



RECOGNITION AND VERIFICATION OF CREDENTIALS IN OPEN EDUCATION

Report of Intellectual Output 3

Authors

Ehrenreich, Jochen; Mazar, Ildiko; Rampelt, Florian; Schünemann, Isabel; Sood, Ira

Contributors

Camilleri, Anthony; Crnko, Mihajela; Orlic, Davor; Wiechmann, Svenja

Editor

Ehrenreich, Jochen

Layout

Tara Drev

Copyright

(C) 2020, OEPASS Consortium

The Oepass Consortium

Duale Hochschule Baden-Württemberg Heilbronn
Stifterverband
European Distance and e-Learning Network
Budapest University of Technology and Economics
Lithuanian Association of Distance and e-Learning
Knowledge Innovation Centre
National Distance Education University
Tampere University of Technology

DHBW	DE
SV	DE
EDEN	UK
BME	HU
LieDm	LT
KIC	MT
UNED	ES
TAU	FI

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International



Co-funded by the
Erasmus+ Programme
of the European Union



Table of Contents

Abbreviations	5
Summary.....	6
Improving the Portability and Recognition of Open Learning.....	6
Basic Concept 1: Meta-Data Standard.....	7
Basic Concept 2: Learning Passport.....	7
Policy Recommendations	8
1 Introduction	9
Report Structure	11
2 Identification of technologies used for recognising and verifying open credentials.....	12
2.1 Paper Certificates.....	12
2.1.1 Limitations of Paper Certificates.....	12
2.2 Digital Certificates	13
2.2.1 Open Badges as Digital Certificates	14
2.2.2 Micro-Credentials	17
2.2.3 Digital Credentials	17
2.3 Unbundling.....	19
3 Technology in OEPass.....	20
3.1 Meta-Data Standard.....	21
3.2 Blockchain	22
3.2.1 Digital Certificates using Blockchain technology	23
3.3 Learning Passport.....	25
3.4 Integration and APIs	27
3.4.1 Front End Integration: Applications.....	27
3.4.2 Back End Integration: Campus IT Systems.....	27
4 Recognition	28
4.1 Standards and Guidelines for Recognition	28
4.2 Automated Credential Recognition.....	28
5 Identification of meta-data standards used for recognising and verifying open credentials	31
5.1 EUROLMAI & CWA 16133: Guidelines on a European Learner Mobility model.....	31
5.2 ELMO.....	32
5.3 Learning Object Metadata	32
5.4 Schema.org.....	32
5.5 Open Badges	33
5.6 Qualifications Meta-data Schema (QMS)	33
5.7 MicroHE Meta-data Standard	34
6 Proposition of an appropriate meta-data standard for the learning passport.....	35
6.1 Requirements for an Appropriate Standard	35
6.2 Assessment of existing standards	35
6.2.1 EUROLMAI & CWA 16133.....	36
6.2.2 ELMO.....	36
6.2.3 Learning Object Metadata	36
6.2.4 Schema.org.....	36

6.2.5	Open Badges	36
6.2.6	Qualifications Metadata Schema	37
6.2.7	MicroHE Meta-data standard.....	37
7	Proposition of an onto-logy for recognition of open learning	37
7.1	Learning Experience	38
7.2	Information identifying the awarding body	38
7.3	Information identifying the holder of the credential	39
7.4	Credit system	39
8	Policies and Regu-lations.....	40
9	Blockchain Questions and Answers	43
10	Appendix.....	49
	Appendix 1: Stakeholders for Consultation and Collaboration.....	49
	Appendix 2: ESCO, ISCO and EQF	51
	Appendix 3: EQF	53
	Annexe 4: Initiatives for Digital Credentials	53
11	References	56

