everis
an NTT DATA Company

Europass framework for digitally-signed credentials

Background document

European Commission

Document prepared for the expert workshop taking place on 6 November 2018

promoted by the European Commission

Executive summary

Digitally-signed credentials are understood as electronic documents (generally referred to as 'digital certificates') which are issued by awarding bodies to individuals to confirm and provide proof of their learning outcomes. A framework for digitally-signed credentials is being developed as part of a policy initiative from the European Commission aimed at fostering the gradual adoption of digital certificates and providing a secure and trustworthy system that ensures data privacy and protection. In addition, this framework is also expected to contribute to ensuring a common understanding of qualifications and types of certifications across and beyond the European Union in the context of digital certificates, and to promoting the recognition of qualifications, competences and skills acquired in formal, informal and non-formal contexts throughout an individual's life. Credentials from different learning contexts can be better captured and documented by adopting a credit-based framework and by embedding well-established classifications and credit systems at European level. To foster an easy and flexible adoption of a framework for digitally-signed credentials, it will be built on open standards and be made available for free.

The main target stakeholders of the framework are anticipated to be: individuals (including learners, jobseekers, workers, or volunteers) who will be awarded digitally-signed credentials, store them and will have the possibility to decide with whom to share them; different awarding bodies (among which education and training institutions, businesses, civil society organisations) that may issue digital certificates to individuals; and employers and other organisations which may be interested in verifying the authenticity of digital certificates of individuals. Other stakeholders are expected to have a supporting role in the implementation of the framework, including the European Commission, the EU Member States, and accreditation bodies.

In order to ensure a better understanding the framework for digitally-signed credentials, a conceptual model was developed with four main components:

- *Principles*, which are aimed at governing the framework as a whole. Ten principles have been identified: user-centricity, inclusion and accessibility, subsidiarity and proportionality, openness, data protection by design and by default, interoperability, transparency, resilience, qualifications as a public good, and reusability;
- *Functions*, which describe the different purposes of the framework according to its governing principles and which serve an ecosystem of stakeholders. The main functions of the framework are: identify, issue, store, share and verify;
- *Infrastructure*, which encompasses the main functional building blocks (e.g. services and tools) that should be tailored to addressing the needs of the functions and the specificities of the standards of the framework; and
- *Standards*, which should be understood as the foundation that supports and sustains the other components. Four different types of standards will be considered, including metadata, technical, workflow management, and quality standards.

A European Digital Credentials Infrastructure (EDCI) is proposed to implement the framework for digitally-signed credentials. In order to help operationalise the framework, four core building blocks form part of the EDCI, including eIDAS components, standards, software and services.

List of abbreviations

API	Application Programming Interface
CEN	European Committee on Standardisation
CV	Curriculum Vitae
DIDs	Decentralised Identifiers
EC	European Commission
ECTS	European Credit Transfer and Accumulation System
ECVET	European Credit system for Vocational Education and Training
EDCI	Europass Digital Credentials Infrastructure
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services (Regulation (EU) N°910/2014)
ENIC/NARIC	European Network of Information Centres in the European Region / National Academic Recognition Information Centres in the European Region
EQAVET	European Quality Assurance for Vocational Education and Training
EQF	European Qualifications Framework for Lifelong Learning
ESCO	European Classification of Skills, Competences, Qualifications and Occupations
EU	European Union
EURES	European network of Employment Services
GDPR	General Data Protection Regulation
HRMS	Human Resource Management Systems
ICT	Information and Communication Technologies
IPFS	InterPlanetary File System
IT	Information Technology
MS	Member State
NQF	National Qualifications Framework
PKI	Public Key Infrastructure
SIS	Student Information Systems

Glossary

Unless otherwise mentioned, the definitions provided below were developed by the authors of this publication for the specific purposes of this project.

Certificate – An official document, issued by an awarding body, which records achievements of an individual following an assessment against a predefined standard[1].

Certification of learning outcomes – Process of issuing a certificate, diploma or title formally attesting that a set of learning outcomes (knowledge, know-how, skills and/or competences) acquired by an individual have been assessed by a competent body against a predefined standard.[2]

Competence – Ability to apply learning outcomes adequately in a defined context (education, work, personal or professional development)[3].

Digitally-signed credential – Electronic document which is issued by an awarding body to an individual to confirm and provide proof of her/his learning outcomes.

Diploma mills – Institutions or organisations that grant large numbers of educational degrees based on inadequate or inferior education and assessment of the credential owners.

Electronic Seal – Data in electronic form attached to, or logically associated, with other data in electronic form to ensure the latter's origin and integrity[4].

e-portfolio – Digital dynamic tool that enables individuals to document, display and manage their skills, qualifications and experience throughout the lifespan of their career.

Experience – Knowledge, skills and competences which an individual gained by undertaking an activity for a certain period of time.

Interoperability – Ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems[5]. *Technical interoperability* means the ability of information and communication technology systems to interact so as to enable the sharing of information, achieved through agreement by all parties and owners of the information[6].

[1] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office.
[2] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office.
[3] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office.
[4] REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[5] European Union (2017). New European Interoperability Framework – Promoting seamless services and data flows for European public administrations. Luxembourg: Publications office
[6] DECISION (EU) 2018/646 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC.

Lifelong learning – All learning activities undertaken throughout life, which result in improving knowledge, know-how, skills, competences and/or qualifications for personal, social and/or professional reasons[7].

Qualification – Formal outcome (certificate, diploma or title) of an assessment process which is obtained when a competent body determines that an individual has achieved learning outcomes to given standards and/or possesses the necessary competence to do a job in a specific area of work. A qualification confers official recognition of the value of learning outcomes in the labour market and in education and training. A qualification can be a legal entitlement to practise a trade[8].

Qualification Record – An electronic record of information on qualifications described through specific elements such as EQF level, awarding body or competent authority, internal quality assurance processes, external quality assurance/regulatory body, ways to acquire qualification, among others[9].

Qualified Electronic Seals – An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal[10].

Self-Sovereignty – State where a user has complete direct ownership and control over their own data.

Share – Functionalities that allow individuals to publish or provide access to third parties to their information on skills, qualifications and experience.

Skill – Ability to apply knowledge and use know-how to compete tasks and solve problems[11].

Store – Functionalities that allow individuals to save their information and documentation in electronic form, such as into their Europass2 account or download it for local storage.

Trust Service Provider – An individual or legal entity which creates, verifies, and validates electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services.

[7] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office.
[8] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office
[9] COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning (2017/C 189/03).
[10] REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[11] Cedefop (2014). Terminology of European education and training policy – A selection of 130 key terms (second edition). Luxembourg: Publications office.

Table of contents

1. Introduction

Back in 2004, the European Parliament and the Council established a framework to achieve better transparency of qualifications and competences through Europass. Throughout the last 14 years, Europass evolved to a portfolio of five documents that is aimed at making individuals' skills and qualifications clearly and easily understood in Europe. Considering the growing needs of a digital society and the challenges faced to reach out to all potential users, a new Europass framework was adopted in April 2018 (hereafter referred to as 'Europass2')[12]. At the same time, in order to make use of the largely untapped potential of digital technology in education and to promote the development of digital competences, the European Commission adopted in January 2018 the Digital Education Action Plan[13].

Both policy initiatives highlight the importance of a digital infrastructure and tools to document, share and verify learning achievements (including skills and qualifications). To this end, the European Commission is committed to **develop a framework for digitally-signed credentials**[14] (as put forth in action 3 of the Digital Education Action Plan). The technical approach to be designed for the framework should allow for *identifying, issuing, storing, sharing* and *verifying* digitally-signed credentials in a cross-border context. Europass2 is expected to support the implementation of this framework by offering, among others, the possibility to store and share digitally-signed credentials from its users.

The present document summarises the main objectives, scope, conceptual model and technical specifications to implement the Europass framework for digitally-signed credentials.

