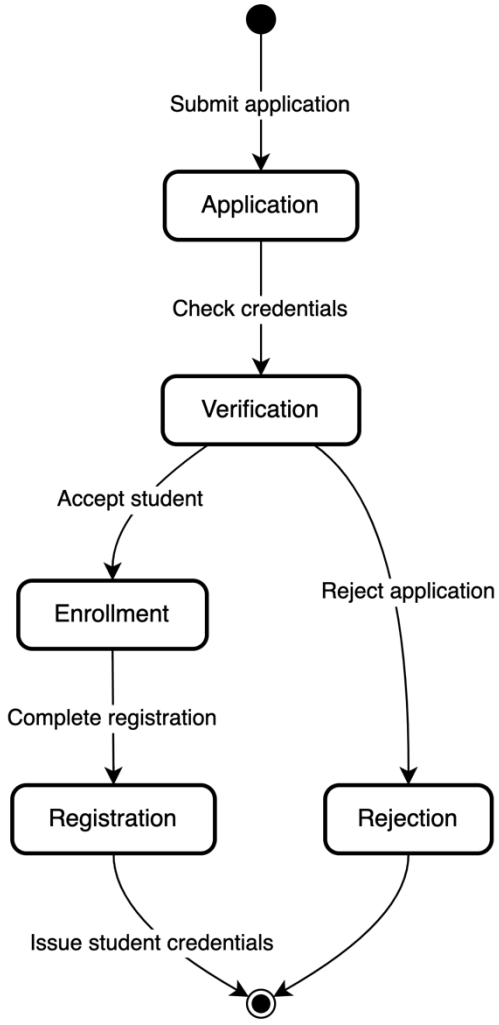
## 2.2 Cross-Border Recognition Flow

This visualization demonstrates how credentials are recognized across national borders. It maps the interaction between home institutions, host country authorities, and European qualification frameworks, showing the process flow for international credential recognition.

# 3. Business Process Flows

## 3.1 Student Enrollment Process

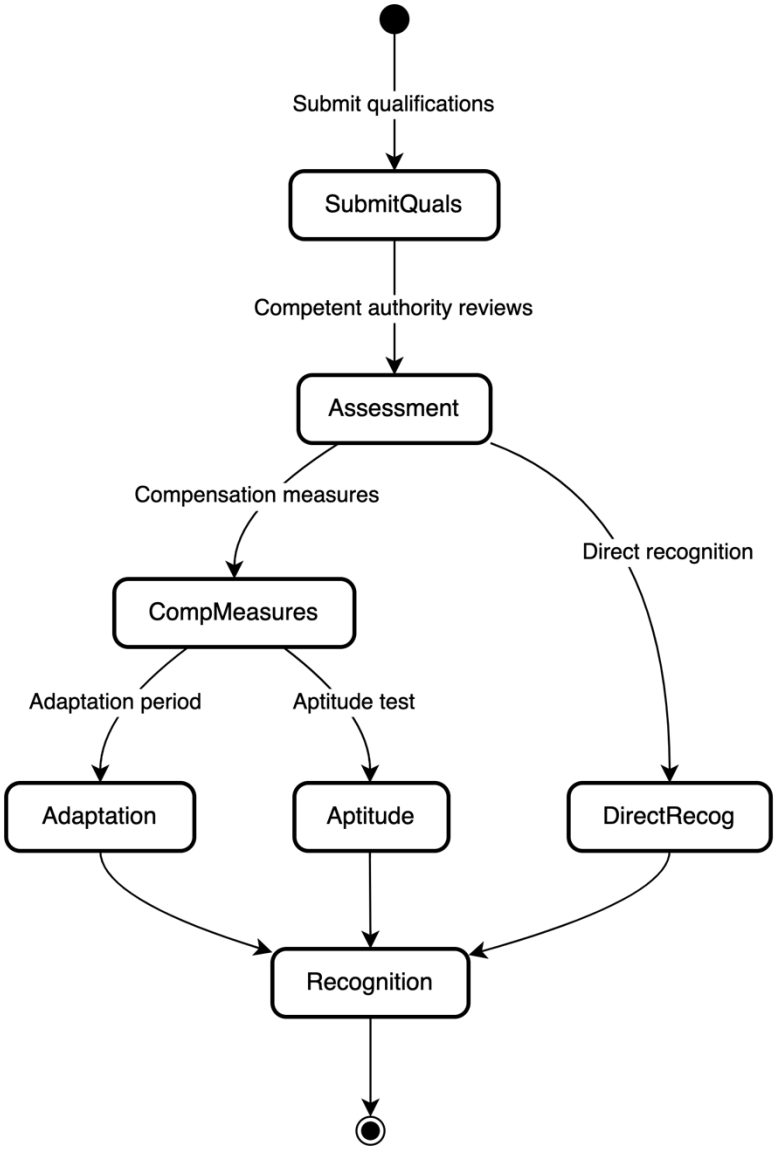
This diagram outlines the enrollment journey from initial application through credential verification to successful registration. It identifies key decision points, verification steps, and the final issuance of student credentials, showing how digital systems streamline traditional processes.




## 3.2 Professional Qualification Recognition

This diagram maps the various pathways for recognizing professional qualifications across borders. It shows assessment processes, compensation measures where needed, and the steps to achieve full recognition, illustrating how digital credentials facilitate professional mobility.

Co-funded by the European Union

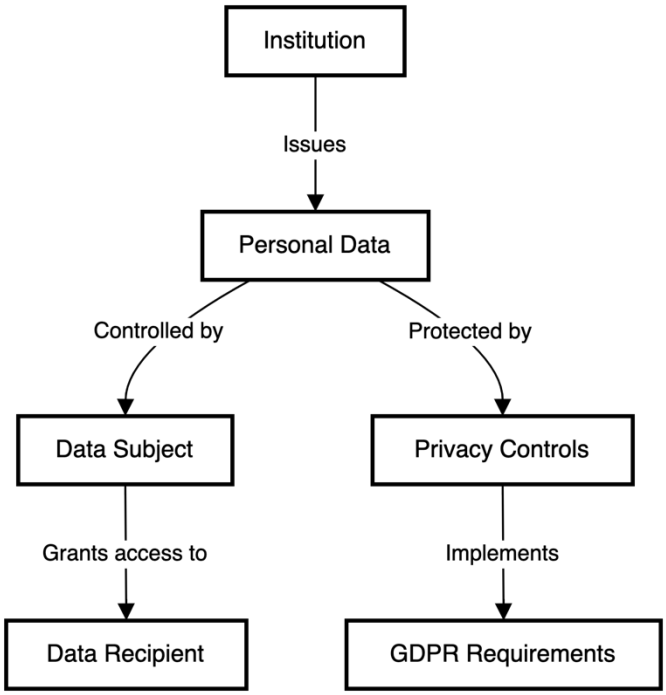



4. Data Protection and Privacy

4.1 Personal Data Flow Controls

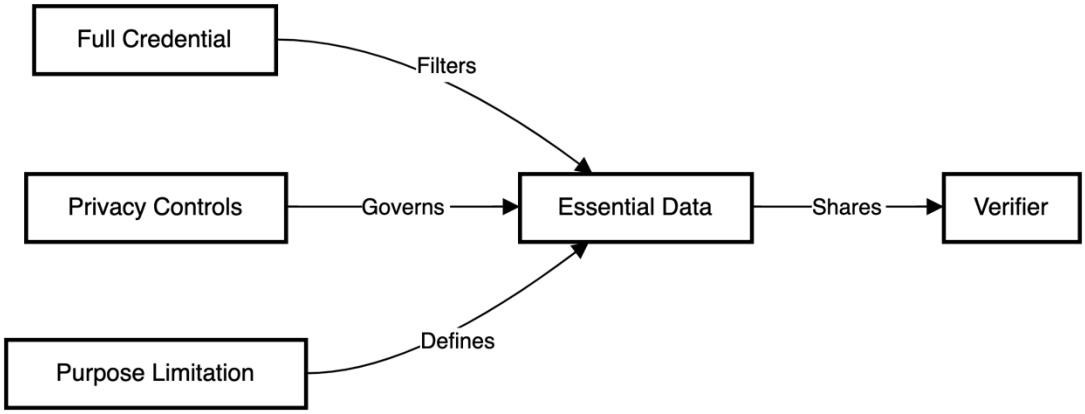
This diagram illustrates how personal data is protected throughout the credential ecosystem. It shows control points, authorization flows, and privacy protection measures, demonstrating compliance with data protection requirements while maintaining system functionality.

Co-funded by the European Union




4.2 Data Minimization Principle

This diagram demonstrates how the principle of data minimization is implemented in credential sharing. It shows how credentials can be filtered to share only essential information based on specific needs, supporting privacy while enabling verification.

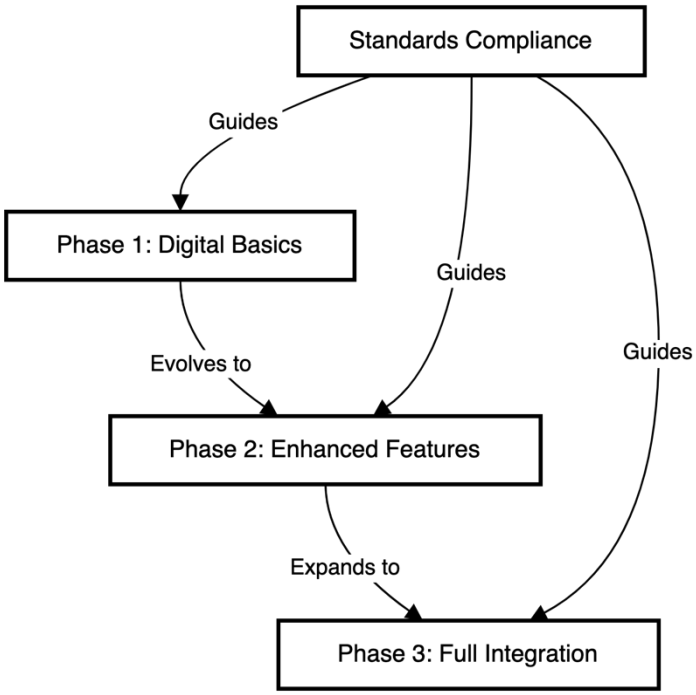



5. Implementation Guidelines

5.1 Phased Adoption Model

This diagram presents a structured approach to implementing digital credentials. It shows the progression from basic digital documentation through to full system integration, illustrating how organizations can manage the transition in controlled stages.

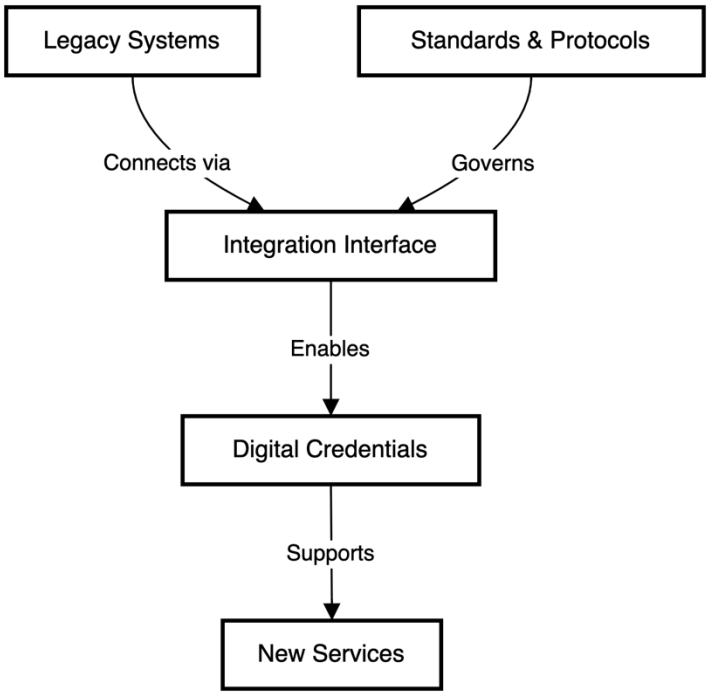
Co-funded by the European Union




5.2 Integration Patterns

This diagram shows how new digital credential systems can be integrated with existing educational management systems. It demonstrates the interfaces between legacy and new systems, showing how organizations can maintain continuity while modernizing their credential management. This model supports stakeholders in identifying integration best practices that enhance system resilience and operational efficiency.