Abbreviations

API	Application Programming Interface
ECTS	European Credit Transfer System
ECVET	European credit system for vocational education and training
EHEA	European Higher Education Area
ENIC	European Network of Information Centres in the European Region
EQF	European Qualifications Framework
ESCO	European Skills, Competences, Qualifications and Occupations
ESG	European Standards and Guidelines
HE	Higher Education
HEI	Higher Education Institutions
ID	Identity
ISCO	International Standard Classification of Occupations
MicroHE	Erasmus+ Project Support Future Learning Excellence through Micro-Credentialing in Higher Education
MIT	Massachusetts Institute of Technology
MOOC	Massive Open Online Course
NARIC	National Academic Recognition Information Centres in the European Union
NQF	National Qualifications Frameworks
OEPass	Open Education Passport, Erasmus+ Project
OER	Open Education Resources

Summary

Improving the Portability and Recognition of Open Learning

This report explores scenarios, stakeholders and guidelines to make online and open learning comparable and recognisable within higher education. This is challenging: while formal recognition according to the Lisbon Recognition Convention (LRC) is about recognising credits from *accredited study programmes* offered by different *higher education institutions*, open learning extends far beyond the realm of higher education. It includes different formats and providers in a wide range from formal to non-formal and even informal learning.

Physical Mobility: transfer credits	Virtual Mobility: transfer credits
between higher education institutions (HEIs)	from online and other non-traditional short learning programmes which might be offered not only by HEIs, but also by other education and training sectors
from accredited study programmes	which are typically not higher education accredited
with credits described in ECTS	which are often not described in ECTS, instead use alternative systems of credentials
with controlled assessment environments	where identity verification processes and assessments are more complex and challenging than in face-to-face settings
with learning agreement from home HEI	without formal statement from home HEI about the perception of externally acquired learning
with module description that provides information about workload, learning outcome and assessment conditions	which lack transparency regarding academic content and learning methodologies
→ Trust and Transparency	→ Lack of Trust and Transparency

Table 1: Challenges of Virtual Mobility.

We will propose a possible solution, which we call the Learning Passport, and lay out a system of technology, standardization, procedures and governance models to realize this solution. It aims at increasing trust in open and innovative practices, by providing valid pathways to recognition, at widening the scope of internationalisation and credit-mobility by fully encompassing virtual mobility experiences into Bologna-tools and lastly at improving the transparency and recognition of open qualifications. With the Learning Passport, we want to stimulate the development and discussion of such an open and interoperable system for digital credentials, building on the European Credit Transfer and Accumulation System (ECTS) and on the European Qualifications Framework (EQF).

Basic Concept 1: Meta-Data Standard

To achieve the credibility and accountability needed for formal recognition of open learning within the European higher education systems, the project OEPass (Open Education Passport) is creating a standard format for describing open education and virtual mobility experiences according to the standards and guidelines of the European Higher Education Area (EHEA). This Learning Passport should not only ensure accountable and verifiable documentation of open learning, but also facilitate the (potentially automated) translation of open learning credentials (which are sometimes called micro-credentials) into ECTS credits with a formal value for higher education.

The Learning Passport thus provides higher education institutions with sufficient information so that they can make an informed and consistent decision on whether to recognize such a micro-credential as ECTS credit towards a specific degree programme.