[12] DECISION (EU) 2018/646 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC. Last accessed on 07/06/2018 at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D0646&qid=1528377899596&from=EN

[13] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan {SWD(2018) 12 final} (COM(2018) 22 final). Last accessed on 07/06/2018 at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN

[14] Although it was originally designated 'framework for digitally-signed qualifications', a decision was taken to find a broader designation that considers and allows for capturing formal, informal and non-formal learning outcomes (as qualifications are intimately related to formal education).

2. Europass framework for digitally-signed credentials

As outlined in the Digital Education Action Plan, the way forward to make better use of digital technology for teaching and learning encompasses an action to *"provide a framework for issuing digitally-certified qualifications and validating digitally-acquired skills that are trusted, multilingual and can be stored in professional profiles (CVs) such as Europass. The framework will be fully aligned with the European Qualifications Framework for Lifelong Learning (EQF) and the European Classification of Skills, Competences, Qualifications and Occupations (ESCO)"*.[15]

Digitally-signed credentials are electronic documents which are awarded by qualified bodies to individuals to confirm and provide proof of their learning outcomes.

Although a few initiatives have recently spurred in the field of digitally-signed credentials, there remains a need to **adapt and align current paper-based certificates** to the present digital era. Digitally-signed credentials pose challenges related to security, privacy and trust. On the one hand, the **personal data** of the individual need to be secured. On the other hand, a wide range of stakeholders, such as employers, education and training institutions, public employment services or civil society organisations need to be able to **verify the authenticity and accreditation of digital certificates**. Adding to the complexity of developing further existing or new technical approaches for digitally-signed credentials is the capacity to encompass the diverse landscape of **formal, informal and non-formal learning** processes in the European Union and beyond, along with multiple forms of capturing their outcomes. Finally, from a perspective of lifelong learning, individuals should be able to progressively **store and share digital certificates** which document their skills, competences, qualifications, and practical, mobility and volunteering experiences. A framework for digitally-signed credentials is intended to help the European Union overcome these challenges.

The **key objectives** for developing a framework for digitally-signed qualifications are:

- Fostering the gradual adoption of digital certificates;
- Provide a secure and trustworthy system that ensures data privacy and protection;
- Ensuring a common understanding of qualifications and types of certifications across and beyond the European Union in the context of digital certificates; and
- Contributing to the promotion of recognition of qualifications, competences and skills acquired in formal, informal and non-formal contexts throughout an individual's life.

[15] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan {SWD(2018) 12 final} (COM(2018) 22 final). Last accessed on 07/06/2018 at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN

2.1. Scope

In this context, a digitally-signed credential **should recognise learning outcomes achieved in formal, informal and non-formal settings**. Likewise, this framework should consider all learning activities undertaken throughout life. As such, this framework should encompass any kind of **credential**, i.e. a learning outcome acquired or demonstrated by an individual after completing a formal, informal and/or non-formal learning process. The figure below describes the three types of credentials that will be supported by the proposed framework.

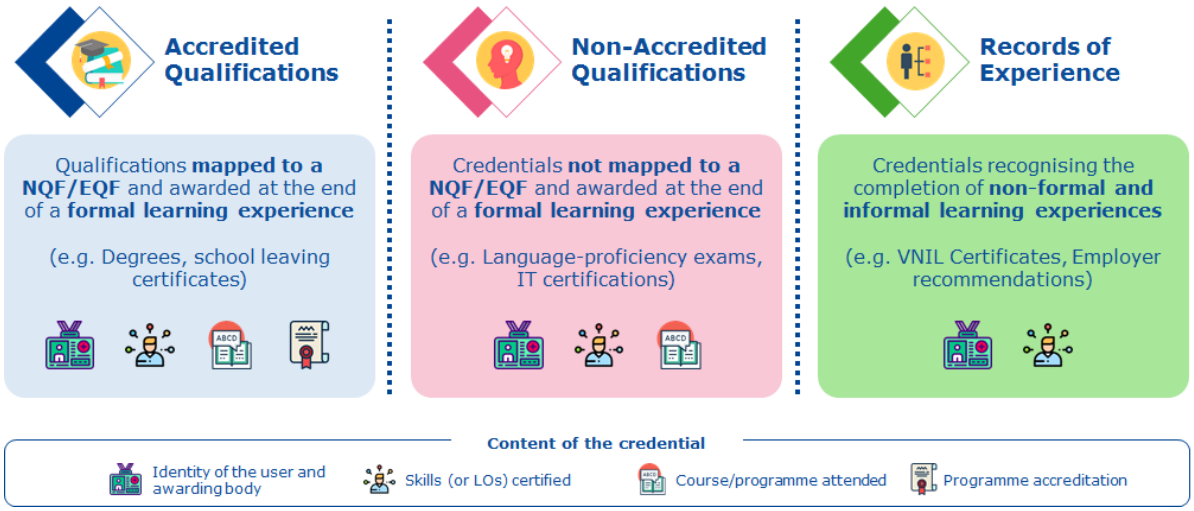

Figure 1. Types of credentials

A **credit-based framework** can help capture diverse learning outcomes (in the form of credentials) from a lifelong perspective. Credit systems allow for flexibility in documenting and acknowledging learning achievements from different settings. In this context, a credit is a special kind of digitally-signed credential which can be stacked with other credits to form a new kind of credential (see figure below).

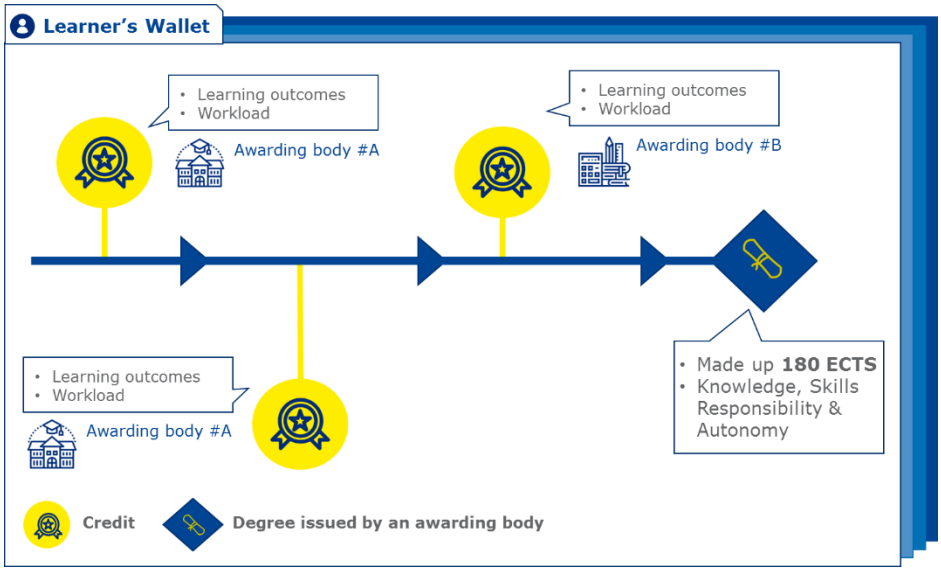

Figure 2. Example of a credit-based framework (ECTS)

At the same time, ensuring that qualifications, competences and skills can be easily identified and understood by any EU Member State needs to be prioritised. This can be achieved by **embedding well-established classifications and credit systems at European level**, namely the European Qualifications Framework for Lifelong Learning (EQF), the European Classification of Skills, Competences, Qualifications and Occupations (ESCO), the European Credit Transfer and Accumulation System (ECTS) and the European Credit system for Vocational Education and Training (ECVET).

Finally, the framework for digitally-signed qualifications should be **based on open standards** (both semantic and technical standards) and made **available for free** to foster its easy and flexible adoption. As Europass is currently being re-shaped and modernised, the framework for digitally-signed credentials will not only provide access to the technical specifications of the framework, but also be part of its core features and functionalities. More concretely, Europass's web-based tools, namely the e-portfolio, should allow for storing and sharing end-users' digital certificates.