Co-funded by the European Union




Co-funded by
the European Union

# Annex C: Data models

## *Introduction*

Standardized data models are fundamental building blocks in modern information systems, providing a consistent framework for data organization, storage, and exchange across different platforms and applications. Their implementation offers several key benefits:

1. Interoperability: Standardized data models enable seamless integration between different systems and stakeholders, reducing the complexity of data exchange and integration processes.
2. Data Quality: By establishing uniform data structures and relationships, these models help maintain data consistency and reduce errors that often arise from disparate data formats.
3. Efficiency: Development and maintenance costs are significantly reduced as standardized models eliminate the need for custom data mapping and transformation between systems.
4. Scalability: As organizations grow and evolve, standardized data models provide a stable foundation for system expansion and modification.

## *Structure and navigation*

This chapter presents four essential data models that form the backbone of our information architecture. Each model is designed to address specific business needs while maintaining consistency with the overall system architecture described in previous sections.

The data models covered in this chapter are:

1. AllianceID Data Model
2. Educational ID Data Model
3. MyAcademicId Data Model
4. European Learning Model (ELM) Data Model

Each data model section includes:

- Purpose and scope
- Entity relationships
- Attribute definitions
- Implementation considerations

## *Relationship to Previous Sections*

The data models presented in this annex build upon and support the concepts, requirements, and frameworks established in previous sections:

Co-funded by the European Union

- Connection to Chapter 2: European Education Landscape
  - The data models accommodate the diverse approaches to educational licensing and credential management described in Section 2.1
  - Support for both administrative and legislative approaches outlined in Section 2.4
  - Integration with electronic diploma issuance practices discussed in Section 2.7
  - Alignment with existing data models and ontologies covered in Section 2.9
- Alignment with Chapter 3: Current Challenges
  - Addresses credential issuance and verification challenges outlined in Section 3.1
  - Supports qualification recognition needs described in Section 3.2
  - Resolves data management and interoperability issues identified in Section 3.3
  - Accommodates stakeholder needs and concerns from Section 3.6
- Support for Chapter 4: Operational Model
  - Implements the trust model and governance framework detailed in Section 4.1
  - Enables credential lifecycle management processes outlined in Section 4.2
  - Supports roles and responsibilities defined in Section 4.3
  - Facilitates compliance monitoring requirements from Section 4.4
- Implementation of Chapter 5: Onboarding Processes
  - Provides data structures needed for educational onboarding (Section 5.1)
  - Supports professional qualifications onboarding (Section 5.2)
  - Enables secure credential issuance and management throughout onboarding
- Foundation for Chapter 6: Use Cases
  - Enables non-foundational identity scenarios from Section 6.7.1
  - Supports learning achievement use cases from Section 6.7.2
  - Facilitates professional qualification processes from Section 6.7.3
- Technical Framework Integration (Chapter 8)
  - Forms core component of technical architecture (Section 8.2)
  - Supports country-specific implementations (Section 8.4)
  - Enables maintenance and updates described in Section 8.6

These data models serve as the technical foundation that enables the business processes, governance frameworks, and user journeys described throughout the document. By implementing standardized formats based on W3C-VCDM and ELM specifications, they ensure interoperability while supporting the specific requirements of educational and professional credentialing across Europe.

Co-funded by the European Union

### *AllianceID Data Model*

#### Introduction

The Verifiable AllianceID is a JSON-schema based data model designed to represent and validate digital identifiers for natural persons participating in University Alliances. This data model implements the W3C Verifiable Credentials Data Model 1.1 specification, providing a standardized way to issue and verify digital credentials for alliance members.

Key benefits of this data model include:

- Standardized identification across European University Alliances
- Interoperability with abroad initiatives (e.g. OpenBadges)
- Flexible identifier scheme for different alliance contexts

#### Implementation Considerations

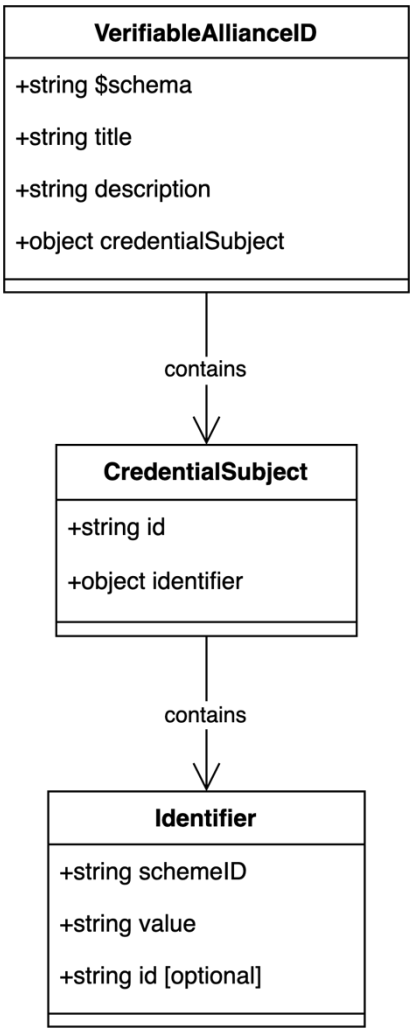
- Identifier Format
  - Validate identifier format: `urn:schac:europeanUniversityAllianceCode:int:euai:<sHO>:<code>`
  - Implement proper escaping for special characters
  - Consider backward compatibility with legacy systems
- Schema Inheritance
  - Handle proper extension of VCDM1.1 attestation schema
  - Implement validation for both base and extended schemas
  - Consider version management for schema updates

### *Field Specifications*

| Field | Path | Description | Type | Mandatory |
|---|---|---|---|---|
| **Schema Reference** | $schema | JSON Schema version reference | string | Yes |
| **Title** | title | Credential type identifier | string | Yes |
| **Credential Subject ID** | credentialSubject.id | Unique identifier of the credential subject | string | Yes |
| **Identifier** | credentialSubject.identifier | Container for alliance identification details | object | Yes |
| **Scheme ID** | credentialSubject.identifier.schemeID | Schema used for alternative identification | string | Yes |
| **Value** | credentialSubject.identifier.value | Alternative identification value | string | Yes |
| **Identifier URI** | credentialSubject.identifier.id | URI of the identifier | string (URI) | No |

Co-funded by the European Union

## Schema Structure Visualization




## JSON serialisation

```
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "Verifiable AllianceID",
 "description": "Schema of an EBSI Verifiable University Alliance ID for a natural person participating in the Alliance",
 "type": "object",
 "allOf": [
  {
   "$ref": "./node_modules/@cef-ebsi/vcdm1.1-attestation-schema/schema.json"
  },
  {
   "properties": {
    "credentialSubject": {
     "description": "Defines additional properties on credentialSubject to describe IDs that do not have a substantial level of assurance.",
     "type": "object",
     "properties": {
      "id": {
       "description": "Defines a unique identifier of the credential subject",
       "type": "string"
      },
      "identifier": {
       "type": "object",
       "description": "Defines the identifier for the University Alliance. Format: urn:schac:europeanUniversityAllianceCode:int:euai:<sHO>:<code>. sHO: the schacHomeOrganization of the Alliance that issued the credential, <code> the university alliance code",
```

```
          "$ref": "#/$defs/identifier"
        }
       },
       "required": ["id", "identifier"]
     }
    }
   }
  ],
  "$defs": {
   "identifier": {
    "description": "Defines an alternative Identifier object",
    "type": "object",
    "properties": {
     "schemeID": {
      "description": "Defines the schema used to define alternative identification",
      "type": "string"
     },
     "value": {
      "description": "Define the alternative identification value",
      "type": "string"
     },
     "id": {
      "description": "The URI of the identifier",
      "type": "string",
      "format": "uri"
     }
    },
    "required": ["schemeID", "value"]
   }
  }
 }
```


### *Educational ID Data Model*

#### Introduction

The Verifiable Educational ID is a comprehensive data model designed to represent educational identity credentials for natural persons participating in educational use cases. This model extends the VCDM1.1 attestation schema and incorporates standard educational attributes aligned with eduGAIN and SCHAC (SCHema for ACademia) specifications. It provides a robust framework for representing educational identities with various attributes including personal information, institutional affiliations, and identity assurance levels.

Key benefits:

- Standardized representation of educational identities across institutions
- Integration with existing educational identity frameworks (eduGAIN)
- Support for multiple affiliation types and roles
- Flexible identity assurance mechanisms

#### Implementation Considerations

- Identity Management
  - Implement proper handling of multiple affiliation types
  - Consider privacy implications of educational data
  - Manage credential expiration and renewal
- Data Validation
  - Validate email format and institutional domains

  - Implement proper date formatting (yyyyMMdd)
  - Handle multi-value fields (eduPersonAffiliation)
- Integration
  - Interface with eduGAIN infrastructure
  - Handle SCHAC attribute synchronization
  - Implement proper error handling for missing required fields

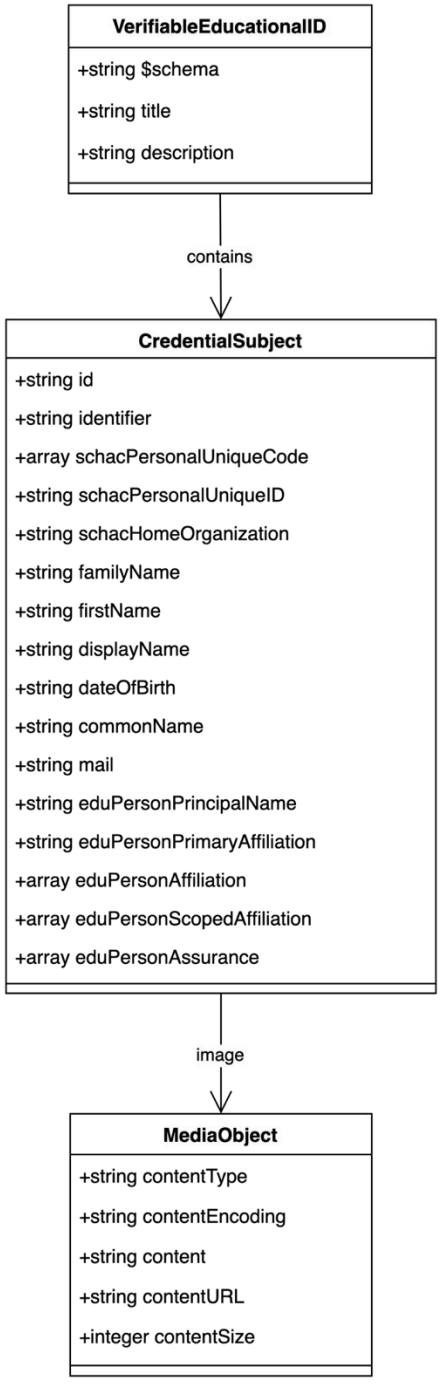
### Field Specifications

| Field | Path | Description | Type | Mandatory |
|---|---|---|---|---|
| **ID** | credentialSubject.id | DID:Key value generated by user wallet | string | Yes |
| **Identifier** | credentialSubject.identifier | Global unique identifier (eduPersonPrincipalName) | string | Yes |
| **Scoped Affiliation** | credentialSubject.eduPersonScopedAffiliation | Affiliations within Home Organization | array of strings | Yes |
| **Personal Unique Code** | credentialSubject.schacPersonalUniqueCode | Institution or country-specific unique codes | array of strings | No |
| **Personal Unique ID** | credentialSubject.schacPersonalUniqueID | Country-specific unique identifier | string | No |
| **Home Organization** | credentialSubject.schacHomeOrganization | Home institution identifier | string | No |
| **Family Name** | credentialSubject.familyName | Current family name(s) | string | No |
| **First Name** | credentialSubject.firstName | Current first name(s) | string | No |
| **Display Name** | credentialSubject.displayName | Name for white-pages applications | string | No |
| **Date of Birth** | credentialSubject.dateOfBirth | Birth date (yyyyMMdd format) | string (date) | No |
| **Common Name** | credentialSubject.commonName | Birth name | string | No |
| **Email** | credentialSubject.mail | Primary institutional email | string | No |
| **Principal Name** | credentialSubject.eduPersonPrincipalName | Unique persistent identifier | string | No |
| **Primary Affiliation** | credentialSubject.eduPersonPrimaryAffiliation | Primary role within organization | string | No |
| **Affiliations** | credentialSubject.eduPersonAffiliation | All roles within organization | array of strings | No |
| **Assurance** | credentialSubject.eduPersonAssurance | Identity assurance profiles | array of strings | No |