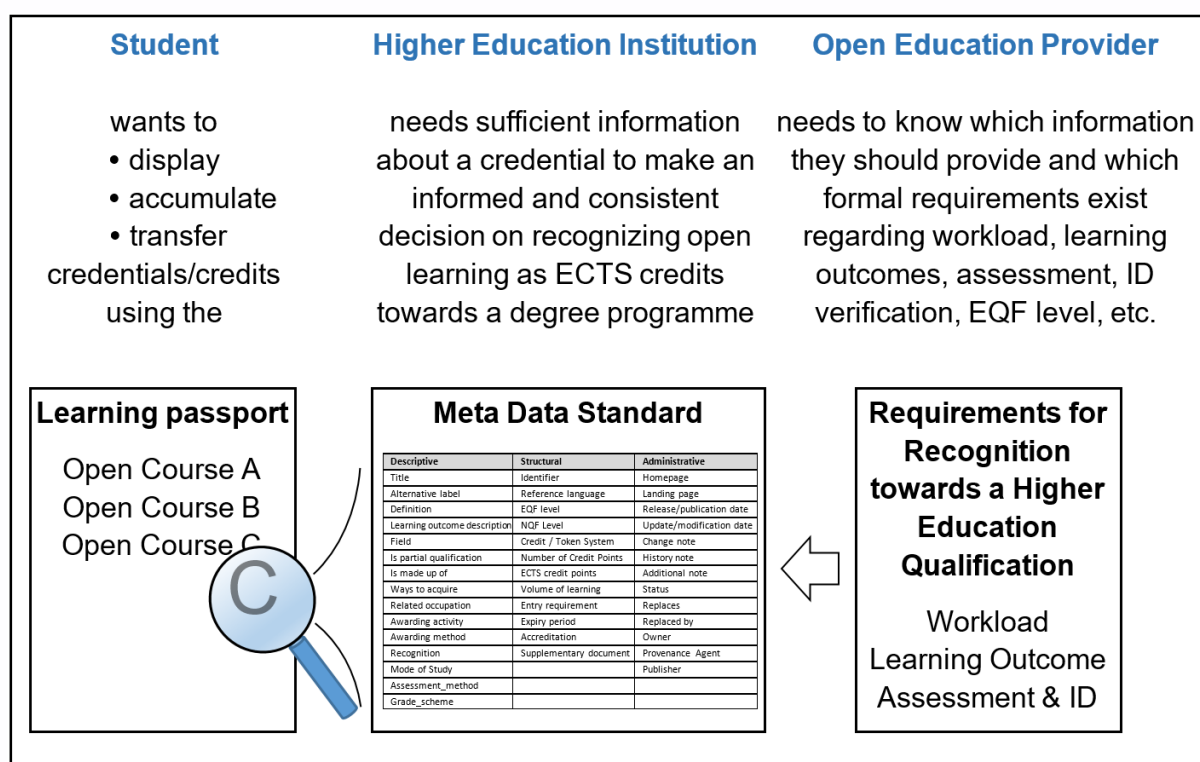


Figure 1: Basic concept of the Meta-Data Standard.

Basic Concept 2: Learning Passport

The Learning Passport could pave the way for the transition from paper-based to digital credentials in the European Higher Education Area. We envisage that a *digital credentialing solution* would include the following components:

- a secure digital Learning Passport where students and lifelong learners collect credentials from various formal and non-formal (possibly also informal) learning experiences,
- a way for students to share such credentials, for example in CVs, online portfolios etc.,

- an international consortium of educational institutions jointly operating the digital credentialing solution and taking responsibility for governance and evolution of the Learning Passport, as well as for admission of new full and associate members,
- digital certificates/credentials issued to a student by members of the consortium,
- a way to ensure that only consortium members, i.e., accredited institutions, can issue such digital credentials,
- a way to authenticate the certificate and ensure its validity,
- a way to verify the learning outcomes (described in ECTS) documented by the credential, as well as its link to the EQF, automatically.

Many initiatives around the world are developing and proposing digital credentialing solutions, often using Blockchain technology for verifiable transactions. Well-known examples are Open Badges and Blockcerts, illustrating the wide range of possible applications from badges for participation to micro-credentials and even full academic degrees. Identifying a single best solution is not easy. Most likely, a number of open-source, interoperable technologies will emerge, and these standards and technologies will evolve through the support of a community.

Policy Recommendations

Technology

- Establish a European Meta-Data Standard for Open Learning Recognition
- Establish a European Learning Passport
- Provide guidance for HEIs on the transition pathway towards Digital Credentials
- Promote a European discussion and consensus on the usage of Blockchain technology for Digital Credentialing

Standards and Guidelines for Recognition

- Promote a European discussion and consensus on Standards and Guidelines for Open Learning Recognition
- Encourage HEIs to embrace the trend towards Unbundling of Education

Policies and Regulations

- Promote the establishment of a Meta-Data Standard and a Learning Passport through European Policy Instruments: Bologna process, Europass and ESCO

1 Introduction

An ‘open credential’ could be defined as a credential which is fully transparent and which can be used for a multitude of purposes. These might include accumulation towards a qualification, as evidence of skills for employment or as a means of transferring evidence of expertise between countries. Such an open credential would fit seamlessly into European recognition frameworks, and would be instantly verifiable at the click of a button, and would include all necessary information about the learning it represents. It would also allow collection by various software systems to create online CVs, backpacks etc.