2.2. Main stakeholders

The framework for digitally-signed credentials expects to target different types of stakeholders which will play distinct roles.

Individuals or credential owners (including learners, jobseekers, workers or volunteers) will be awarded digitally-signed qualifications which record their learning outcomes achieved in formal, informal and non-formal contexts. This framework recognises the diversity of individuals (e.g. different goals, experiences and digital skills) and takes into account their distinct needs throughout their lives. First and foremost, this framework ensures ownership over and protection of the personal data of individuals. They receive and *store* certificates, and they ultimately decide with whom they wish to *share* them.

The various learning contexts addressed within the scope of this framework impact on the multiplicity of **awarding bodies** that may *issue* digitally-signed qualifications to learners. These comprise education and training institutions, businesses, civil society organisations, or any other organisation which can recognise, validate and/or certify an individual's skills, competences or qualifications. The awarding bodies need to *identify* the individual to whom a digital certificate will be issued. On the other hand, **employers** will be interested in *verifying* the authenticity of digitally-signed qualifications of jobseekers, along with permission to issue such qualifications. At the same time, **other organisations** like education and training institutions or civil society organisations, may also wish to verify skills, competences or qualifications documented in a digital certificate for other purposes than seeking employment (e.g. there might be prerequisites to join a training course, or some volunteering activities may require certain skills).

To exemplify the roles of these stakeholders, two user stories are provided in the figure below.

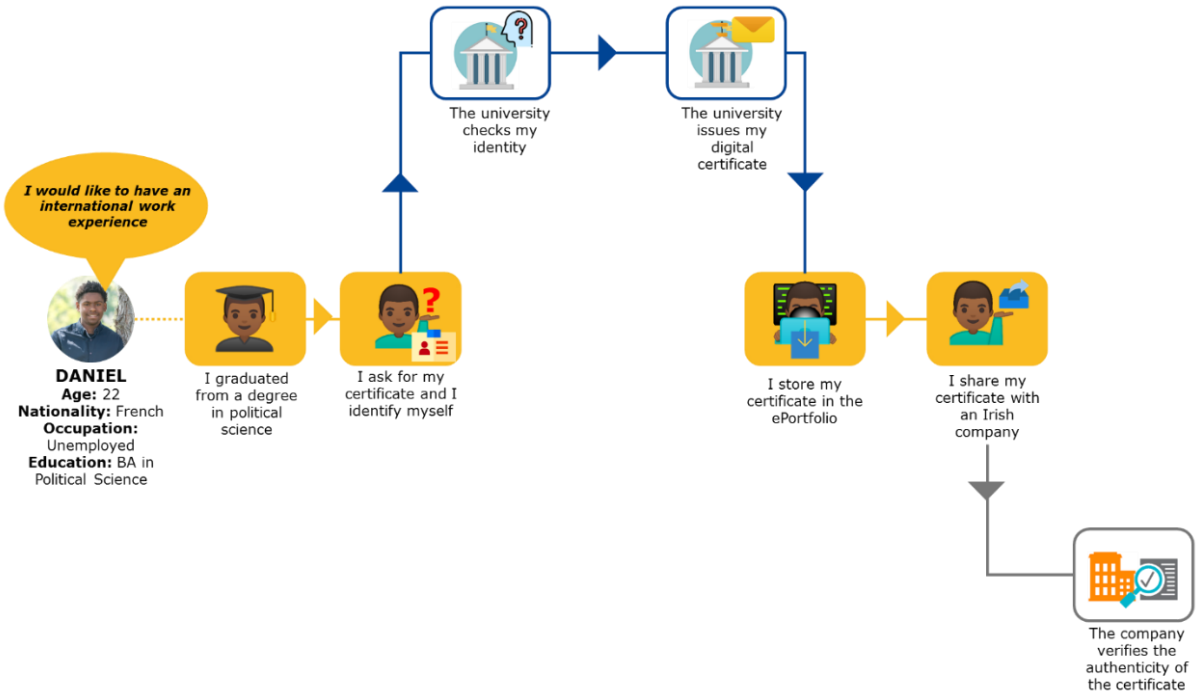

Figure 3. User story exemplifying the roles of stakeholders (from the perspective of a learner)

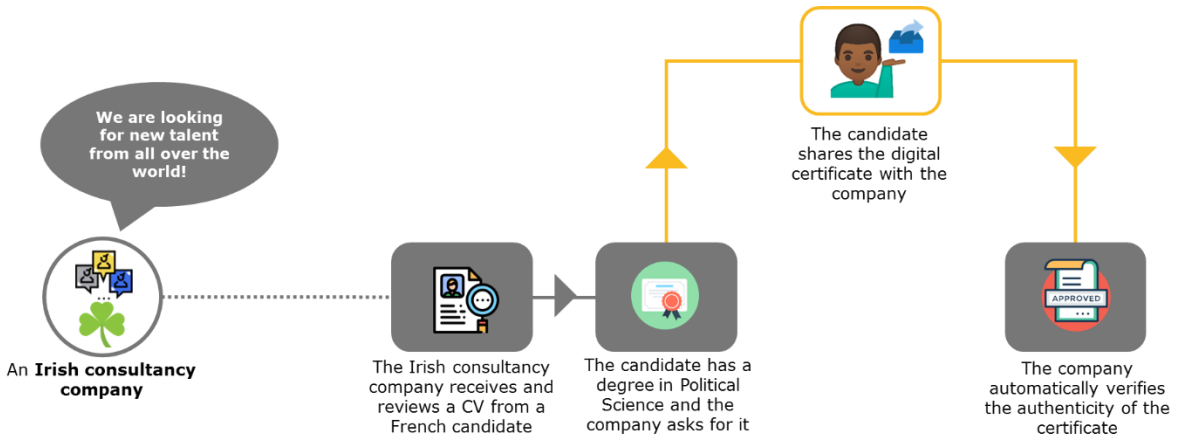

Figure 4. User story exemplifying the roles of stakeholders (from the perspective of a verifier)

On the other hand, other stakeholders have a *supporting role in the implementation* of the framework. The **European Commission** is the precursor of this framework and will oversee and support its implementation at EU level, while the **EU Member States** should create the conditions to ensure a gradual adoption of the framework at national level. Moreover, both the European Commission and the EU Members States could potentially be interested in the data that would be generated from the awarded qualifications. These data could be useful for policy-making purposes, such as job forecasting, educational planning, skills-matching, among others. Finally, **accreditation bodies**[16] may have an interest in ensuring that only authorised awarding bodies are allowed to issue credentials/qualifications.

[16] In the public sector, accreditation bodies are typically Quality Assurance Agencies for Higher Education (see, for example, https://www.eqar.eu/register/map/?list=true), and Ministries of Education for compulsory education. In the private sector, professional associations or multi-national companies can often design their own qualifications and then accredit training centres to provide them.

The framework is designed to accrue multiple benefits to each of the stakeholders taking part of this ecosystem. These benefits are listed in the table below.