Co-funded by the European Union

| | | | | |
|---|---|---|---|---|
| **Image** | credentialSubject.image | Profile image data | Media Object | No |

## Schema Structure Visualization




## JSON serialisation

```
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "Verifiable Educational ID",
 "description": "Schema of a Verifiable Educational ID for a natural person participating in the educational use cases",
 "type": "object",
```

```
 "allOf": [
  {
   "$ref": "./node_modules/@cef-ebsi/vcdm1.1-attestation-schema/schema.json"
  },
  {
   "properties": {
    "credentialSubject": {
     "description": "Defines additional properties on credentialSubject to describe IDs that do not have a substantial level of assurance.",
     "type": "object",
     "properties": {
      "id": {
       "description": "Defines a unique identifier of the credential subject. DID:Key value, generated by the user wallet and associated to the credential holder. Refer specification available at https://api-pilot.ebsi.eu/docs/specs/did-methods/did-method-for-natural-person ",
       "type": "string"
      },
      "identifier": {
       "description": "Defines an alternative identifier for the credential subject and has as value the value of eduPersonPrincipalName attribute of the credential subject within the Home Organization (needs to be globally unique and persistent).",
       "type": "string"
      },
      "schacPersonalUniqueCode": {
       "description": " schacPersonalUniqueCode can have different forms urn:schac:personalUniqueCode:int:esi:<sHO>:<code> (where <sHO> is the Higher Education Institution's schacHomeOrganization) and urn:schac:personalUniqueCode:int:esi:<country-code>:<code> (<code> is a string that uniquely identifies the person).",
       "type": "array",
       "items": {
        "type": "string"
       }
      },
      "schacPersonalUniqueID": {
       "description": "value is different in different countries, mostly urn:schac:personalUniqueID:<country-code>:<code>.",
       "type": "string"
      },
      "schacHomeOrganization": {
       "description": "Specifies the home organization of the credential subject",
       "type": "string"
      },
      "familyName": {
       "description": "Defines current family name(s) of the credential subject which corresponds to the eduGAIN attribute sn",
       "type": "string"
      },
      "firstName": {
       "description": "Defines current first name(s) of the credential subject which corresponds to the eduGAIN attribute givenName",
       "type": "string"
      },
      "displayName": {
       "description": "The name(s) that should appear in white-pages-like applications",
       "type": "string"
      },
      "dateOfBirth": {
       "description": "Defines date of birth of the credential subject (format: yyyyMMdd)",
       "type": "string",
       "format": "date"
      },
      "commonName": {
       "description": "Defines the first and the family name(s) of the credential subject at the time of their birth",
       "type": "string"
      },
      "mail": {
       "description": "(primary) e-mail address of the credential subject as registered by the educational institution issuing the Verifiable Educational ID",
       "type": "string"
      },
      "eduPersonPrincipalName": {
```

```
          "description": "Unique, persistent identifier of the credential subject",
          "type": "string"
         },
         "eduPersonPrimaryAffiliation": {
          "description": "Primary Affiliation within Home Organization ",
          "type": "string"
         },
         "eduPersonAffiliation": {
          "description": "Affiliation within Home Organization. It can contain multiple values such as member, student, employee, faculty, staff, affiliate, alumni, etc.",
          "type": "array",
          "items": {
           "type": "string"
          }
         },
         "eduPersonScopedAffiliation": {
          "description": "The person's affiliations within Home Organization scoped with the Home Organization",
          "type": "array",
          "items": {
           "type": "string"
          }
         },
         "eduPersonAssurance": {
          "description": "represents identity assurance profiles (IAPs) https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0",
          "type": "array",
          "items": {
           "type": "string"
          }
         },
         "image": {
          "$ref": "#/$defs/MediaObjectType"
         }
        },
        "required": ["id", "identifier", "eduPersonScopedAffiliation"]
      }
     }
    }
  ],
  "$defs": {
   "URIType": {
    "type": "string",
    "format": "uri"
   },
   "StringType": {
    "type": "string"
   },
   "LiteralType": {
    "$ref": "#/$defs/StringType"
   },
   "IntegerType": {
    "type": "integer"
   },
   "GenericIdType": {
    "allOf": [
     {
      "$ref": "#/$defs/URIType"
     },
     {
      "if": {
       "type": "string",
       "pattern": "^(http|urn)"
      },
      "then": {
       "type": "string",
       "pattern": "^(http://data.europa.eu/snb/|http://publications.europa.eu/resource/authority/|urn:epass:.+:[0-9]+$|urn:epass:concept(Scheme)?:[0-9A-Za-z\\-]*$)"
      }
     }
```

```
    ]
   },
   "Many!LangStringType": {
    "type": "object",
    "propertyNames": {
     "pattern":
"^(aa|ab|ae|af|ak|am|an|ar|as|av|ay|az|ba|be|bg|bh|bi|bm|bn|bo|br|bs|ca|ce|ch|co|cr|cs|cu|cv|cy|da|de|dv|dz|ee|el|en|eo|es|et|
eu|fa|ff|fi|fj|fo|fr|fy|ga|gd|gl|gn|gu|gv|ha|he|hi|ho|hr|ht|hu|hy|hz|ia|id|ie|ig|ii|ik|in|io|is|it|iu|iw|ja|ji|jv|jw|ka|kg|ki|kj|kk|kl|km|kn|ko|kr|
ks|ku|kv|kw|ky|la|lb|lg|li|ln|lo|lt|lu|lv|mg|mh|mi|mk|ml|mn|mo|mr|ms|mt|my|na|nb|nd|ne|ng|nl|nn|no|nr|nv|ny|oc|oj|om|or|os|pa|
pi|pl|ps|pt|qu|rm|rn|ro|ru|rw|sa|sc|sd|se|sg|sh|si|sk|sl|sm|sn|so|sq|sr|ss|st|su|sv|sw|ta|te|tg|th|ti|tk|tl|tn|to|tr|ts|tt|tw|ty|ug|uk|ur|
uz|ve|vi|vo|wa|wo|xh|yi|yo|za|zh|zu)$"
    },
    "minProperties": 1
   },
   "ConceptSchemeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ConceptScheme"
     }
    },
    "required": []
   },
   "ConceptType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Concept"
     },
     "prefLabel": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "notation": {
      "$ref": "#/$defs/LiteralType"
     },
     "inScheme": {
      "$ref": "#/$defs/ConceptSchemeType"
     },
     "definition": {
      "$ref": "#/$defs/Many!LangStringType"
     }
    },
    "required": []
   },
   "MediaObjectType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "MediaObject"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "contentType": {
```

```
        "$ref": "#/$defs/ConceptType"
      },
      "attachmentType": {
        "$ref": "#/$defs/ConceptType"
      },
      "contentEncoding": {
        "$ref": "#/$defs/ConceptType"
      },
      "contentSize": {
        "$ref": "#/$defs/IntegerType"
      },
      "content": {
        "$ref": "#/$defs/StringType"
      },
      "contentURL": {
        "$ref": "#/$defs/URIType"
      }
    },
    "required": ["contentType", "contentEncoding", "content"]
  }
 }
}
```


### *MyAcademicId Data Model*

#### Introduction

The MyAcademicId data model defines a schema for verifiable credentials specifically designed for academic identity management across European educational institutions. This model implements the eduPerson standard attributes and incorporates the European Student Identifier (ESI) framework, making it particularly valuable for academic mobility and cross-institutional identity management.

Key benefits:

- Standardized academic identity representation across European institutions
- Support for student mobility through European Student Identifier (ESI)
- Integration with REFEDS Assurance Framework (RAF)
- Compatibility with eduPerson attribute schema
- Persistent and non-revocable identification through community identifiers

#### Implementation Considerations

- Identifier Management
  - Implement hex-based identifier generation (64 digits max)
  - Ensure identifier uniqueness within erasmus.eduteams.org scope
  - Handle identifier persistence requirements
- Affiliation Handling
  - Validate affiliation syntax against eduPerson standard
  - Implement proper scope handling for affiliations
  - Manage multiple organization affiliations
- Integration Requirements
  - Interface with REFEDS Assurance Framework
  - Handle proper URI formatting for assurance values
  - Implement proper ESI lifecycle management

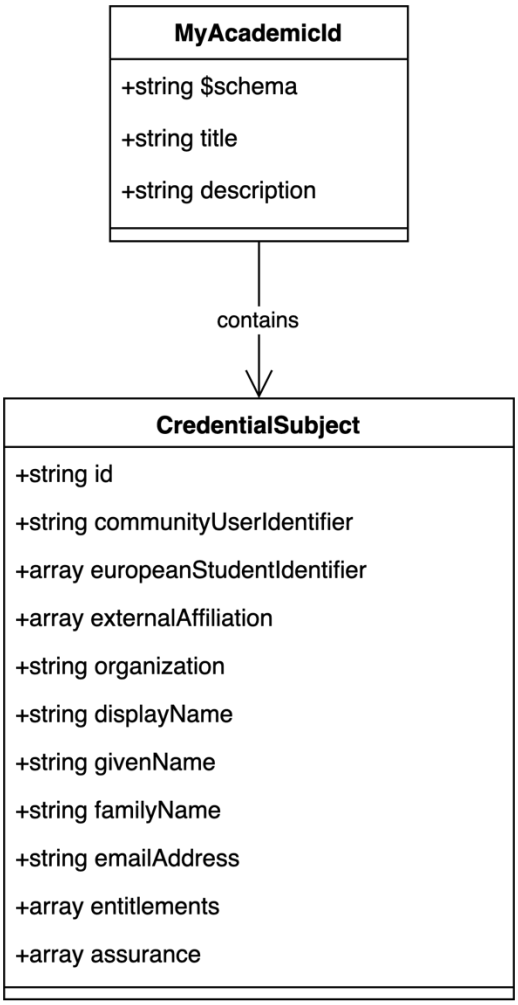
Co-funded by the European Union

### Field Specifications

| Field | Path | Description | Type | Mandatory |
|---|---|---|---|---|
| **ID** | credentialSubject.id | User's DID identifier | string | Yes |
| **Community User ID** | credentialSubject.communityUserIdentifier | Unique, persistent identifier in MyAcademicId namespace | string | Yes |
| **Display Name** | credentialSubject.displayName | User's full name (firstname lastname) | string | Yes |
| **Given Name** | credentialSubject.givenName | User's given name(s) | string | Yes |
| **Family Name** | credentialSubject.familyName | User's surname(s) | string | Yes |
| **Email Address** | credentialSubject.emailAddress | User's email address | string (email) | Yes |
| **Assurance** | credentialSubject.assurance | Identity assurance levels (RAF) | array of URIs | Yes |
| **European Student ID** | credentialSubject.europeanStudentIdentifier | ESI for student mobility | array of strings | No |
| **External Affiliation** | credentialSubject.externalAffiliation | Affiliations with home organizations | array of strings | No |
| **Organization** | credentialSubject.organization | User's primary organization | string | No |
| **Entitlements** | credentialSubject.entitlements | User's rights and privileges | array of strings | No |