Initial work has already been done in this area by MIT and by the Open University (UK), and the OEPass partnership contributed to this area of work by suggesting:

- A standard set of meta-data descriptors for recognising open learning in line with the learning passport¹;
- An implementation guide for using Blockchain (or other centralised digital certificate schemes) to record this meta-data;
- An ontology connecting qualification frameworks, diploma supplements, ECTS modules, systems for accreditation and open learning accreditation systems, and
- A technological roadmap, which would allow fully-open credentials.

The specific activities undertaken to achieve these results included:

1. The identification of technologies used for recognising and verifying open credentials
2. Identification of meta-data standards used for recognising and verifying open credentials
3. Proposition of an appropriate meta-data standard for the learning passport
4. Proposition of an ontology for recognition of open learning
5. Creation of a technological roadmap for implementation of such a proposal

A standard format for describing open education in terms of ECTS

There is no European approach to recognising, transferring or scaling open education modules. EU recognition instruments such as the European Credit Transfer and Accumulation System (ECTS), the Diploma Supplement and the European Qualifications Framework (EQF) support the award of qualifications in the areas of formal learning. They are supported by recognition procedures for non-formal and informal learning. The recognition and transfer of individual credits through ECTS was created for an era of physical mobility, and is optimised accordingly. While these tools can be used to support open education and virtual mobility, a number of caveats exist to their use. Little guidance exists on how to document open education experiences for the purposes of credit transfer.

¹ <https://oepass.eu/outputs/learningpassport/>

EU standards for qualifications	
European Qualifications Framework: gives an indication as to the level of various qualifications	not for non-formal education or open learning / micro-credentials
European Diploma Supplement: provides a standardised template to give additional information about a degree	only for degrees
European Credit Transfer System: allows for individual learning units to be described in terms of knowledge, skills, responsibility and autonomy	only for Higher Education
European Skill, Competences, Qualifications and Occupations database: provides a multi-lingual standard terminology	not used by the tools above

Table 2: EU Standards for Qualifications.

Procedures for recognition of prior learning or of non-formal/informal learning do not scale to the massive numbers of students enrolling in open education programmes such as Massive Open Online Courses (MOOCs). Many open educational providers are creating parallel systems of credentials - leading to a situation where millions of students per year are enrolling in open courses offered by universities, which do not necessarily award valid or recognised forms of credit. OEPass intends to address these issues by creating a *standard format* for describing open education and virtual mobility experiences in terms of ECTS which:

- addresses common criticisms, especially a lack of trust, of open education, in particular with respect to student assessment and identity,
- is scalable to hundreds or thousands of students through automatic issuing and verification of certificates,
- can capture a wide range of non-formal and formal open education experiences.

We aim to identify a meta-data standard (or recognition framework) for documenting micro-credentials in terms of ECTS using existing recognition tools. Just like the ECTS standard has made physical student mobility in Europe so much easier, a harmonised European approach to recognizing and transferring open education credentials will enable virtual student mobility, empowering students to adapt their learning portfolio to changing labour market demands and new technological trends. The World Economic Forum cites an estimate by Scott McLeod and Karl Fisch postulating that “65% of children entering primary school today will ultimately end up working in completely new job types that don’t yet exist” (World Economic Forum, 2016, p. 3). Their multi-source learning and skills/competence acquisition could greatly benefit from widely approved open standards applied to credential recognition.

We envisage students becoming digital pioneers and entrepreneurs of their studies as they work on challenging projects and seek out learning resources online or from other specialist sources. We envisage higher education institutions adapting their curriculums and accompanying their students on their open learning journey.