Stakeholder	Desired outcomes
 Credential owners	• Enable the possibility to create a single portfolio of all learning achievements across a lifetime in a standardised format; • Avoid diploma mills thanks to easy verification of accreditation status of qualifications; • Experience a more efficient application procedure to higher education institutions leading to a complete paperless application process; • Facilitate the creation of verified public profiles for jobseekers to promote themselves on the job market; • Automate paperless submission of credentials to employers or other organisations; and • Control access to the information in their credentials.
 Awarding Bodies	• Reduce the cost for issuing secure credentials; • Eliminate administration of verifying credentials; and • Decrease costs in verifying records as part of admissions processes
 Employers and other organisations	• Contribute to significant efficiency gains in processing recruitment applications; • Ensure more certainty and transparency in recruitment; • Reduce costs in verifying credentials; and • Receive less fraudulent credential.
 European Commission	• Support the implementation of the European Educational Area through improved recognition, transparency of credentials; • Combat cross-border crime, in particular credential-fraud; and • Improve labour mobility by standardising formats for credentials and facilitating understanding of foreign-awarded credentials.
 Member States	• Contribute to significant efficiency gains from standardised structures for all credentials; and • Reduce workload for ENIC/NARIC points.
 Accreditation Bodies	• Create a definite, reliable infrastructure to support the publication of accreditation decisions; and • Establish a single source of information for accredited qualifications in Europe, which may reduce the scope of diploma mills to defraud persons.

3. Conceptual model

A conceptual model has been created to identify and explain the fundamental propositions and basic functions of the framework for digitally-signed credentials. This model is also aimed at defining the minimum requirements and tools to implement the framework. The main components of this conceptual model include:

1) **Principles**, which are aimed at governing the framework as a whole;
2) **Functions**, which describe the different purposes of the framework according to its governing principles. Moreover, the functions should serve an ecosystem of stakeholders;
3) **Infrastructure**, which encompasses the main functional building blocks (e.g. services and software) that should be tailored to addressing the needs of the functions and the specificities of the standards of the framework; and
4) **Standards**, which should be understood as the foundation that supports and sustains the other components.

A representation of the conceptual model can be found below. Each component of the framework is described in more detail in the subsequent sections of this chapter.

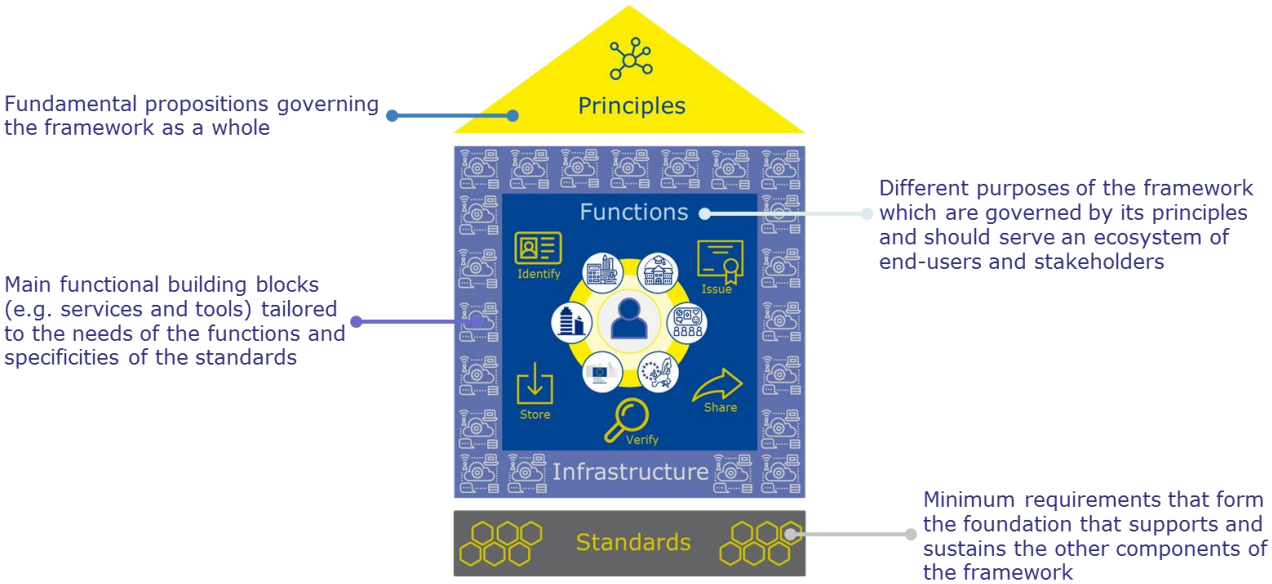

Figure 5. Conceptual model for a framework for digitally-signed credentials

3.1. Principles

A set of 10 principles have been created to govern the framework for digitally-signed credentials. They are aimed at underpinning the functions, infrastructure and standards of the framework.

User-Centricity. A diverse ecosystem of stakeholders will be making use of and/or benefiting from the framework, as well as supporting its implementation. Their needs vary considerably and they should be taken into account when defining the use cases for the framework. In addition, the needs and requirements of distinct stakeholders should be carefully analysed and integrated when designing and developing the infrastructure that allows for identifying, awarding, storing, sharing and verifying a certificate. As such, the infrastructure of the framework should be *easy to use* for all stakeholders. Lastly, individuals should be at the centre of the framework. Their learning achievements trigger the award of a digital certificate, and they control whom to share it with for verification.

Subsidiarity and Proportionality. The European Union is governed by the principles of subsidiarity and proportionality, under which *decentralisation* is favoured unless *centralisation* is in the public interest. Moreover, efforts to set up and implement the framework should be aligned with its needs and objectives. Centralised systems are generally easier to manage than decentralised systems as they operate on a single standard. The former also tend to be of lower complexity and therefore easier to use as well as having a lower overall cost of operation (due to efficiencies of scale). However, once implemented, the sheer size of centralised systems means that systems can be difficult and expensive to iterate and can stifle innovation.

Inclusion and accessibility. The framework should consider the *diversity* of individuals who are going to be awarded, store and share digital certificates. In addition, it should also take into account the individuals who issue and verify them. *Multilingualism* is an important feature of the framework as it fosters inclusion by making it possible to understand the content of digital certificates (i.e. recognised skills, competences and qualifications), at least, at EU level. The infrastructure of the framework should be *accessible* to all individuals (including people with disabilities, elderly and other disadvantaged groups) regardless of their level of digital skills.

Openness. Considering that this framework is aimed at encouraging the gradual adoption of digital certificates, it should be built on open standards and foster the use of open source software technologies. Such open approaches tend to reduce costs, promote collaboration between different parties, ensure interoperability, and reduce the risk of lock-ins with dominant solution providers, allowing thus for flexibility and freedom.

Data protection by design and by default. In accordance with the General Data Protection Regulation (GDPR), the framework should ensure the implementation of technical and organisational measures, such as pseudonymisation and data minimisation, in order to collect and process only the strictly necessary personal data for each specific purpose (particularly, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility). The fullest embodiment of the principle is *self-sovereignty* whereby an individual has direct ownership and control over their own data.

Interoperability. Stakeholders should be able to seamlessly interact with various qualifications platforms, by exchanging information within or outside of the Europass2 ecosystem, related to their identities (DIDs) and their public and personal data (while ensuring full compliance with the GDPR).

Transparency. The infrastructure of the framework should present each end-user and stakeholder the correct information at the right time to allow them to use a digital qualification for its intended purpose. Transparency applies to the standards used for identification, issue, storage, sharing and verification. It implies *traceability* of how each function is implemented each time it is used, availability of the underlying metadata within a digital qualification and of summative data on the whole system to stakeholders.

Resilience. The system should continue functioning and reliably offering its services even in the face of adverse conditions. As such, the framework and its infrastructure should be *resistant to fraud* (i.e. from malicious use of the system for unintended purposes), and ensure *data integrity* (i.e. protection of data from unauthorised changes due to hacking) and *data availability* (i.e. ensuring that data are always accessible and are not destroyed by natural disasters, mistakes in technical implementations or hacks).

Reusability. Existing solutions, specifications, standards and tools developed by others which have proven to be sound, useful and relevant elsewhere should be considered and reused to the

extent possible. Furthermore, new solutions, specifications, standards and tools should be further reusable by others in the public interest.

Credentials as a Public Good. Awarding qualifications, and recognising and validating the competences and skills of individuals is in the public interest of the EU Member States. The technical infrastructure should therefore take into account that certain credentials can only be issued by accredited awarding bodies according to pre-set rules.