Co-funded by the European Union

## Schema Structure Visualization




## JSON serialisation


```
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "MyAcademicId",
 "description": "Schema of an MyAcademicId Verifiable Credential",
 "type": "object",
 "allOf": [
  {
   "$ref": "./node_modules/@cef-ebsi/vcdm1.1-attestation-schema/schema.json"
  },
  {
   "properties": {
    "credentialSubject": {
     "description": "Defines additional properties on credentialSubject to describe IDs that do not have a substantial level of assurance.",
     "type": "object",
     "properties": {
      "id": {
       "description": "Defines a unique identifier of the credential subject. DID of the user",
       "type": "string"
      },
      "communityUserIdentifier": {
       "description": "User's Community Identifier is an opaque and non-revocable identifier (i.e. it cannot change over time) that follows the syntax of eduPersonUniqueId attribute of eduPerson. It consists of "uniqueID" part and fixed scope "erasmus.eduteams.org", separated by at sign. The uniqueID part contains up to 64 hexadecimal digits (a-f, 0-9). The identifier is
```

unique and persistent within the MyAcademicId namespace. The identifier can be used for identity matching, etc. OID: 1.3.6.1.4.1.5923.1.1.1.13 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-eduPersonUniqueId",
"type": "string"
},
"europeanStudentIdentifier": {
"description": "The European Student Identifier (ESI) of the user. ESI ensures mobility. Lifetime is limited to the period of student's mobility. ESI structure is defined in the document referenced below. ESI SHOULD NOT be parsed to extract information about the originating organisation of the student since the identifier structure is subject to a change. OID: 1.3.6.1.4.1.25178.1.2.14 Definition: https: //wiki.geant.org/display/SM/European+Student+Identifier",
"type": "array",
"items": {
"type": "string"
}
},
"externalAffiliation": {
"description": "Affiliation within Home Organization. One or more home organisations (such as, universities, research institutions or private companies) this user is affiliated with. The syntax and semantics follows eduPersonScopedAffiliation attribute. Affiliation is external to the MyAcademicId. OID: 1.3.6.1.4.1.25178.4.1.11 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-eduPersonScopedAffiliation",
"type": "array",
"items": {
"type": "string"
}
},
"organization": {
"description": "This attribute describes the organization of this user. OID: 1.3.6.1.4.1.25178.1.2.9",
"type": "string"
},
"displayName": {
"description": "User's name (firstname lastname). For more complex names. OID: 2.16.840.1.113730.3.1.241 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-displayName",
"type": "string"
},
"givenName": {
"description": "strings that are the part of a person's name that is not their surname (see RFC4519). OID: 2.5.4.Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-givenName",
"type": "string"
},
"familyName": {
"description": "strings that are a person's surname (see RFC4519). OID: 2.5.4.4 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-sn",
"type": "string"
},
"emailAddress": {
"description": "address of the user. OID: 0.9.2342.19200300.100.1.3 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-homePostalAddress",
"type": "string",
"format": "email"
},
"entitlements": {
"description": "This attribute describes the entitlements of this user. OID: 1.3.6.1.4.1.5923.1.1.1.7 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-eduPersonEntitlement",
"type": "array",
"items": {
"type": "string"
}
},
"assurance": {
"description": "Assurance of the identity of the user, following REFEDS Assurance Framework (RAF). OID: 1.3.6.1.4.1.5923.1.1.1.11 Definition: https: //wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-eduPersonAssurance",
"type": "array",
"items": {
"type": "string",
"format": "uri"
}
}
},

```
        "required": [
          "id",
          "communityUserIdentifier",
          "displayName",
          "givenName",
          "familyName",
          "emailAddress",
          "assurance"
        ]
      }
    }
  }
 ]
}
```

### *European Learning Model (ELM) Data Model*

#### Introduction

The Europass EDC schema defines the structure for European Digital Credentials based on ELM (European Learning Model) 3.2. This comprehensive data model implements the W3C Verifiable Credentials Data Model and provides a standardized way to represent educational credentials in the European context.

Key benefits:

- Full compliance with European Learning Model 3.2
- Support for multilingual content
- Rich metadata for credential display and verification
- Comprehensive learning outcome documentation
- Flexible credential profiling system
- Support for multiple assessment and grading schemes
- Integration with European educational frameworks

#### Implementation Considerations

- Multilingual Support
  - Implement proper language tag handling
  - Handle right-to-left script requirements
  - Manage translation consistency
- Display Requirements
  - Implement proper rendering of credential displays
  - Handle different device and format requirements
  - Manage credential visualization standards
- Technical Integration
  - Interface with European Learning Model
  - Handle proper version management
  - Implement assessment and grading schemes

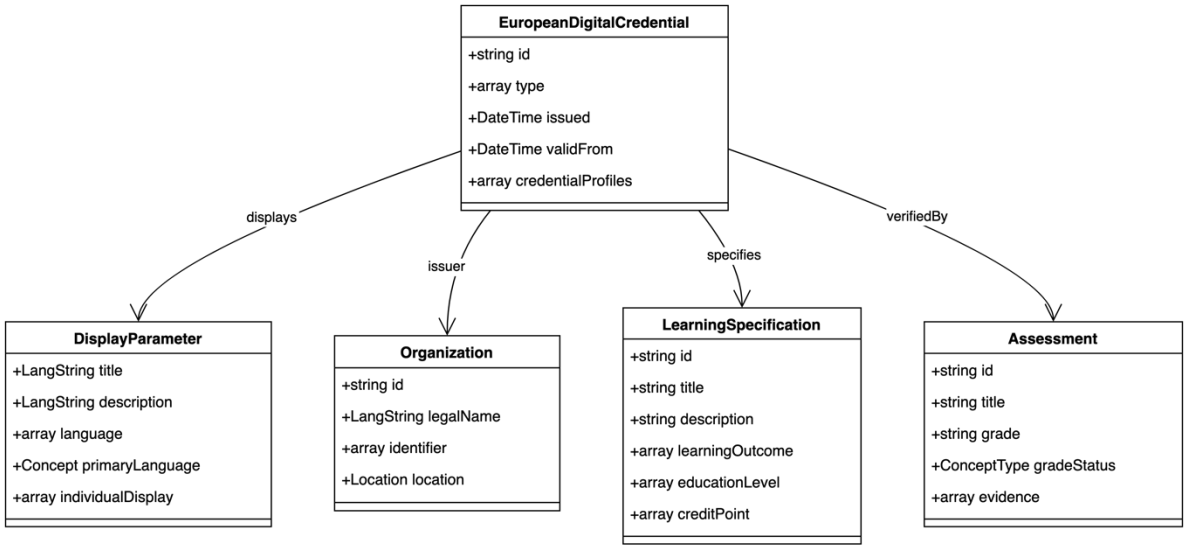
Co-funded by the European Union

### Field Specifications

| Field | Path | Description | Type | Mandatory |
|---|---|---|---|---|
| **Credential Profiles** | credentialProfiles | Defines the credential's classification | ConceptType array | Yes |
| **Display Parameter** | displayParameter | Visual presentation parameters | DisplayParameterType | Yes |
| **Issuer** | issuer | Credential issuing organization | Agent/Person/Organization | Yes |
| **Credential Subject** | credentialSubject | The recipient of the credential | Agent/Person/Organization | Yes |
| **Issue Date** | issued | Credential issuance date | DateTime | Yes |
| **Valid From** | validFrom | Credential validity start date | DateTime | Yes |
| **Credential Schema** | credentialSchema | Schema validation information | CredentialSchemaType | Yes |
| **Identifier** | identifier | Credential unique identifiers | Identifier/LegalIdentifier | No |
| **Attachment** | attachment | Associated media objects | MediaObject array | No |
| **Expiration Date** | expirationDate | Credential expiry date | DateTime | No |
| **Evidence** | evidence | Supporting evidence | EvidenceType array | No |
| **Terms of Use** | termsOfUse | Usage conditions | TermsOfUseType array | No |
| **Credential Status** | credentialStatus | Verification status | CredentialStatusType | No |
| **Proof** | proof | Cryptographic proof | ProofType array | No |