Report Structure

This report outlines what will be required to roll out a system of digital credentials in the European higher education area. It is structured as follows:

Chapters 2 and 3 reflect on the feasibility of technical solutions for the challenges of recognition of open learning. It gives an overview of the solution that the OEPass consortium eventually selected for recommendation, which is currently being developed as a proof-of-concept. The chapter has a focus on technical details as well. The OEPass project is coordinating work on the metadata standard in collaboration with another EU-funded project, MicroHE (Support Future Learning Excellence through Micro-Credentialing in Higher Education, <https://micro-credentials.eu/>). Within the scope of the two projects collectively, we will develop and test a working model. The aim is not to have a perfect operational solution by the end of both projects, but to showcase how a digital credentialing solution (possibly based on verified transactions on Blockchain) could look like in the future and to highlight the strengths and discover the potential pitfalls of such a system. This model implementation can serve as an opportunity for learning and can later be used as a reference for further discussions and developments.

Because stakeholder adoption of such a system for digital credentials depends not purely on technical factors, this report also briefly looks at enabling factors and the procedures and governance models that participating partners in such a system have to agree on.

Chapters 4 until 7 explore the different standards and guidelines for the recognition of open credentials.

Chapter 8 discusses the procedures and governance models that participating partners in such a system have to agree on.

Chapter 9 provides questions and answers on the use of Blockchain technology for digital credentialing.

The appendix in chapter 10 provides background information on potential stakeholders for consultation and on ESCO and the EQF, which are at the heart of the proposed meta-data standard.

2 Identification of technologies used for recognising and verifying open credentials

This chapter describes a variety of technologies which are currently used to credentialise open learning, and which are often mentioned as the future of digital learning.

2.1 Paper Certificates

Most records are still issued on paper or other physical formats, although digitisation efforts by governments and industries are proceeding all over the world (Cheng et al., 2016). There is no ‘perfect format’ for certificates, with many countries using hybrid-certificates whereby paper certificates are backed up by digital databases.

However, the significant limitations of each system clearly show a need for a better, more robust certification technology.

2.1.1 Limitations of Paper Certificates

Paper certificates are still the most widely used, seen in many quarters as being the most secure form of certification, since they are:

- difficult to forge due to security features built into the certificates themselves;
- (usually) held directly by the recipient, who thus has full control over their certificate;
- relatively easy to store securely for prolonged periods of time, e.g. by keeping them in a safe;
- they can be presented by the recipient anywhere, to any person for any purpose.

Furthermore, having been the standard for hundreds of years, paper certificates are built into institutional, regulatory and legislative workflows for practically all use-cases of such certificates.

However, paper certificates also have significant disadvantages:

- While being hard to forge, no certificate is immune from the risk of forgery. Thus, the issuer is obliged to retain a central register of issued certificates that may be used to verify certificate authenticity;

- Certificate registries can be significant points of failure: if problems emerge within the registry, although the certificates may remain valid, the ability to verify them could be lost;
- Keeping such a register of claims, and answering queries as to the validity of certificates is a manual process, which requires a considerable amount of human resources and time;
- Security features in the physical certificate derive exclusively from the difficulty level and expertise required to create the document. The more secure the certificate, the more expensive it is to produce;
- There are no limitations on the ability of the issuer to fraudulently state the timestamp or other details of the certificate;
- Once issued, there is no way to revoke a certificate without having the owner relinquish control of it;
- If a third party needs to interact with the certificates, e.g. to verify claims made in CVs, they need to read and verify each certificate individually and manually, a significantly time-consuming process.

2.2 Digital Certificates

At high-level, digital certificates may take three forms, namely:

- Reproductions of paper certificates – these are usually scanned versions or photographs of paper certificates. For many low-security applications, these are considered to be equivalent to paper certificates. These are typically not considered ‘true’ digital certificates, and are not further discussed in this section;
- Unsigned digital certificates – these consist of digital documents such as a PDF or a Word Document. These documents are extremely easy to edit, forge and reproduce at scale – as such their use is not recommended for any trust-based applications;
- Digitally-signed digital certificates – which are both computer-readable and tamper-proof. The security of the certificate derives from the security of cryptographic protocols, which ensure that the certificate is cheaper to produce than its paper equivalent but extremely expensive to reproduce by anyone except the issuer.

Digital certificates hold many advantages over paper certificates in that they require less time and far fewer resources to issue, maintain and use, since:

- the veracity of certificates can be checked against the registry automatically, without human intervention;
- where a third party needs to use the certificates, these can be automatically collated, verified and even summarised if they are issued in a standardised format;
- digital certificates can be revoked by the issuer;
- they can be multilingual;
- certain types of issuer-fraud, such as changing the timestamp or changing the certificate serial, can be made impossible depending on the design of the system.