3.2. Functions

The framework for digitally-signed qualifications serves an ecosystem of stakeholders. This ecosystem puts individuals at its core as the data owners. They will be awarded digital certificates which document their lifelong learning outcomes. This ecosystem is also comprised of *education and training institutions, businesses and civil society organisations* which *issue* digitally-signed qualifications (which can later be stored and shared by individuals), as well as *employers and other organisations* which will *verify* them. Finally, European and national stakeholders will *support the implementation* of the framework, namely the European Commission, the EU Member States and accreditation bodies.

In order to better serve the ecosystem of stakeholders, the framework should have different functions which are, at the same time, governed by the principles. This conceptual model encompasses five distinct functions:

- **Identify** the individual who is going to be awarded a certificate documenting her/his skills, competences or qualifications;
- **Issue** a digitally-signed credential or a revocation certificate to an individual. Both certificates should be issued by an awarding body;
- **Store** the digital certificate after having been issued by an awarding body. Individuals should have the possibility to save their certificate to the Europass's e-Portfolio or other platforms and wallets;
- **Share** the digital certificate with an employer or other organisations. Individuals should be able to decide with whom they wish to share their certificate with; and
- **Verify** the authenticity of the digital certificate that has been willingly shared by an individual with an employer or other organisations. The accreditation of the awarding body could also be verified (i.e. if an awarding body is authorised to issue a certain certification about a specific qualification).

The system should also be able to support distinct **credential-types** as well as **multiple workflows** for issuing and verifying those qualification-types. Thus, the system would be able to support, for instance, EQF-linked formal qualifications awarded by accredited education and training institutions, non-formal qualifications (including industry-certifications or training awarded by civil society organisations), qualifications validating non-formal and informal learning outcomes awarded by competent authorities, or those awarded by employers documenting employment experiences.

3.3. Infrastructure

The infrastructure encompasses several building blocks (e.g. services and software) which are aimed at helping operationalise the framework. The infrastructure should address the needs of the functions and the specificities of the standards of the framework. The functions identified above need to be translated into specific services which, in turn, will be delivered through tailored software components.

3.4. Standards

The standards establish a number of minimum requirements that support and sustain the other components of the framework. As a guiding rule, open standards should be used as they facilitate interoperability and data exchange, while fostering a cooperative approach to maintain and further develop them, and contributing to its adoption. European classification systems and reference frameworks (including EQF and ESCO) play an important role in ensuring a shared understanding of qualifications and in utilising a multilingual common reference terminology within and beyond the European Union. The following combination of standards will be particularly considered within this framework:

- **Base standard for a Europass digitally-signed qualification:** this standard would define the minimum properties of any qualification to be included within the Europass framework for digitally-signed qualifications and determine a link to ESCO;
- **Metadata standards for individual qualifications:** each type of qualification/credential to be integrated into the system will require an associated metadata standard (for instance, based on EQF, ECTS or ECVET). These standards will also require the definition of relations between different qualifications/credentials and credits-systems (e.g. between ECTS and academic degrees);
- **Technical standards:** in particular those governing the signature and verification of qualifications/credentials, as well as any application programming interfaces (APIs) required to access data;
- **Workflow management standards:** for each type of qualification/credential a work-flow standard would determine: the steps required in identification, issuance, storage, verification and sharing; the actors involved in each step and their various roles; and any specific rules or requirements for the steps.

4. A European Digital Credentials Infrastructure (EDCI)

The European Digital Credentials Infrastructure (EDCI) encompasses the technical specifications to implement the framework for digitally-signed credentials. The emphasis on 'infrastructure' recognises the existence of the core building blocks of standards, software and services which are aimed at helping operationalise the framework. The EDCI should address the needs of the functions and the specificities of the standards of the underlying framework, which in turn are translated into specific services and delivered through tailored software components.

The next sections describe a set of six inter-related criteria, presented as the key business needs of the identified stakeholders, which should, in turn, underpin and govern the functions, infrastructure and standards of the EDCI and its supporting framework as a whole.

4.1. Security of credentials

The EDCI must be designed to **provide security, data privacy and trust** in digitally-signed credentials as a default component of the system. The personal data of the credential owners need to be secured, while a wide range of stakeholders, such as employers, education and training institutions, public and private employment services or civil society organisations need to be able to verify the authenticity and validity of digitally-signed credentials.

Credentials need to be maintained and made available for the long-term (ideally in perpetuity). In the case of self-hosting solutions, the maintenance of online records implies ongoing custodial responsibilities and costs. Very few awarding bodies are likely to remain in existence for a lifetime, yet credential owners need to have the confidence that proof of their accomplishments will remain available for a long period of time, even if the organisation changes or ceases to exist.

Hosting credentials may provide a convenient way for credential owners to share a link, but it does not provide confidence for *verifiers*. If new credentials are going to gain the gravitas of traditional records, they will have to be stored in a more secure format. The EDCI must be designed to identify, issue, store, share and verify digitally-signed credentials in an independently verifiable format. Public or private blockchain technologies, peer-to-peer files systems (IPFS), among others, may provide immutability for digitally-signed credentials. The EDCI should continue functioning and reliably offer its services even in the face of adverse conditions.

4.2. Transparency and provenance of credentials

The EDCI must provide stakeholders with functionalities that will enable them to easily verify the authenticity of the digitally-signed credentials. The recognition of skills, competences and qualifications acquired in formal, informal and non-formal contexts throughout a credential owner's life is very much associated with the ability to easily and cost-effectively assess the provenance of those credentials. Trust in digitally-signed credentials in an independently verifiable format in cyberspace is based on two key requirements:

- **Authentication**, i.e. *prove to me that you are who you say you are*; and
- **Authorisation**, i.e. *prove to me that you have the necessary permissions to do what you ask*.

In an orthodox online transaction, trust is achieved by automating three functions traditionally left to a 'trusted third party' or intermediary, such as a bank: a) *validating; b) safeguarding*; and *c)* then *preserving* transactions. Within the context of digitally-signed credentials, trust in their transparency and provenance is vested in the technologies deployed to store and verify credentials.

Blockchain and Public Key Infrastructure (PKI) technologies are closely associated with the verification process. The main difference between PKI and blockchains is that, with blockchains, the verification authority is being decentralised. The technical benefits of this are independent time-stamping and a globally redundant network for instant verification. **Independent time-stamping** is a security enhancement beyond traditional PKI. A blockchain provides its own timestamp for when each credential was conferred to an owner, which is a type of transaction. This ultimately gives awarding bodies the ability to rotate their issuing keys without undermining the ability to verify those transactions. They are not surrendering any authority in this situation. They still issue, store the records as they always have; they are simply gaining a level of security that did not exist before. Overall, blockchains offer promising new features which help to achieve security goals while enabling individuals to hold their own official records, independent of any authority.

From a process perspective, this requires checking that the credential originated from a particular awarding body while that issuing key was valid, which needs a timestamp beyond anything written into the credential itself. If a private key is ever compromised, nothing prevents an attacker from issuing fake credentials and backdating in the content. Even if an awarding body publicly revoked those fake credentials, an independent verifier would not know the difference between a valid and invalid credential, unless there were some reliable sources of when the transaction took place. A network of thousands of computers that all contain the same copy of historical transactions removes the vulnerability of relying upon a single authority. The effect is improved availability, the capacity to independently verify, and redundancy that avoids single points of failure.

The EDCI should present each stakeholder the correct information at the right time to allow them to use a digitally-signed credential for its intended purpose. Transparency applies to the standards used for identification, issuance, storage, sharing and verification. It implies **traceability** of how each function is implemented each time it is used, availability of the underlying metadata within a digitally-signed credential and of summative data on the whole system to stakeholders.