Co-funded by the European Union

## Schema Structure Visualization




## JSON serialisation

```
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "Europass EDC credential",
 "description": "Schema for EDC credential based on ELM 3.2",
 "type": "object",
 "allOf": [
  {
   "$ref": "./node_modules/@cef-ebsi/vcdm1.1-attestation-schema/schema.json"
  },
  {
   "$ref": "#/$defs/EuropeanDigitalCredentialType"
  }
 ],
 "$defs": {
  "CredentialSubjectType": {
   "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
  },
  "IntegerType": {
   "type": "integer"
  },
  "PositiveIntegerType": {
   "type": "integer",
   "minimum": 0
  },
  "PercentageIntegerType": {
   "type": "integer",
   "minimum": 0,
   "maximum": 100
  },
  "DecimalType": {
   "type": "number"
  },
  "BooleanType": {
   "type": "boolean"
  },
  "IRIType": {
   "type": "string"
  },
  "URIType": {
   "type": "string",
```

```
    "format": "uri"
   },
   "Many!HTMLType": {
    "anyOf": [
     {
      "$ref": "#/$defs/HTMLType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/HTMLType"
      }
     }
    ]
   },
   "HTMLType": {
    "type": "string"
   },
   "DateTimeType": {
    "type": "string",
    "format": "date-time"
   },
   "EmailType": {
    "type": "string",
    "anyOf": [
     {
      "format": "email"
     },
     {
      "format": "uri",
      "pattern": "^mailto:[^@]*[^\\.]@[^\\.]($|[^@]*[^\\.]$)"
     }
    ]
   },
   "DurationType": {
    "type": "string",
    "format": "duration"
   },
   "Many!PeriodOfTimeType": {
    "anyOf": [
     {
      "$ref": "#/$defs/PeriodOfTimeType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/PeriodOfTimeType"
      }
     }
    ]
   },
   "PeriodOfTimeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "PeriodOfTime"
     },
     "startDate": {
      "$ref": "#/$defs/DateTimeType"
     },
     "endDate": {
      "$ref": "#/$defs/DateTimeType"
     },
     "prefLabel": {
      "$ref": "#/$defs/Many!LangStringType"
```

```
    }
   },
   "required": []
  },
  "Many!StringType": {
   "anyOf": [
    {
     "$ref": "#/$defs/StringType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/StringType"
     }
    }
   ]
  },
  "StringType": {
   "type": "string"
  },
  "GenericIdType": {
   "$ref": "#/$defs/URIType"
  },
  "LiteralType": {
   "$ref": "#/$defs/StringType"
  },
  "Many!AgentType": {
   "anyOf": [
    {
     "$ref": "#/$defs/AgentType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/AgentType"
     }
    }
   ]
  },
  "AgentType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "Agent"
    },
    "identifier": {
     "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
    },
    "altLabel": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "prefLabel": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "location": {
     "$ref": "#/$defs/Many!LocationType"
    },
    "contactPoint": {
     "$ref": "#/$defs/Many!ContactPointType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
    "groupMemberOf": {
     "$ref": "#/$defs/Many!GroupType"
```

```
    },
    "dateModified": {
      "$ref": "#/$defs/DateTimeType"
    }
   },
   "required": []
  },
  "Many!PersonType": {
   "anyOf": [
    {
     "$ref": "#/$defs/PersonType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/PersonType"
     }
    }
   ]
  },
  "PersonType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "Person"
    },
    "identifier": {
     "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
    },
    "location": {
     "$ref": "#/$defs/LocationType"
    },
    "nationalID": {
     "$ref": "#/$defs/LegalIdentifierType"
    },
    "fullName": {
     "$ref": "#/$defs/LangStringType"
    },
    "givenName": {
     "$ref": "#/$defs/LangStringType"
    },
    "familyName": {
     "$ref": "#/$defs/LangStringType"
    },
    "birthName": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "patronymicName": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "memberOf": {
     "$ref": "#/$defs/Many!OrganisationType"
    },
    "dateOfBirth": {
     "$ref": "#/$defs/DateTimeType"
    },
    "placeOfBirth": {
     "$ref": "#/$defs/LocationType"
    },
    "citizenshipCountry": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "gender": {
     "$ref": "#/$defs/ConceptType"
    },
```

```
    "contactPoint": {
     "$ref": "#/$defs/Many!ContactPointType"
    },
    "groupMemberOf": {
     "$ref": "#/$defs/Many!GroupType"
    },
    "dateModified": {
     "$ref": "#/$defs/DateTimeType"
    },
    "hasCredential": {
     "$ref": "#/$defs/Many!EuropeanDigitalCredentialType"
    },
    "hasClaim": {
     "$ref": "#/$defs/Many!ClaimNodeType"
    }
   },
   "required": []
  },
  "Many!EuropeanDigitalCredentialType": {
   "anyOf": [
    {
     "$ref": "#/$defs/EuropeanDigitalCredentialType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/EuropeanDigitalCredentialType"
     }
    }
   ]
  },
  "Many!ClaimNodeType": {
   "anyOf": [
    {
     "$ref": "#/$defs/ClaimNodeType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/ClaimNodeType"
     }
    }
   ]
  },
  "ClaimNodeType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningAchievementType"
    },
    {
     "$ref": "#/$defs/LearningActivityType"
    },
    {
     "$ref": "#/$defs/LearningAssessmentType"
    },
    {
     "$ref": "#/$defs/LearningEntitlementType"
    },
    {
     "$ref": "#/$defs/ClaimTypeNodeType"
    }
   ]
  },
  "Many!OrganisationType": {
   "anyOf": [
    {
     "$ref": "#/$defs/OrganisationType"
    },
    {
```

```
      "type": "array",
      "items": {
       "$ref": "#/$defs/OrganisationType"
      }
     }
    ]
   },
   "OrganisationType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Organisation"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "altLabel": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "homepage": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "location": {
      "$ref": "#/$defs/Many!LocationType"
     },
     "accreditation": {
      "$ref": "#/$defs/Many!AccreditationType"
     },
     "eIDASIdentifier": {
      "$ref": "#/$defs/LegalIdentifierType"
     },
     "registration": {
      "$ref": "#/$defs/LegalIdentifierType"
     },
     "legalName": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "vatIdentifier": {
      "$ref": "#/$defs/Many!LegalIdentifierType"
     },
     "taxIdentifier": {
      "$ref": "#/$defs/Many!LegalIdentifierType"
     },
     "logo": {
      "$ref": "#/$defs/MediaObjectType"
     },
     "hasSubOrganization": {
      "$ref": "#/$defs/Many!OrganisationType"
     },
     "subOrganizationOf": {
      "$ref": "#/$defs/OrganisationType"
     },
     "hasMember": {
      "$ref": "#/$defs/Many!PersonType"
     },
     "groupMemberOf": {
      "$ref": "#/$defs/Many!GroupType"
     },
     "contactPoint": {
```

```
      "$ref": "#/$defs/Many!ContactPointType"
     },
     "dateModified": {
      "$ref": "#/$defs/DateTimeType"
     }
    },
    "required": ["legalName", "location"]
   },
   "MediaObjectType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "MediaObject"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "contentType": {
      "$ref": "#/$defs/ConceptType"
     },
     "attachmentType": {
      "$ref": "#/$defs/ConceptType"
     },
     "contentEncoding": {
      "$ref": "#/$defs/ConceptType"
     },
     "contentSize": {
      "$ref": "#/$defs/IntegerType"
     },
     "content": {
      "$ref": "#/$defs/StringType"
     },
     "contentURL": {
      "$ref": "#/$defs/URIType"
     }
    },
    "required": ["contentType", "contentEncoding", "content"]
   },
   "Many!AccreditationType": {
    "anyOf": [
     {
      "$ref": "#/$defs/AccreditationType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/AccreditationType"
      }
     }
    ]
   },
   "Many!IssuerNodeType": {
    "anyOf": [
     {
      "$ref": "#/$defs/IssuerNodeType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/IssuerNodeType"
      }
     }
```

```
    ]
   },
   "IssuerNodeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "IssuerNode"
     },
     "eidasLegalIdentifier": {
      "$ref": "#/$defs/LegalIdentifierType"
     }
    },
    "required": ["eidasLegalIdentifier"]
   },
   "AccreditationType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Accreditation"
     },
     "dcType": {
      "$ref": "#/$defs/ConceptType"
     },
     "identifier": {
      "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "homepage": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "dateIssued": {
      "$ref": "#/$defs/DateTimeType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "decision": {
      "$ref": "#/$defs/ConceptType"
     },
     "report": {
      "$ref": "#/$defs/WebResourceType"
     },
     "organisation": {
      "$ref": "#/$defs/Many!OrganisationType"
     },
     "limitQualification": {
      "$ref": "#/$defs/QualificationType"
     },
     "limitField": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "limitEQFLevel": {
      "$ref": "#/$defs/Many!ConceptType"
```

```
    },
    "limitJurisdiction": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "limitCredentialType": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "accreditingAgent": {
      "$ref": "#/$defs/OrganisationType"
    },
    "reviewDate": {
      "$ref": "#/$defs/DateTimeType"
    },
    "expiryDate": {
      "$ref": "#/$defs/DateTimeType"
    },
    "landingPage": {
      "$ref": "#/$defs/Many!WebResourceType"
    },
    "status": {
      "$ref": "#/$defs/StringType"
    },
    "dateModified": {
      "$ref": "#/$defs/DateTimeType"
    }
   },
   "required": ["title", "accreditingAgent", "dcType"]
  },
  "Many!QualificationType": {
   "anyOf": [
    {
      "$ref": "#/$defs/QualificationType"
    },
    {
      "type": "array",
      "items": {
        "$ref": "#/$defs/QualificationType"
      }
    }
   ]
  },
  "QualificationType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
      "$ref": "#/$defs/GenericIdType"
    },
    "type": {
      "const": "Qualification"
    },
    "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "identifier": {
      "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
    },
    "title": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
    },
    "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
    },
```

```
"homepage": {
 "$ref": "#/$defs/Many!WebResourceType"
},
"altLabel": {
 "$ref": "#/$defs/Many!LangStringType"
},
"category": {
 "$ref": "#/$defs/Many!LangStringType"
},
"dateModified": {
 "$ref": "#/$defs/DateTimeType"
},
"language": {
 "$ref": "#/$defs/Many!ConceptType"
},
"volumeOfLearning": {
 "$ref": "#/$defs/DurationType"
},
"mode": {
 "$ref": "#/$defs/Many!ConceptType"
},
"learningOutcomeSummary": {
 "$ref": "#/$defs/NoteType"
},
"thematicArea": {
 "$ref": "#/$defs/Many!ConceptType"
},
"educationSubject": {
 "$ref": "#/$defs/Many!ConceptType"
},
"creditPoint": {
 "$ref": "#/$defs/Many!CreditPointType"
},
"educationLevel": {
 "$ref": "#/$defs/Many!ConceptType"
},
"learningSetting": {
 "$ref": "#/$defs/ConceptType"
},
"maximumDuration": {
 "$ref": "#/$defs/DurationType"
},
"targetGroup": {
 "$ref": "#/$defs/Many!ConceptType"
},
"entryRequirement": {
 "$ref": "#/$defs/NoteType"
},
"learningOutcome": {
 "$ref": "#/$defs/Many!LearningOutcomeType"
},
"influencedBy": {
 "$ref": "#/$defs/Many!LearningActivitySpecificationType"
},
"provenBy": {
 "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
},
"entitlesTo": {
 "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
},
"awardingOpportunity": {
 "$ref": "#/$defs/Many!AwardingOpportunityType"
},
"hasPart": {
 "$ref": "#/$defs/Many!QualificationType"
},
"isPartOf": {
 "$ref": "#/$defs/Many!QualificationType"
},
```


Co-funded by the European Union

```
    "specialisationOf": {
     "$ref": "#/$defs/Many!QualificationType"
    },
    "generalisationOf": {
     "$ref": "#/$defs/Many!QualificationType"
    },
    "isPartialQualification": {
     "$ref": "#/$defs/BooleanType"
    },
    "eqfLevel": {
     "$ref": "#/$defs/ConceptType"
    },
    "nqfLevel": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "accreditation": {
     "$ref": "#/$defs/Many!AccreditationType"
    },
    "qualificationCode": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "status": {
     "$ref": "#/$defs/StringType"
    }
   },
   "required": ["title"]
  },
  "Many!LearningOutcomeType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningOutcomeType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/LearningOutcomeType"
     }
    }
   ]
  },
  "LearningOutcomeType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "LearningOutcome"
    },
    "dcType": {
     "$ref": "#/$defs/ConceptType"
    },
    "identifier": {
     "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
    },
    "title": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
    "reusabilityLevel": {
     "$ref": "#/$defs/ConceptType"
    },
    "relatedSkill": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "relatedESCOSkill": {
```