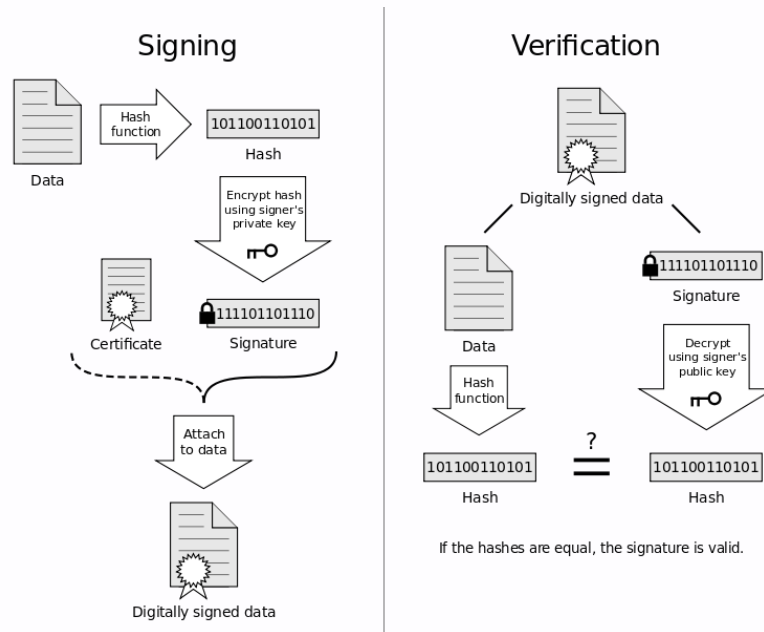


Figure 2: A digital signature is a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

Disadvantages associated with digital certificates could be that:

- without the use of digital signatures (i.e. a digital code – generated and authenticated by public key encryption – which is attached to an electronically transmitted document to verify its contents and the sender's identity), they can be easy to forge;
- where digital signatures are used, these require the involvement of third-party certificate providers to guarantee the integrity of the transaction – these third parties have significant control over every aspect of the certification and verification process, which, theoretically, can be abused;
- there is no universally used open standard for digital signatures, leading to certificates that can only be verified within the context of specific software ecosystems;
- just like paper certificates, electronic records can also be destroyed – keeping them safe requires sophisticated, multi-tier backup systems which are prone to failure;
- should the registry fail, the certificates themselves become worthless since unlike paper certificates, they hold no intrinsic value without the registry;
- registries of digital certificates are prone to large-scale data-leaks.

2.2.1 Open Badges as Digital Certificates

An open badge is a special digital certificate comprised of a digital image and some metadata. The data can be baked into the badge, meaning that it is embedded into the image file. The individuals and organizations who issue badges create the badge metadata - which is de-

signed to support verification of badges, so that an earner's badges can be checked for authenticity. The Open Badges Developers Guide² provides a set of technical resources to guide through the processes of creating, issuing and displaying Open Badges.