If credentials are to continue to be considered a 'public good', where the recognition and validation of the skills and competences of individuals is in the public interest of the EU Member States, then the EDCI must take into account that **certain credentials can only be issued by accredited awarding bodies** according to pre-set rules.

Finally, from a broader perspective, the EDCI should consider the **diversity** of credential owners who are going to be awarded, store and share digital certificates. In addition, it should also take into account the individuals who issue and verify them. **Multilingualism** is an important feature of the framework as it fosters inclusion by making it possible to understand the content of digitally-signed credentials (i.e. recognised skills, competences and qualifications), at least, at EU level. The EDCI should aim to be **accessible** to all individuals (including people with disabilities, elderly and other disadvantaged groups) regardless of their level of digital skills.

4.3. Ownership with potential to share credentials without lock-in

The power to issue a digitally-signed credential always resides with an awarding body. Yet the ownership of credentials lies with credential owners who are empowered to own, manage and share details of their credentials, without the need to call upon the awarding body as a trusted intermediary. This can also be thought of as credential owners acquiring significant 'self-authority' over the way personal data and identity are shared online and being able to choose to release all or parts of it in return for access to services they want – *without the need of constant recourse to a third party intermediary* to validate such data or identity.

Ideally, credentials should not have ongoing dependence upon an awarding body or vendor (e.g. of an IT solution) in order to be accessed, shared, or verified. This is the only way to provide a verification infrastructure that has no single point of failure. Owners can hold and share their digitally-signed credentials, and this new public infrastructure must allow for those credentials to have a **durable and long-lasting source of independent verification**. As a rule, stakeholders must be able to access the credential and all related information, such as transcripts, through a cost-effective EDCI. Lowering the cost of issuing credentials for awarding bodies and credential owners has to extend to the checking and verification of credentials to employers and other organisations. Within this context, ownership is very much linked to the concept of **digital self-sovereign identity**. Within an educational context, the term is on its way to becoming synonymous with the empowerment of individual learners to own, manage and share details of their credentials, without the need to call upon the education institution as a trusted intermediary. This can also be thought of as citizens acquiring significant 'self-authority' over the way personal data and identity are shared online, and being able to choose to release all or parts of it in return for access to services they want – without the need of constant recourse to a third party intermediary to validate such data or identity. Owners have the right to own and use their credential records in a manner that is private and that has **no dependence** upon outside agents or vendors in order to share or verify digitally-signed credentials. Ideally, the option for self-sovereignty needs to be explicitly architected into the EDCI.

The EDCI should facilitate the choice of stakeholders (from credential owners, awarding bodies and verifiers, to other organisations that have a supporting role) who do not wish to be locked in with intermediaries (be they awarding bodies or product vendors). **Openness** (open-source, open-access, borderless, neutral) goes a long way to preventing such lock-ins.

4.4. Mitigation of risks for credential fraud

Fraud inevitably has an impact on the reputation of awarding bodies (particularly traditional higher education institutions). It is a pre-requisite that no credential owner or verifier (or even an individual within an awarding body) can tamper with a credential after it has been recorded by an awarding body or verified by multiple employers or other organisations. Attempts to change digital data in one location must be capable of being interpreted as fraudulent and an attack on the record's integrity, with the result that it will be rejected (e.g. by the awarding body that issued it). The EDCI should this be **resistant to fraud** (i.e. from malicious use of the system for unintended purposes) and ensure **data integrity** (i.e. protection of data from unauthorised changes) and **data availability** (i.e. making sure that data are always accessible and are not destroyed by natural disasters, mistakes in technical implementations or hacks).

Digitally-signed credentials need to be **tamper-proof**. There are many risks associated with paper-based certificates; for instance, diploma mills are rife in many parts of the world. In practice, many digitally-signed credentials can be effortlessly spoofed, particularly 'verification

sites' which, in some instances, are simply webpage scams and may be easy to fake (a slightly altered domain name can be hard to spot). Image files with information attached (such as Open Badges) are easily shareable as a discrete object and, prima facie, appear to provide greater comfort. However, when verification occurs, it is not the visible badge on display which is checked but the hosted version of that badge. This means the display of a badge could be completely changed and it would still be successfully verified. Therefore, such online representations are not advisable as they cannot be completely and securely verified.

4.5. Facilitation of interoperable credentials

Interoperability refers to the ability of IT systems to exchange information between them. Stakeholders will need to be able to seamlessly interact with various qualifications platforms, by **exchanging information within or outside of the Europass2 ecosystem**, related to their identities (decentralised identifiers) and their public and personal data (while ensuring full compliance with the General Data Protection Regulation).

Interoperability also means that the EDCI can interact with other systems within the European Higher Education Area, in particular those set up by the Bologna and Copenhagen Processes. These include the Procedures of the ENIC/NARIC Networks, the European Credit Transfer and Accumulation System (ECTS), the Diploma and Credential Supplements, the Overarching and National Qualification Frameworks, the European Standards and Guidelines for Quality Assurance of Higher Education, the European Credit System for Vocational Education and Training (ECVET), and the European Quality Assurance for Vocational Education and Training (EQAVET).

As such, the business need does not just lie on securing a better user experience, but also on ensuring that the EDCI is future-proof. Organisations need to interact with others with the objective of attaining mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems[17]. Technical interoperability should thus support the possibility that awarding bodies (and other organisations that wish to contribute to the community) begin to develop and re-use open standards so that digitally-signed credentials can operate outside of *walled gardens* (i.e. IT environments that would control the stakeholders' access to the EDCI) and be recognised and accessed anywhere in the EU and beyond.

4.6. Data protection by design and by default

In accordance with GDPR, the EDCI should ensure the implementation of technical and organisational measures, such as pseudonymisation and data minimisation. These measures are aimed at collecting and processing only the strictly necessary personal data for each specific purpose (particularly, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility). The fullest embodiment of the principle is **self-sovereignty** whereby an individual has direct ownership and control over their own data in all times.

[17] European Union (2017). New European Interoperability Framework – Promoting seamless services and data flows for European public administrations. Luxembourg: Publications office

5. EDCI's business rules

This chapter is aimed at defining the structure of the EDCI and its behaviour. Business rules have been defined for each function of the framework for digitally-signed credentials, namely identify, issue, store, share and verify. Different building blocks envisaged as part of the EDCI (described in chapter 6) will be referenced throughout the following sections.