Co-funded by the European Union

```
      "$ref": "#/$defs/Many!ConceptType"
     }
    },
    "required": ["title"]
   },
   "Many!ContactPointType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ContactPointType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ContactPointType"
      }
     }
    ]
   },
   "ContactPointType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ContactPoint"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "address": {
      "$ref": "#/$defs/Many!AddressType"
     },
     "phone": {
      "$ref": "#/$defs/Many!PhoneType"
     },
     "emailAddress": {
      "$ref": "#/$defs/Many!MailboxType"
     },
     "contactForm": {
      "$ref": "#/$defs/Many!WebResourceType"
     }
    },
    "required": []
   },
   "Many!NoteType": {
    "anyOf": [
     {
      "$ref": "#/$defs/NoteType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/NoteType"
      }
     }
    ]
   },
   "NoteType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
```

```
    "type": {
     "const": "Note"
    },
    "noteLiteral": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "subject": {
     "$ref": "#/$defs/ConceptType"
    },
    "noteFormat": {
     "$ref": "#/$defs/ConceptType"
    }
   },
   "required": ["noteLiteral"]
  },
  "Many!AddressType": {
   "anyOf": [
    {
     "$ref": "#/$defs/AddressType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/AddressType"
     }
    }
   ]
  },
  "AddressType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "Address"
    },
    "identifier": {
     "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
    },
    "fullAddress": {
     "$ref": "#/$defs/NoteType"
    },
    "countryCode": {
     "$ref": "#/$defs/ConceptType"
    }
   },
   "required": ["countryCode"]
  },
  "Many!PhoneType": {
   "anyOf": [
    {
     "$ref": "#/$defs/PhoneType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/PhoneType"
     }
    }
   ]
  },
  "PhoneType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
```

```
    },
    "type": {
     "const": "Phone"
    },
    "phoneNumber": {
     "$ref": "#/$defs/StringType"
    },
    "countryDialing": {
     "$ref": "#/$defs/StringType"
    },
    "areaDialing": {
     "$ref": "#/$defs/StringType"
    },
    "dialNumber": {
     "$ref": "#/$defs/StringType"
    }
   },
   "required": []
  },
  "Many!MailboxType": {
   "anyOf": [
    {
     "$ref": "#/$defs/MailboxType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/MailboxType"
     }
    }
   ]
  },
  "MailboxType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/EmailType"
    },
    "type": {
     "const": "Mailbox"
    }
   },
   "required": []
  },
  "Many!WebResourceType": {
   "anyOf": [
    {
     "$ref": "#/$defs/WebResourceType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/WebResourceType"
     }
    }
   ]
  },
  "WebResourceType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "WebResource"
    },
    "title": {
```

```
      "$ref": "#/$defs/Many!LangStringType"
     },
     "language": {
      "$ref": "#/$defs/ConceptType"
     },
     "contentURL": {
      "$ref": "#/$defs/URIType"
     }
    },
    "required": ["contentURL"]
   },
   "Many!ConceptType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ConceptType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ConceptType"
      }
     }
    ]
   },
   "Single!ConceptType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ConceptType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ConceptType"
      },
      "minItems": 1,
      "maxItems": 1
     }
    ]
   },
   "ConceptType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Concept"
     },
     "prefLabel": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "notation": {
      "$ref": "#/$defs/LiteralType"
     },
     "inScheme": {
      "$ref": "#/$defs/ConceptSchemeType"
     },
     "definition": {
      "$ref": "#/$defs/Many!LangStringType"
     }
    },
    "required": []
   },
   "ConceptSchemeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
```

```
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ConceptScheme"
     }
    },
    "required": []
   },
   "Many!LocationType": {
    "anyOf": [
     {
      "$ref": "#/$defs/LocationType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/LocationType"
      }
     }
    ]
   },
   "LocationType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Location"
     },
     "identifier": {
      "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "address": {
      "$ref": "#/$defs/Many!AddressType"
     },
     "geographicName": {
      "$ref": "#/$defs/Many!AddressType"
     },
     "spatialCode": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "geometry": {
      "$ref": "#/$defs/Many!GeometryType"
     }
    },
    "required": ["address"]
   },
   "Many!GeometryType": {
    "anyOf": [
     {
      "$ref": "#/$defs/GeometryType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/GeometryType"
      }
     }
    ]
   },
   "GeometryType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
```

```
    "id": {
      "$ref": "#/$defs/GenericIdType"
    },
    "type": {
      "const": "Geometry"
    },
    "longitude": {
      "$ref": "#/$defs/StringType"
    },
    "latitude": {
      "$ref": "#/$defs/StringType"
    }
  },
  "required": []
},
"Many!GroupType": {
  "anyOf": [
    {
      "$ref": "#/$defs/GroupType"
    },
    {
      "type": "array",
      "items": {
        "$ref": "#/$defs/GroupType"
      }
    }
  ]
},
"GroupType": {
  "type": "object",
  "additionalProperties": false,
  "properties": {
    "id": {
      "$ref": "#/$defs/GenericIdType"
    },
    "type": {
      "const": "Group"
    },
    "prefLabel": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "altLabel": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
    },
    "location": {
      "$ref": "#/$defs/Many!LocationType"
    },
    "contactPoint": {
      "$ref": "#/$defs/Many!ContactPointType"
    },
    "member": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
    }
  },
  "required": ["prefLabel"]
},
"Many!AgentOrPersonOrOrganisationType": {
  "anyOf": [
    {
      "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
    },
    {
      "type": "array",
      "items": {
        "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
      }
```

```
    }
   ]
  },
  "AgentOrPersonOrOrganisationType": {
   "anyOf": [
    {
     "$ref": "#/$defs/AgentType"
    },
    {
     "$ref": "#/$defs/PersonType"
    },
    {
     "$ref": "#/$defs/OrganisationType"
    }
   ]
  },
  "LearningAchievementSpecificationOrSpecificationType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningAchievementSpecificationType"
    },
    {
     "$ref": "#/$defs/QualificationType"
    }
   ]
  },
  "IdentifierOrLegalIdentifierType": {
   "anyOf": [
    {
     "$ref": "#/$defs/IdentifierType"
    },
    {
     "$ref": "#/$defs/LegalIdentifierType"
    }
   ]
  },
  "Many!IdentifierType": {
   "anyOf": [
    {
     "$ref": "#/$defs/IdentifierType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/IdentifierType"
     }
    }
   ]
  },
  "IdentifierType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "Identifier"
    },
    "dcType": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "notation": {
     "$ref": "#/$defs/LiteralType"
    },
    "schemeAgency": {
     "$ref": "#/$defs/LangStringType"
    },
    "creator": {
```

```
      "$ref": "#/$defs/IRIType"
     },
     "dateIssued": {
      "$ref": "#/$defs/DateTimeType"
     },
     "schemeName": {
      "$ref": "#/$defs/StringType"
     },
     "schemeVersion": {
      "$ref": "#/$defs/StringType"
     },
     "schemeId": {
      "$ref": "#/$defs/URIType"
     }
    },
    "required": ["notation"]
   },
   "Many!LegalIdentifierType": {
    "anyOf": [
     {
      "$ref": "#/$defs/LegalIdentifierType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/LegalIdentifierType"
      }
     }
    ]
   },
   "LegalIdentifierType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LegalIdentifier"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "notation": {
      "$ref": "#/$defs/LiteralType"
     },
     "schemeAgency": {
      "$ref": "#/$defs/LangStringType"
     },
     "creator": {
      "$ref": "#/$defs/IRIType"
     },
     "dateIssued": {
      "$ref": "#/$defs/DateTimeType"
     },
     "schemeName": {
      "$ref": "#/$defs/StringType"
     },
     "schemeVersion": {
      "$ref": "#/$defs/StringType"
     },
     "schemeId": {
      "$ref": "#/$defs/URIType"
     },
     "spatial": {
      "$ref": "#/$defs/ConceptType"
     }
    },
    "required": ["notation", "spatial"]
```

```
  },
  "Many!CreditPointType": {
   "anyOf": [
    {
     "$ref": "#/$defs/CreditPointType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/CreditPointType"
     }
    }
   ]
  },
  "CreditPointType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "CreditPoint"
    },
    "framework": {
     "$ref": "#/$defs/ConceptType"
    },
    "point": {
     "$ref": "#/$defs/StringType"
    }
   },
   "required": ["framework", "point"]
  },
  "AmountType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "Amount"
    },
    "unit": {
     "$ref": "#/$defs/ConceptType"
    },
    "value": {
     "$ref": "#/$defs/DecimalType"
    }
   },
   "required": ["unit", "value"]
  },
  "Many!LangStringType": {
   "type": "object",
   "propertyNames": {
    "pattern":
"^(aa|ab|ae|af|ak|am|an|ar|as|av|ay|az|ba|be|bg|bh|bi|bm|bn|bo|br|bs|ca|ce|ch|co|cr|cs|cu|cv|cy|da|de|dv|dz|ee|el|en|eo|es|et|
eu|fa|ff|fi|fj|fo|fr|fy|ga|gd|gl|gn|gu|gv|ha|he|hi|ho|hr|ht|hu|hy|hz|ia|id|ie|ig|ii|ik|in|io|is|it|iu|iw|ja|ji|jv|jw|ka|kg|ki|kj|kk|kl|km|kn|ko|kr|
ks|ku|kv|kw|ky|la|lb|lg|li|ln|lo|lt|lu|lv|mg|mh|mi|mk|ml|mn|mo|mr|ms|mt|my|na|nb|nd|ne|ng|nl|nn|no|nr|nv|ny|oc|oj|om|or|os|pa|
pi|pl|ps|pt|qu|rm|rn|ro|ru|rw|sa|sc|sd|se|sg|sh|si|sk|sl|sm|sn|so|sq|sr|ss|st|su|sv|sw|ta|te|tg|th|ti|tk|tl|tn|to|tr|ts|tt|tw|ty|ug|uk|ur|
uz|ve|vi|vo|wa|wo|xh|yi|yo|za|zh|zu)$"
   },
   "minProperties": 1
  },
  "LangStringType": {
   "allOf": [
    {
     "$ref": "#/$defs/Many!LangStringType"
    },
```

```
    {
     "type": "object",
     "maxProperties": 1
    }
   ]
  },
  "Many!LearningAchievementType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningAchievementType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/LearningAchievementType"
     }
    }
   ]
  },
  "LearningAchievementType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "LearningAchievement"
    },
    "dcType": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "title": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "identifier": {
     "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
    "supplementaryDocument": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "learningOpportunity": {
     "$ref": "#/$defs/LearningOpportunityType"
    },
    "creditReceived": {
     "$ref": "#/$defs/Many!CreditPointType"
    },
    "provenBy": {
     "$ref": "#/$defs/Many!LearningAssessmentType"
    },
    "influencedBy": {
     "$ref": "#/$defs/Many!LearningActivityType"
    },
    "awardedBy": {
     "$ref": "#/$defs/AwardingProcessType"
    },
    "entitlesTo": {
     "$ref": "#/$defs/Many!LearningEntitlementType"
    },
    "specifiedBy": {
     "$ref": "#/$defs/LearningAchievementSpecificationOrQualificationType"
    },
    "hasPart": {
```

```
      "$ref": "#/$defs/Many!LearningAchievementType"
     },
     "isPartOf": {
      "$ref": "#/$defs/Many!LearningAchievementType"
     }
    },
    "required": ["title", "awardedBy"]
   },
   "Many!LearningAchievementSpecificationType": {
    "anyOf": [
     {
      "$ref": "#/$defs/LearningAchievementSpecificationType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/LearningAchievementSpecificationType"
      }
     }
    ]
   },
   "LearningAchievementSpecificationType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LearningAchievementSpecification"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "identifier": {
      "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "homepage": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "altLabel": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "category": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "dateModified": {
      "$ref": "#/$defs/DateTimeType"
     },
     "language": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "volumeOfLearning": {
      "$ref": "#/$defs/DurationType"
     },
     "mode": {
      "$ref": "#/$defs/Many!ConceptType"
```

```
    },
    "learningOutcomeSummary": {
      "$ref": "#/$defs/NoteType"
    },
    "thematicArea": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "educationSubject": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "creditPoint": {
      "$ref": "#/$defs/Many!CreditPointType"
    },
    "educationLevel": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "learningSetting": {
      "$ref": "#/$defs/ConceptType"
    },
    "maximumDuration": {
      "$ref": "#/$defs/DurationType"
    },
    "targetGroup": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "entryRequirement": {
      "$ref": "#/$defs/NoteType"
    },
    "learningOutcome": {
      "$ref": "#/$defs/Many!LearningOutcomeType"
    },
    "influencedBy": {
      "$ref": "#/$defs/Many!LearningActivitySpecificationType"
    },
    "provenBy": {
      "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    },
    "entitlesTo": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
    },
    "awardingOpportunity": {
      "$ref": "#/$defs/Many!AwardingOpportunityType"
    },
    "hasPart": {
      "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "isPartOf": {
      "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "specialisationOf": {
      "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "generalisationOf": {
      "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "status": {
      "$ref": "#/$defs/StringType"
    }
  },
  "required": ["title"]
},
"Many!LearningActivityType": {
  "anyOf": [
    {
      "$ref": "#/$defs/LearningActivityType"
    },
    {
      "type": "array",
      "items": {
```

```
        "$ref": "#/$defs/LearningActivityType"
      }
     }
    ]
   },
   "LearningActivityType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LearningActivity"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "temporal": {
      "$ref": "#/$defs/Many!PeriodOfTimeType"
     },
     "location": {
      "$ref": "#/$defs/Many!LocationType"
     },
     "learningOpportunity": {
      "$ref": "#/$defs/LearningOpportunityType"
     },
     "workload": {
      "$ref": "#/$defs/DurationType"
     },
     "directedBy": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
     },
     "awardedBy": {
      "$ref": "#/$defs/AwardingProcessType"
     },
     "influences": {
      "$ref": "#/$defs/Many!LearningAchievementType"
     },
     "specifiedBy": {
      "$ref": "#/$defs/LearningActivitySpecificationType"
     },
     "hasPart": {
      "$ref": "#/$defs/Many!LearningActivityType"
     },
     "isPartOf": {
      "$ref": "#/$defs/Many!LearningActivityType"
     },
     "levelOfCompletion": {
      "$ref": "#/$defs/PercentageIntegerType"
     }
    },
    "required": ["title", "awardedBy"]
   },
```

```
  "Many!LearningActivitySpecificationType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningActivitySpecificationType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/LearningActivitySpecificationType"
     }
    }
   ]
  },
  "LearningActivitySpecificationType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "LearningActivitySpecification"
    },
    "dcType": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "identifier": {
     "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
    },
    "title": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
    "supplementaryDocument": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "homepage": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "altLabel": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "category": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "dateModified": {
     "$ref": "#/$defs/DateTimeType"
    },
    "language": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "volumeOfLearning": {
     "$ref": "#/$defs/DurationType"
    },
    "contactHour": {
     "$ref": "#/$defs/Many!StringType"
    },
    "mode": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "influences": {
     "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "hasPart": {
```

```
      "$ref": "#/$defs/Many!LearningActivitySpecificationType"
     },
     "isPartOf": {
      "$ref": "#/$defs/Many!LearningActivitySpecificationType"
     },
     "specialisationOf": {
      "$ref": "#/$defs/Many!LearningActivitySpecificationType"
     },
     "generalisationOf": {
      "$ref": "#/$defs/Many!LearningActivitySpecificationType"
     },
     "status": {
      "$ref": "#/$defs/StringType"
     }
    },
    "required": ["title"]
   },
   "Many!LearningAssessmentType": {
    "anyOf": [
     {
      "$ref": "#/$defs/LearningAssessmentType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/LearningAssessmentType"
      }
     }
    ]
   },
   "LearningAssessmentType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LearningAssessment"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "dateIssued": {
      "$ref": "#/$defs/DateTimeType"
     },
     "location": {
      "$ref": "#/$defs/LocationType"
     },
     "grade": {
      "$ref": "#/$defs/NoteType"
     },
     "gradeStatus": {
      "$ref": "#/$defs/ConceptType"
```

```
    },
    "shortenedGrading": {
      "$ref": "#/$defs/ShortenedGradingType"
    },
    "resultDistribution": {
      "$ref": "#/$defs/ResultDistributionType"
    },
    "idVerification": {
      "$ref": "#/$defs/ConceptType"
    },
    "awardedBy": {
      "$ref": "#/$defs/AwardingProcessType"
    },
    "assessedBy": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
    },
    "proves": {
      "$ref": "#/$defs/Many!LearningAchievementType"
    },
    "hasPart": {
      "$ref": "#/$defs/Many!LearningAssessmentType"
    },
    "isPartOf": {
      "$ref": "#/$defs/Many!LearningAssessmentType"
    },
    "specifiedBy": {
      "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    }
   },
   "required": ["title", "grade", "awardedBy"]
  },
  "Many!LearningAssessmentSpecificationType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningAssessmentSpecificationType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/LearningAssessmentSpecificationType"
     }
    }
   ]
  },
  "LearningAssessmentSpecificationType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "LearningAssessmentSpecification"
    },
    "dcType": {
     "$ref": "#/$defs/ConceptType"
    },
    "identifier": {
     "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
    },
    "title": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
```

```
    "supplementaryDocument": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "homepage": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "altLabel": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "category": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "dateModified": {
     "$ref": "#/$defs/DateTimeType"
    },
    "language": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "mode": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "gradingScheme": {
     "$ref": "#/$defs/GradingSchemeType"
    },
    "proves": {
     "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "hasPart": {
     "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    },
    "isPartOf": {
     "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    },
    "specialisationOf": {