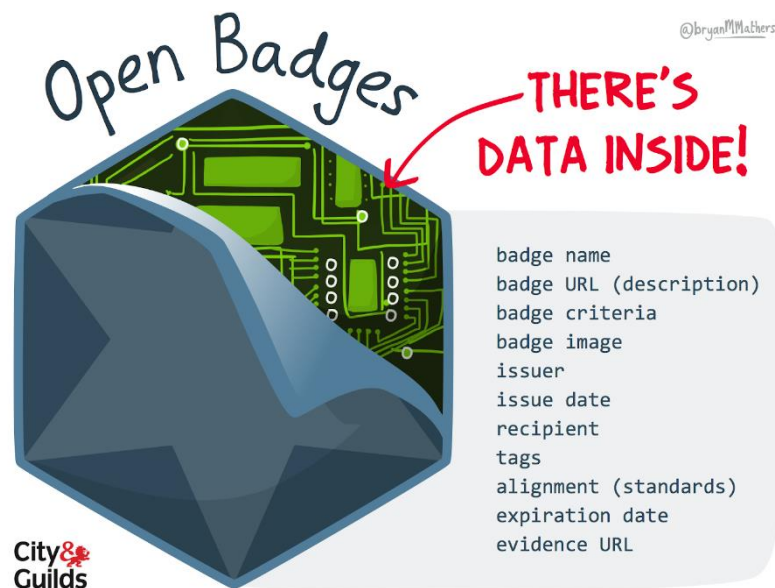


Figure 3: The Open Badge anatomy by Bryan Mathers, City and Guilds³: The badge metadata includes information about the learning content, earner and issuer.

The Open Badge Standard⁴ was originally developed by the Mozilla Foundation with funding from the MacArthur Foundation. Although the standard officially transitioned to the IMS Global Learning Consortium in January 2017, the so-called Mozilla Backpack, a decentralised badge aggregator/repository site⁵ where earners can collect and store their badges, is still operational. There are many similar aggregators of open badges in the world like the Open Badge Factory⁶, Credly⁷ and others.

The Open Badge Standard is under constant development, in October 2018, the latest version is 2.0⁸. Some consequential updates to this structure are coming with the next version of the Specification, particularly enabling embedding of complete BadgeClass and Issuer Profile documents into an Assertion (and into baked badges). See current issues in progress for details on Github⁹.

The OBI (Open Badge Infrastructure) is a set of software tools and specifications to support people and organizations who want to adopt badging. The OBI is the core underlying technical scaffolding for the badge ecosystem.

² <https://openbadges.org/developers/>

³ <http://huxleypiguk.blogspot.com/2016/06/digital-me-and-city-and-guilds.html>

⁴ https://en.wikipedia.org/wiki/Mozilla_Open_Badges

⁵ <https://backpack.openbadges.org/>

⁶ <https://openbadgefactory.com/>

⁷ <https://credly.com/>

⁸ <https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/index.html>

⁹ <https://github.com/IMSGlobal/openbadges-specification/issues?q=is%3Aopen+is%3Aissue+milestone%3A%222.0+Prototypes%22>

The OBI supports a multitude of issuers, including education and training providers, who confer badges into the ecosystem, as well as many displayers and earners using badges to share their competencies and achievements. Anyone can earn badges across many issuers, collect them in one place tied to their identity, and then share them with various websites and audiences (including career sites, social networks or personal portfolios).

The OBI aims to support badge issuing, collection and display. This involves:

- allowing earners to tie badges to their identity and carry their badges with them wherever they go;
- displaying badges to parties the earner cares about (e.g. employers, college admin, peers);
- allowing earners to manage collections of badges and control visibility of those collections;
- all of this is supported within a framework that is **open and decentralised** to facilitate badging across sites and sources.

Thus, advantages include that:

- badges are easy to collect and display;
- granularity of open badges offers a way to acknowledge smaller achievements;
- empowering for students in the sense that it acknowledges an achievement;
- a combination of badges may help students to self-direct their efforts in the right direction;
- they can be shared easily;
- they capture the learning which might otherwise never be recognised (Devedzic and Jovanovic, 2015).

While open badges have several advantages, including the potentials listed above, they also have limitations. As open badges can be awarded to acknowledge any achievement, including any level of learning of any type (from formal to informal), the quality is determined by the developer. Therefore, when it comes to assessing achievement in learning, the developer has to make sure to assess learner performance properly.

Typical criticism on open badges¹⁰ include:

- The long history of physical badges in military and quasi-military settings might encourage similar hierarchical relationships when employed online.
- Badges are a type of extrinsic motivator that could compete with an individual's intrinsic motivation for accomplishment and mastery.
- Validity: whether they can be viewed as “trusted credentials”. In particular: it is difficult to evaluate the real value of a badge;
- Badges are hard to exchange across different institutions, highlighting the problem of commonality;
- It only provides a vague evaluation for the skill, highly subjective in nature and can be interpreted in different ways.

¹⁰ https://en.wikipedia.org/wiki/Digital_badge#Criticism

- Carpet badging: the fear that too many badges will undermine their value.