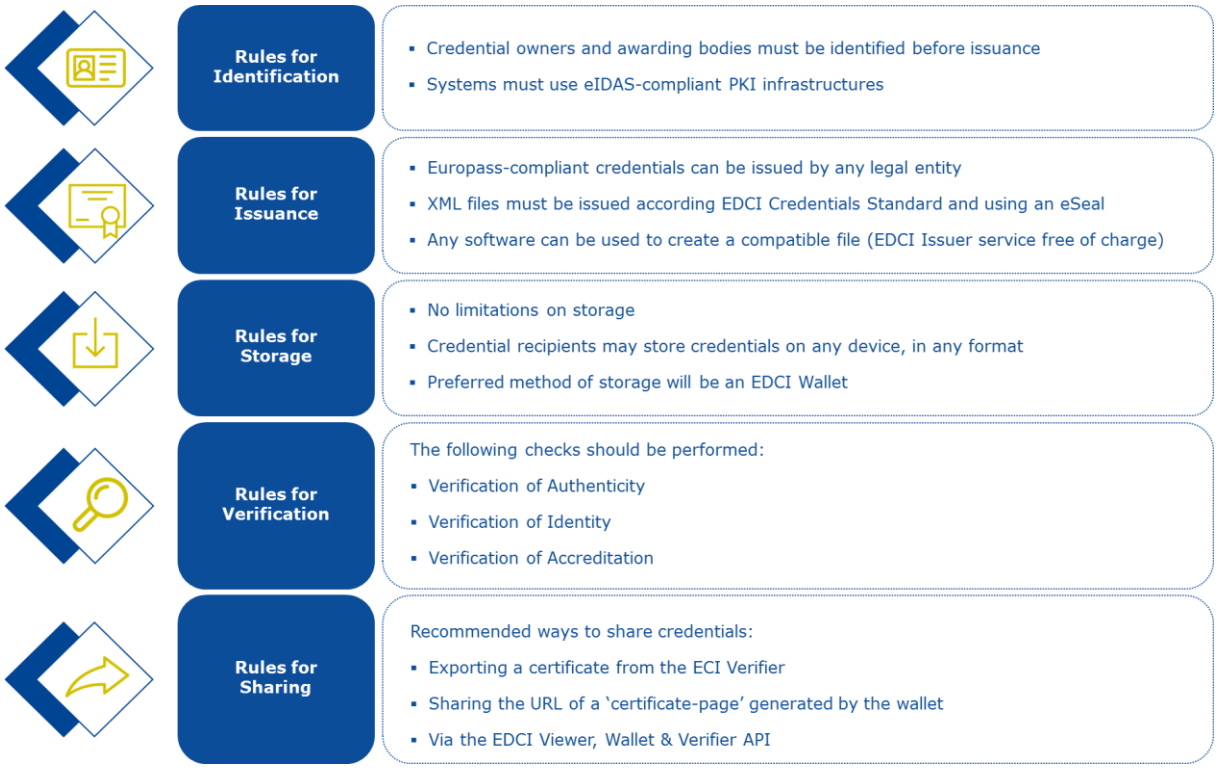

Figure 6. Overview of the business rules

5.1. Rules for Identification

Credential owners and awarding bodies must be identified to trigger the issuance of digitally-signed credentials. Therefore, the proposed solution will rely on **eIDAS-compliant PKI infrastructures** to identify persons (i.e. credential owners) and organisations (i.e. awarding bodies). The system will require a 'substantial' or 'high' trust level for all transactions[18], while using a secondary identification option only for credential owners who cannot obtain suitable qualified digital keys (e.g. third country nationals).

This means that identity of awarding bodies and of credential owners will be initially ascertained by **Trust Service Providers**[19] in each Member State, and then verified for the purposes of the EDCI by using qualified electronic seals (in the case of legal entities) and/or digital signatures (in the case of natural persons) which have been issued by those Trust Service Providers.

[18] These trust levels are intended in the sense meant by the eIDAS Directive.
[19] The EU keeps a database of nationally accredited Trust Service Providers at: https://webgate.ec.europa.eu/tl-browser/#/.

5.2. Rules for Issuance

Any legal entity can issue a Europass2-compliant credential, however only organisations with appropriate national accreditation may issue accredited qualifications. Any XML file which is issued according to the requirements of the Europass2 **EDCI Credentials Standard** and sealed using an **e-Seal** is considered to be a Europass2-compliant credential.

When issuing a credential, an awarding body must also indicate in the credential the URL of a revocation list, where they commit to publish a revocation certificate should this be required in the future. The format of Revocation Certificates and the features of a compatible revocation list will be determined by the **EDCI Credential Revocation Standard**.

Any software may be used to create a compatible file. The European Commission provides an **EDCI Issuer** service free of charge to do so, as well as provide code samples for third party integration, e.g. into HRMS or SIS as part of the **EDCI Code Library**.

Regardless of the technical solution, as long as an awarding body follows the aforementioned eSeal directive and the **EDCI Credentials Standard**, any technology for issuing credentials can be used.

5.3. Rules for Storage

There are no limitations on storage. Credentials owners may store the delivered credential on any device, in any format. The **EDCI Credential Standard** does not specify any limitations as to whether the awarding body may keep its own copy of the credentials, but merely specifies that an awarding body must indicate its retention policy in the credential itself.

The preferred method of storage of a digitally-signed credential will be in an **EDCI Wallet**, but owners will not be required to use a wallet to store credentials. The European Commission is advised to provide an **EDCI Wallet** service free of charge, as well as code samples for third parties to integrate EDCI Wallets into their own software, as part of the **EDCI Code Library**.

The EDCI will use XML so that the mark-up in the files will be readable with a text editor. A simple browser application, the **EDCI Viewer**, will be able to render the digitally-signed credentials directly, without the need for any stakeholder (e.g. a learner or an employer) to store any information in a database.

5.4. Rules for Verification

Credentials can be rendered and parsed by **EDCI Viewer** software, which will allow for the display, export and verification of credentials. The software will be designed according to the requirements of the EDCI Viewer, Wallet & Verifier Standard. The European Commission will provide the first implementation of the standard as a free of charge progressive web app, as well as code snippets for third party integration as part of the **EDCI Code Library**.

Third-party vendors of **EDCI Viewer** software will be able to certify that their software complies with the standard by applying for an audit done in line with the **EDCI Viewer, Wallet & Verifier Certification standard**, which will outline audit requirements.

Individuals who do not wish to use the EDCI-Viewer would still be able to view the credential by opening it in a text viewer, but would not be able to automatically verify the credential, or to render it according to the rules set by the issuer.

5.4.1. Rules for Verification of Authenticity

In this case, the verifier (e.g. an employer) would automatically do the following checks on all types of credentials to verify authenticity:

- Has the credential been issued according to the standard specified for that credential-type? (technical check of XML file for validity);
- Did the awarding body really issue the certificate? (check of the e-seal);
- Is the credential still valid? (check against expiry information embedded in certificate); and
- Has the certificate been revoked? (check against revocation list)

All the above checks will be able to PASS or FAIL, while the revocation check may also be UNABLE TO VERIFY if the revocation list cannot be accessed.

5.4.2. Rules for Verification of Identity

Where a credential owner chooses to authenticate themselves to the **EDCI Viewer** software using a qualified electronic signature, the following check will be performed:

- Is the person presenting the certificate the owner? (comparison of personally identifiable information embedded in the certificate with that of wallet owner); and

The check can PASS or FAIL, depending on whether the information matches. If the check cannot be performed, the EDCI Viewer will mark it as UNABLE TO VERIFY.

5.4.3. Rules for Verification of Accreditation

Where the credential being verified is an *accredited qualification* (see chapter 2 for more information about the types of credentials), the following additional check must be performed:

- Is the awarding body authorised to issue the qualification? (check against **EDCI Accreditation database**).

The check can PASS or FAIL, depending on whether the awarding body and qualification are found in the accreditation database.

To operate the accreditation checks, an **EU-level blockchain**, operated by the European Commission or a group of Member States, should hold a database of accreditation transactions recording each accreditation of qualification or revocation of accreditation of a qualification in the European Union. New or updated records will be added to such a database by the national authorities responsible for developing NQFs. Each authority would be able to delegate writing of records to other organisations under certain conditions (e.g. to a Quality Assurance Agency for Higher Education qualifications or to a Ministry of Education for school-leaving certificates). Each

transaction record would be secured via an electronic seal. The database would hold three types of information, including accreditation transaction records, transaction revocation records and qualification records. The figure below provides a definition for each type of information.

Figure 7. Types of information to be stored in the database

In this case, Member States would have the option of:

- Running their own database of **qualification records** which then would be scraped by the **EDCI Accreditation Database**; or
- Storing their original qualification records directly in the **EDCI Accreditation Database**.

5.5. Rules for Sharing

Sharing implies the transfer of both the data embedded in the digitally-signed credential and the results of all the verification checks described above to a third party (e.g. employer).

There are three recommended ways for a credential owner to share a credential:

- Exporting a certificate from the **EDCI Verifier** (as PDF, badge, printout, etc.);
- Sharing the URL of a 'certificate-page' generated by the wallet; and
- Via the **EDCI Viewer, Wallet & Verifier API**, whereby the underlying data of a credential in the wallet are shared with a third party application such as recruitment software.

While a credential owner could opt to store credentials on their device without using a wallet, and share them by transferring the XML file to a third party (e.g. via e-mail), this is not recommended, as the credential owner loses direct control over the credential.