     "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    },
    "generalisationOf": {
     "$ref": "#/$defs/Many!LearningAssessmentSpecificationType"
    },
    "status": {
     "$ref": "#/$defs/StringType"
    }
   },
   "required": ["title"]
  },
  "Many!LearningEntitlementType": {
   "anyOf": [
    {
     "$ref": "#/$defs/LearningEntitlementType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/LearningEntitlementType"
     }
    }
   ]
  },
  "LearningEntitlementType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "LearningEntitlement"
    },
    "dcType": {
```

```
      "$ref": "#/$defs/Many!ConceptType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "dateIssued": {
      "$ref": "#/$defs/DateTimeType"
     },
     "expiryDate": {
      "$ref": "#/$defs/DateTimeType"
     },
     "awardedBy": {
      "$ref": "#/$defs/AwardingProcessType"
     },
     "entitledBy": {
      "$ref": "#/$defs/Many!LearningAchievementType"
     },
     "hasPart": {
      "$ref": "#/$defs/Many!LearningEntitlementType"
     },
     "isPartOf": {
      "$ref": "#/$defs/Many!LearningEntitlementType"
     },
     "specifiedBy": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
     }
    },
    "required": ["title", "awardedBy"]
   },
   "Many!LearningEntitlementSpecificationType": {
    "anyOf": [
     {
      "$ref": "#/$defs/LearningEntitlementSpecificationType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/LearningEntitlementSpecificationType"
      }
     }
    ]
   },
   "LearningEntitlementSpecificationType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LearningEntitlementSpecification"
     },
     "dcType": {
      "$ref": "#/$defs/Single!ConceptType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
```

```
    },
    "title": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
    },
    "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
    },
    "homepage": {
      "$ref": "#/$defs/Many!WebResourceType"
    },
    "altLabel": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "category": {
      "$ref": "#/$defs/Many!LangStringType"
    },
    "dateModified": {
      "$ref": "#/$defs/DateTimeType"
    },
    "entitlementStatus": {
      "$ref": "#/$defs/ConceptType"
    },
    "limitOrganisation": {
      "$ref": "#/$defs/Many!OrganisationType"
    },
    "limitJurisdiction": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "limitOccupation": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "limitNationalOccupation": {
      "$ref": "#/$defs/Many!ConceptType"
    },
    "entitledBy": {
      "$ref": "#/$defs/Many!LearningAchievementSpecificationOrQualificationType"
    },
    "hasPart": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
    },
    "isPartOf": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
    },
    "specialisationOf": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
    },
    "generalisationOf": {
      "$ref": "#/$defs/Many!LearningEntitlementSpecificationType"
    },
    "status": {
      "$ref": "#/$defs/StringType"
    }
  },
  "required": ["title", "entitlementStatus", "dcType"]
},
"Many!LearningOpportunityType": {
  "anyOf": [
    {
      "$ref": "#/$defs/LearningOpportunityType"
    },
    {
      "type": "array",
      "items": {
```

```
        "$ref": "#/$defs/LearningOpportunityType"
      }
     }
    ]
   },
   "LearningOpportunityType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "LearningOpportunity"
     },
     "dcType": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "homepage": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "temporal": {
      "$ref": "#/$defs/PeriodOfTimeType"
     },
     "duration": {
      "$ref": "#/$defs/DurationType"
     },
     "mode": {
      "$ref": "#/$defs/Many!ConceptType"
     },
     "learningSchedule": {
      "$ref": "#/$defs/ConceptType"
     },
     "scheduleInformation": {
      "$ref": "#/$defs/NoteType"
     },
     "admissionProcedure": {
      "$ref": "#/$defs/NoteType"
     },
     "priceDetail": {
      "$ref": "#/$defs/Many!PriceDetailType"
     },
     "providedBy": {
      "$ref": "#/$defs/OrganisationType"
     },
     "grant": {
      "$ref": "#/$defs/Many!GrantType"
     },
     "location": {
      "$ref": "#/$defs/Many!LocationType"
     },
     "learningAchievementSpecification": {
      "$ref": "#/$defs/LearningAchievementSpecificationOrQualificationType"
     },
```

```
    "learningActivitySpecification": {
     "$ref": "#/$defs/LearningActivitySpecificationType"
    },
    "hasPart": {
     "$ref": "#/$defs/Many!LearningOpportunityType"
    },
    "isPartOf": {
     "$ref": "#/$defs/Many!LearningOpportunityType"
    },
    "bannerImage": {
     "$ref": "#/$defs/MediaObjectType"
    },
    "applicationDeadline": {
     "$ref": "#/$defs/Many!DateTimeType"
    },
    "defaultLanguage": {
     "$ref": "#/$defs/ConceptType"
    },
    "descriptionHtml": {
     "$ref": "#/$defs/Many!HTMLType"
    },
    "dateModified": {
     "$ref": "#/$defs/DateTimeType"
    },
    "status": {
     "$ref": "#/$defs/StringType"
    }
   },
   "required": ["title"]
  },
  "Many!PriceDetailType": {
   "anyOf": [
    {
     "$ref": "#/$defs/PriceDetailType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/PriceDetailType"
     }
    }
   ]
  },
  "PriceDetailType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "PriceDetail"
    },
    "identifier": {
     "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
    },
    "prefLabel": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "additionalNote": {
     "$ref": "#/$defs/Many!NoteType"
    },
    "amount": {
     "$ref": "#/$defs/AmountType"
    }
   },
```

```
    "required": []
   },
   "Many!ResultCategoryType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ResultCategoryType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ResultCategoryType"
      }
     }
    ]
   },
   "ResultCategoryType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ResultCategory"
     },
     "label": {
      "$ref": "#/$defs/StringType"
     },
     "score": {
      "$ref": "#/$defs/StringType"
     },
     "maximumScore": {
      "$ref": "#/$defs/StringType"
     },
     "minimumScore": {
      "$ref": "#/$defs/StringType"
     },
     "count": {
      "$ref": "#/$defs/PositiveIntegerType"
     }
    },
    "required": ["label", "count"]
   },
   "Many!ResultDistributionType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ResultDistributionType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ResultDistributionType"
      }
     }
    ]
   },
   "ResultDistributionType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ResultDistribution"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
```

```
    "resultCategory": {
     "$ref": "#/$defs/Many!ResultCategoryType"
    }
   },
   "required": []
  },
  "Many!ShortenedGradingType": {
   "anyOf": [
    {
     "$ref": "#/$defs/ShortenedGradingType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/ShortenedGradingType"
     }
    }
   ]
  },
  "ShortenedGradingType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "ShortenedGrading"
    },
    "percentageLower": {
     "$ref": "#/$defs/IntegerType"
    },
    "percentageEqual": {
     "$ref": "#/$defs/IntegerType"
    },
    "percentageHigher": {
     "$ref": "#/$defs/IntegerType"
    }
   },
   "required": ["percentageLower", "percentageEqual", "percentageHigher"]
  },
  "Many!VerificationCheckType": {
   "anyOf": [
    {
     "$ref": "#/$defs/VerificationCheckType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/VerificationCheckType"
     }
    }
   ]
  },
  "VerificationCheckType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "VerificationCheck"
    },
    "dcType": {
     "$ref": "#/$defs/ConceptType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
```

```
    },
    "verificationStatus": {
      "$ref": "#/$defs/ConceptType"
    },
    "elmSubject": {
      "$ref": "#/$defs/EuropeanDigitalCredentialType"
    }
   },
   "required": ["verificationStatus", "subject", "dcType"]
  },
  "Many!EvidenceType": {
   "anyOf": [
    {
      "$ref": "#/$defs/EvidenceType"
    },
    {
      "type": "array",
      "items": {
       "$ref": "#/$defs/EvidenceType"
      }
    }
   ]
  },
  "EvidenceType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
      "$ref": "#/$defs/GenericIdType"
    },
    "type": {
      "const": "Evidence"
    },
    "evidenceStatement": {
      "$ref": "#/$defs/StringType"
    },
    "evidenceTarget": {
      "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
    },
    "embeddedEvidence": {
      "$ref": "#/$defs/Many!MediaObjectType"
    },
    "accreditation": {
      "$ref": "#/$defs/AccreditationType"
    },
    "dcType": {
      "$ref": "#/$defs/ConceptType"
    }
   },
   "required": []
  },
  "Many!TermsOfUseType": {
   "anyOf": [
    {
      "$ref": "#/$defs/TermsOfUseType"
    },
    {
      "type": "array",
      "items": {
       "$ref": "#/$defs/TermsOfUseType"
      }
    }
   ]
  },
  "TermsOfUseType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
```

```
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "TermsOfUse"
     }
    },
    "required": []
   },
   "Many!ProofType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ProofType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ProofType"
      }
     }
    ]
   },
   "ProofType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Proof"
     }
    },
    "required": []
   },
   "Many!CredentialStatusType": {
    "anyOf": [
     {
      "$ref": "#/$defs/CredentialStatusType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/CredentialStatusType"
      }
     }
    ]
   },
   "CredentialStatusType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "type": "string",
      "enum": ["StatusList2021Entry"]
     }
    },
    "required": []
   },
   "Many!CredentialSchemaType": {
    "anyOf": [
     {
      "$ref": "#/$defs/CredentialSchemaType"
     },
     {
      "type": "array",
      "items": {
```

```
        "$ref": "#/$defs/CredentialSchemaType"
      }
     }
    ]
   },
   "CredentialSchemaType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "type": "string",
      "enum": ["ShaclValidator2017", "JsonSchema"]
     }
    },
    "required": []
   },
   "Many!AmountType": {
    "anyOf": [
     {
      "$ref": "#/$defs/AmountType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/AmountType"
      }
     }
    ]
   },
   "Many!AwardingProcessType": {
    "anyOf": [
     {
      "$ref": "#/$defs/AwardingProcessType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/AwardingProcessType"
      }
     }
    ]
   },
   "AwardingProcessType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "AwardingProcess"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "location": {
      "$ref": "#/$defs/LocationType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
     "used": {
      "$ref": "#/$defs/Many!LearningAssessmentType"
```

```
    },
    "awards": {
      "$ref": "#/$defs/Many!ClaimNodeType"
    },
    "awardingBody": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
    },
    "awardingDate": {
      "$ref": "#/$defs/DateTimeType"
    },
    "educationalSystemNote": {
      "$ref": "#/$defs/ConceptType"
    }
   },
   "required": ["awardingBody"]
  },
  "Many!DisplayParameterType": {
   "anyOf": [
    {
     "$ref": "#/$defs/DisplayParameterType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/DisplayParameterType"
     }
    }
   ]
  },
  "DisplayParameterType": {
   "type": "object",
   "additionalProperties": false,
   "properties": {
    "id": {
     "$ref": "#/$defs/GenericIdType"
    },
    "type": {
     "const": "DisplayParameter"
    },
    "title": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "description": {
     "$ref": "#/$defs/Many!LangStringType"
    },
    "language": {
     "$ref": "#/$defs/Many!ConceptType"
    },
    "primaryLanguage": {
     "$ref": "#/$defs/ConceptType"
    },
    "summaryDisplay": {
     "$ref": "#/$defs/StringType"
    },
    "individualDisplay": {
     "$ref": "#/$defs/Many!IndividualDisplayType"
    }
   },
   "required": ["title", "language", "primaryLanguage", "individualDisplay"]
  },
  "Many!IndividualDisplayType": {
   "anyOf": [
    {
     "$ref": "#/$defs/IndividualDisplayType"
    },
    {
     "type": "array",
     "items": {
      "$ref": "#/$defs/IndividualDisplayType"
```

```
      }
     }
    ]
   },
   "IndividualDisplayType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "IndividualDisplay"
     },
     "language": {
      "$ref": "#/$defs/ConceptType"
     },
     "displayDetail": {
      "$ref": "#/$defs/Many!DisplayDetailType"
     }
    },
    "required": ["language", "displayDetail"]
   },
   "Many!DisplayDetailType": {
    "anyOf": [
     {
      "$ref": "#/$defs/DisplayDetailType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/DisplayDetailType"
      }
     }
    ]
   },
   "DisplayDetailType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "DisplayDetail"
     },
     "image": {
      "$ref": "#/$defs/MediaObjectType"
     },
     "page": {
      "$ref": "#/$defs/PositiveIntegerType"
     }
    },
    "required": ["image", "page"]
   },
   "Many!EuropeanDigitalPresentationType": {
    "anyOf": [
     {
      "$ref": "#/$defs/EuropeanDigitalPresentationType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/EuropeanDigitalPresentationType"
      }
     }
    ]
   },
   "EuropeanDigitalPresentationType": {
```

```
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "EuropeanDigitalPresentation"
     },
     "verifiableCredential": {
      "$ref": "#/$defs/Many!EuropeanDigitalCredentialType"
     },
     "verificationCheck": {
      "$ref": "#/$defs/Many!VerificationCheckType"
     },
     "holder": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
     },
     "proof": {
      "$ref": "#/$defs/Many!ProofType"
     }
    },
    "required": []
   },
   "Many!GradingSchemeType": {
    "anyOf": [
     {
      "$ref": "#/$defs/GradingSchemeType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/GradingSchemeType"
      }
     }
    ]
   },
   "GradingSchemeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "GradingScheme"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     }
    },
    "required": ["title"]
   },
   "Many!GrantType": {
    "anyOf": [
     {
      "$ref": "#/$defs/GrantType"
     },
     {
      "type": "array",
```

```
      "items": {
       "$ref": "#/$defs/GrantType"
      }
     }
    ]
   },
   "GrantType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "Grant"
     },
     "dcType": {
      "$ref": "#/$defs/ConceptType"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "supplementaryDocument": {
      "$ref": "#/$defs/Many!WebResourceType"
     },
     "contentURL": {
      "$ref": "#/$defs/URIType"
     }
    },
    "required": ["title"]
   },
   "Many!ClaimTypeNodeType": {
    "anyOf": [
     {
      "$ref": "#/$defs/ClaimTypeNodeType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/ClaimTypeNodeType"
      }
     }
    ]
   },
   "ClaimTypeNodeType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
     "id": {
      "$ref": "#/$defs/GenericIdType"
     },
     "type": {
      "const": "ClaimTypeNode"
     },
     "title": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "description": {
      "$ref": "#/$defs/Many!LangStringType"
     },
     "identifier": {
      "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
     },
     "additionalNote": {
      "$ref": "#/$defs/Many!NoteType"
     },
```

```
    "supplementaryDocument": {
     "$ref": "#/$defs/Many!WebResourceType"
    },
    "awardedBy": {
     "$ref": "#/$defs/AwardingProcessType"
    }
   },
   "required": ["title", "awardedBy"]
  },
 "EuropeanDigitalCredentialType": {
  "type": "object",
  "properties": {
   "id": {
    "$ref": "#/$defs/GenericIdType"
   },
   "type": {
    "type": "array",
    "items": {
     "type": "string",
     "enum": [
      "VerifiableCredential",
      "VerifiableAttestation",
      "EuropeanDigitalCredential"
     ]
    },
    "minItems": 3,
    "uniqueItems": true
   },
   "identifier": {
    "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
   },
   "credentialProfiles": {
    "$ref": "#/$defs/Many!ConceptType"
   },
   "attachment": {
    "$ref": "#/$defs/Many!MediaObjectType"
   },
   "displayParameter": {
    "$ref": "#/$defs/DisplayParameterType"
   },
   "issuer": {
    "anyOf": [
     {
      "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
     },
     {
      "$ref": "#/$defs/GenericIdType"
     }
    ]
   },
   "credentialSubject": {
    "$ref": "#/$defs/AgentOrPersonOrOrganisationType"
   },
   "issuanceDate": {
    "$ref": "#/$defs/DateTimeType"
   },
   "issued": {
    "$ref": "#/$defs/DateTimeType"
   },
   "validFrom": {
    "$ref": "#/$defs/DateTimeType"
   },
   "expirationDate": {
    "$ref": "#/$defs/Many!DateTimeType"
   },
   "validUntil": {
    "$ref": "#/$defs/DateTimeType"
   },
   "proof": {
```

```
      "$ref": "#/$defs/Many!ProofType"
     },
     "evidence": {
      "$ref": "#/$defs/Many!EvidenceType"
     },
     "termsOfUse": {
      "$ref": "#/$defs/Many!TermsOfUseType"
     },
     "credentialSchema": {
      "$ref": "#/$defs/Many!CredentialSchemaType"
     },
     "credentialStatus": {
      "$ref": "#/$defs/Many!CredentialStatusType"
     },
     "holder": {
      "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
     }
    },
    "required": [
     "credentialProfiles",
     "displayParameter",
     "issuer",
     "credentialSubject",
     "issued",
     "validFrom",
     "credentialSchema"
    ]
   },
   "Many!IdentifierOrLegalIdentifierType": {
    "anyOf": [
     {
      "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/IdentifierOrLegalIdentifierType"
      }
     }
    ]
   },
   "Many!MediaObjectType": {
    "anyOf": [
     {
      "$ref": "#/$defs/MediaObjectType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/MediaObjectType"
      }
     }
    ]
   },
   "Many!DateTimeType": {
    "anyOf": [
     {
      "$ref": "#/$defs/DateTimeType"
     },
     {
      "type": "array",
      "items": {
       "$ref": "#/$defs/DateTimeType"
      }
     }
    ]
   },
   "Many!LearningAchievementSpecificationOrQualificationType": {
    "anyOf": [
```

```
      {
        "$ref": "#/$defs/LearningAchievementSpecificationOrQualificationType"
      },
      {
        "type": "array",
        "items": {
          "$ref": "#/$defs/LearningAchievementSpecificationOrQualificationType"
        }
      }
    ]
  },
  "LearningAchievementSpecificationOrQualificationType": {
    "anyOf": [
      {
        "$ref": "#/$defs/LearningAchievementSpecificationType"
      },
      {
        "$ref": "#/$defs/QualificationType"
      }
    ]
  },
  "Many!AwardingOpportunityType": {
    "anyOf": [
      {
        "$ref": "#/$defs/AwardingOpportunityType"
      },
      {
        "type": "array",
        "items": {
          "$ref": "#/$defs/AwardingOpportunityType"
        }
      }
    ]
  },
  "AwardingOpportunityType": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "$ref": "#/$defs/GenericIdType"
      },
      "type": {
        "const": "AwardingOpportunity"
      },
      "identifier": {
        "$ref": "#/$defs/Many!IdentifierOrLegalIdentifierType"
      },
      "location": {
        "$ref": "#/$defs/LocationType"
      },
      "temporal": {
        "$ref": "#/$defs/PeriodOfTimeType"
      },
      "awardingBody": {
        "$ref": "#/$defs/Many!AgentOrPersonOrOrganisationType"
      },
      "learningAchievementSpecification": {
        "$ref": "#/$defs/LearningAchievementSpecificationOrQualificationType"
      }
    },
    "required": ["awardingBody"]
  }
 }
}
```