For credentials stored in the wallet, owners will be able to publish credentials, or to implement granular access controls determining what is shared with whom and for how long.

All three methods for sharing a digitally-signed credential would always:

- Include the results of the verification checks in their outputs; as well as
- Contain all information for a third party to conduct them again themselves.

6. EDCI's building blocks

The EDCI would comprise **eIDAS components**, as well as **EDCI-specific standards, software and services**. These are depicted in the figure below. A brief description of the main building blocks of the EDCI can be found in the sections that follow.

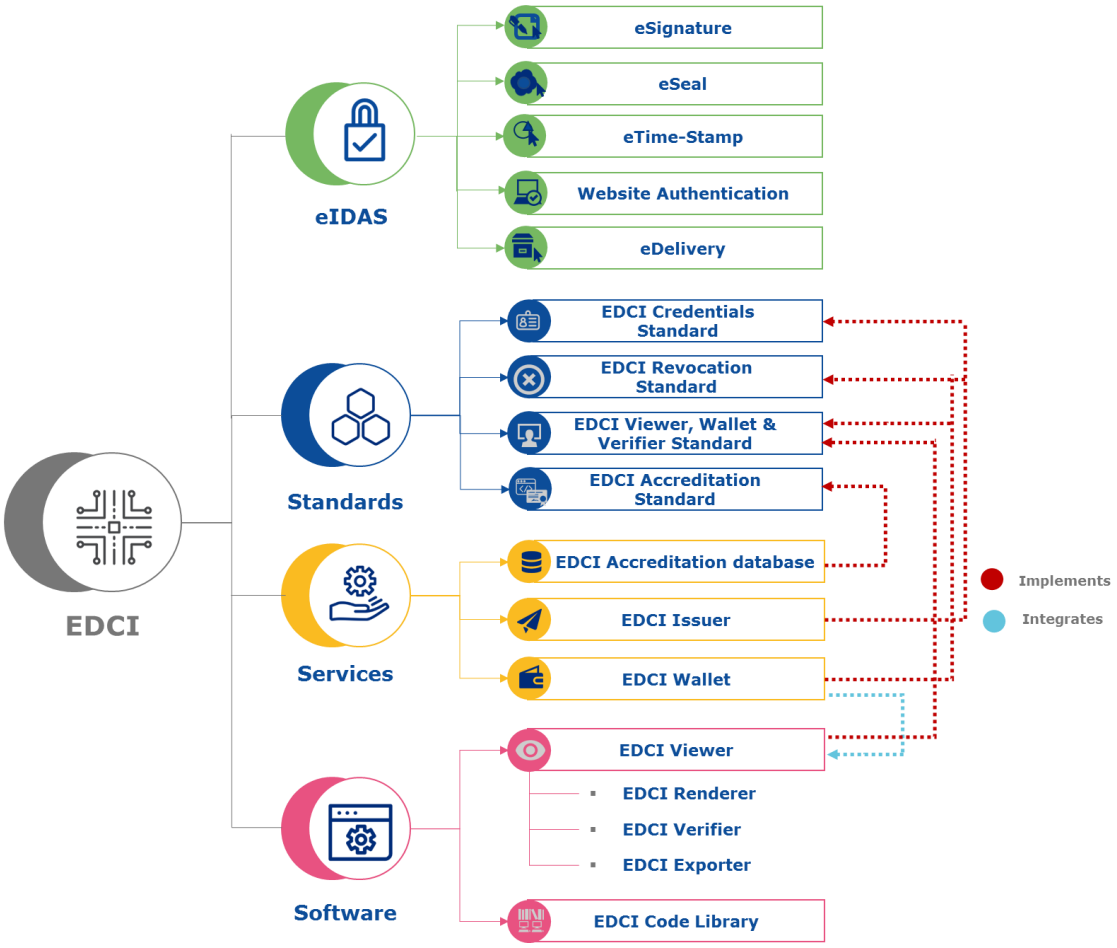

Figure 8. Overview of the main building blocks of the EDCI and how they interact

6.1. eIDAS Components

All building blocks below lean heavily on the eIDAS family of trust services. These are depicted in the figure below.

Figure 9. Main services from the eIDAS relevant to the EDCI

In these requirements, all use of the above terms should be read in the sense understood by the eIDAS directive. Under these requirements:

- **eSignature** in combination with eIdentification (eID) is used to identify credential owners;
- **eSeal** is used to authenticate awarding bodies, and digitally seal credentials;
- **eTime-Stamp** is used to timestamp all transactions by all parts of the system;
- **Website Authentication** is used to secure and authenticate all web-delivered data; and
- **eDelivery** is used to transfer credentials into wallets.

6.2. Standards

The EDCI will consist of a set of four standards which may be directly published by the European Commission, or published as formal standards via the European Committee for Standardisation (CEN). These include:

- **EDCI Credentials Standard** detailing the format, metadata and security features of a Europass-compliant digitally-signed credential;
- **EDCI Credential Revocation Standard** detailing the format of credential-revocation certificates, the requirements for revocation lists as well as the APIs to query such lists;
- **EDCI Viewer, Wallet & Verifier Standard** detailing the core functionalities of EDCI-compliant wallet software, in particular the requirements for verification checks, along with the **EDCI Viewer, Wallet & Verifier Certification Standard** which will detail requirements to audit that a wallet is in compliance with EDCI Wallet Standard; and

- **EDCI Accreditation Standard** detailing how Member States should store qualification data to make them accessible by EU services, how they can directly write to the **EDCI Accreditation Database** via API and how third parties' software can query the **EDCI Accreditation Database** via API.

To enhance overall adoption, it is strongly recommended that EDCIs should replace all national standards describing digital formats of credentials. As such, all EDCI Standards should be published as formal standards through the European Committee on Standardisation (CEN)[20].

6.3. Software

The EDCI will include the following pieces of software:

- **EDCI Viewer** allowing credential owners to view and verify credentials on supported devices;
- **EDCI Code Library** consisting of documented code snippets taken from the **EDCI Wallet** and the **EDCI Issuer**, assisting third parties to develop their own versions of software or to integrate third parties' systems with EDCI services.

6.3.1. EDCI Viewer

The EDCI Viewer is made up of three modules, namely the:

- **EDCI Renderer** allowing a user to view a credential in a graphical format indicated by the awarding body;
- **EDCI Verifier** running the checks described in the 'rules for verification' against the credential; and
- **EDCI Exporter** allowing conversion of the credential into other formats such as PDF or open badges.

The software should be made available on as many devices as possible.

6.3.2. EDCI Code Library

The EDCI Code Library will be a git repository managed by the European Commission[21], with code samples and documentation which would allow third party developers to integrate EDCI-components into their own software and services. As such, the **EDCI Code Library** will contain code examples from the European Commission's own implementations of an:

- EDCI Issuer;
- EDCI Viewer, including EDCI Renderer, EDCI Verifier and EDCI Exporter modules;
- EDCI Wallet; and

[20] The process to implement such standardisation is described here: https://www.cen.eu/work/supportLegislation/Mandates/Pages/default.aspx
[21] The EU already manages such repositories for numerous other projects at https://github.com/ec-europa

- Europass2 Application Tracker (as an example of integrating the EDCI Wallet APIs into HRM-recruitment software).

Needless to say that the above listed modules will be based upon the standards defined above.

6.4. Services

The following services will run as cloud-based web-services to support the implementation of the EDCI:

- **EDCI Accreditation Database** consisting of a registry of all accredited credentials mapped to the EQF;
- **EDCI Issuer** consisting of a web-based software tool that will allow any awarding body (namely education and training institutions) to issue batches of credentials; and
- **EDCI Wallet** consisting of a web-based wallet whereby any owner will be able to view, store, verify and share their credentials in the cloud.