# Annex D: Regulatory references

1. eIDAS Regulation (EU) No 910/2014 and Amendment (EU) 2024/1183

This regulation provides the legal framework for electronic identification, authentication, and trust services in electronic transactions across the EU. The 2024 amendment establishes the European Digital Identity Framework (EUDI), which includes electronic attestations of attributes for credentials. It facilitates the legal recognition of digital credentials across Member States, supporting secure, interoperable credentialing.

2. General Data Protection Regulation (GDPR) (EU) 2016/679

GDPR governs data protection and privacy within the EU, ensuring the rights of individuals to control their personal data. This regulation is crucial for digital credentialing, setting requirements for data security, consent, and lawful data processing, especially in cross-border educational and professional credential exchanges.

3. Single Digital Gateway (SDG) Regulation (EU) 2018/1724

The SDG regulation aims to simplify access to public services and administrative information across Member States. It supports the Once-Only Principle (OOP), ensuring that data collected from citizens is reused, reducing administrative burdens and promoting interoperability for credentials in education and employment.

4. European Qualifications Framework (EQF) Recommendation (2008/C 111/01)

The EQF provides a common reference framework for comparing qualifications across Europe. This supports transparency, comparability, and the recognition of skills and qualifications, contributing to a more integrated European education and employment landscape.

5. Professional Qualifications Directive (PQD) 2005/36/EC and Amendments

This directive supports the recognition of professional qualifications across the EU, allowing professionals to work in other Member States. The directive aligns with the European Digital Identity and credentialing frameworks, ensuring that qualifications are recognised legally and efficiently.

6. European Skills Agenda

The European Skills Agenda sets objectives for upskilling and reskilling across the EU, supporting lifelong learning and workforce mobility. It promotes recognition of micro-credentials and supports initiatives like Europass and ESCO for skill classification, in alignment with digital identity frameworks.

Co-funded by the European Union

7. Digital Education Action Plan (DEAP) 2021-2027

The DEAP outlines actions to advance digital literacy and the use of digital technologies in education. It supports the development of high-quality digital education content and skills, and the digital transformation of educational institutions, promoting compatibility with European digital credentials.

8. European Education Area (EEA) Initiative

The EEA aims to remove barriers to studying and working across Europe by 2025, promoting qualification portability and mobility. Trust frameworks for digital credentials are a key element, as they support seamless recognition of qualifications across borders.

9. European Blockchain Strategy

Part of the European Digital Strategy, this strategy focuses on using blockchain technology to support trusted and secure services. The European Blockchain Services Infrastructure (EBSI) aligns with this strategy, providing a foundation for verifiable digital credentials and promoting interoperability in education and employment.

10. European Data Strategy

This strategy promotes data sovereignty and the establishment of European data spaces, enabling secure and controlled data sharing across sectors. For education, this aligns with efforts to establish interoperable credentialing systems that respect data protection and promote cross-border recognition of qualifications.

11. European Digital Identity Framework (EUDI)

The EUDI framework is a comprehensive system for digital identity, enabling citizens to store and share verified personal attributes and credentials in a secure, standardised way. It supports the use of EUDI wallets, enhancing the portability of credentials and ensuring that digital identities are recognised across the EU.

12. Europass Decision (Decision 2241/2004/EC)

Europass is an EU initiative for transparency in skills and qualifications, making it easier for citizens to present their skills across Europe. The updated Europass Digital Credentials Infrastructure (EDCI) aligns with the European Digital Identity to facilitate the issue and verification of digital credentials.

Co-funded by the European Union