Critically, badges are still not successful and acceptable as an educational currency.

2.2.2 Micro-Credentials

The world of work increasingly demands a quick response from the education system to provide people with the desired qualifications. In response, MOOCs have tried to make their content as digestible and flexible as possible. Degrees are broken into modules; modules into courses; courses into short segments. The MOOCs test for optimal length to ensure people complete the course; six minutes is thought to be the sweet spot for online video and four weeks the ideal course duration.

Universities are responding to this trend by becoming more modular, too. EdX has a micro-master in supply-chain management that can either be taken on its own or count towards a full masters at MIT. Coursera now offers everything from full degrees to single courses – with content often offered for free and learners only having to pay for assessment and accreditation at the end of the course if they want an official and validated credential.

However, while traditionally students could depend on recognition of widely understood signals of experience and expertise such as university degrees, the same cannot be said for micro-credentials like the creatures of MOOCs such as ‘nanodegrees’ and ‘specialisations’. The private sector is proposing various solutions to recognise learning in smaller segments, from the aforementioned nanodegrees, to centralised skill-banks verified by standardised testing to online systems of recommendation similar to those to peer-reviewed literature (The Economist, 2017).

2.2.3 Digital Credentials

In the context of education and training, a credential is a certificate issued by a responsible institution that attests and verifies that a person has achieved specific learning outcomes and acquired specific skills and competences. The learning experience can involve online- or face-to-face-learning, or both. Credentials can be paper-based or digital, and they can be degrees, certificates, badges, diplomas, licenses, and industry certifications, among others (Connecting Credentials [Lumina Foundation], 2016; SUNY, 2018).

The switch from paper-based to digital credentials offers advantages to learners and employees, to educational institutions and to potential employers. A system of universally recognized and stackable micro-credentials for smaller units of learning below degree level (both online and offline) enhances student mobility and employability and enables truly flexible learning paths. It has the potential to take life-long learning to a new level. The following list is an adapted and expanded form of the list found in (Riksen & Kerver, 2016), which was published under the Creative Commons Attribution licence 3.0 Netherlands.

The advantages of digital credentials and the Learning Passport for **learners** are:

- all credentials are conveniently stored online in one place,
- the credentials are securely stored for a long time,
- the learner “owns” his or her credentials,

- the credential incorporates the verification of the identity of both earner and issuer,
- the credential is verifiable,
- there is a permanent link to the credential and the supporting evidence, even after the program or course has been completed, changed or discontinued,
- the credentials may contain links to evidence of tasks performed or of assessment results,
- a digital credential can document achievements from formal education, non-formal learning, lifelong learning, apprenticeships and short programs,
- even small or diverse bits of learning may get visible and documented (and possibly credited),
- the credential's content (meta-data) is searchable,
- a credential may be linked to an online identity,
- digital credentials can be made available to employers and HEIs when applying for work or for a study programme, in full or selectively,
- possibility to create multiple flexible collections of credentials to (a) communicate distinct sets of skills and competences and/or to (b) identify skill/knowledge gaps when pursuing degrees or specific employment,
- potential to utilise the digital certification ecosystem to present existing evidence of prior learning to earn corresponding credential,
- increased possibilities for physical and virtual student mobility.

The advantages for **educational institutions** are:

- option to access additional information about the credential and the acquired knowledge, skills and competences,
- easier admission processes,
- easier recognition processes,
- consistent recognition decisions due to transparent documentation,
- potential to consult data on skill/knowledge/competence demand by labour market,
- the credential's content (meta-data) is searchable,
- version control: time-stamped history of module descriptions and their evolution over time,
- quick issuing of credentials (once the protocol is in place and administrators are trained),
- inexpensive issuing of credentials,
- quick and inexpensive replacement of lost credential,
- safe and secure credentials that are harder to temper with than traditional credentials,
- option to withdraw credentials in case of errors or misuse,
- option to track how and to which extent the digital credentials are being consulted,
- most of the data is already available in the IT system,
- can be linked to the IT system and to administrative processes,
- standardized data format,
- verified transactions via Blockchain are a logical next step,
- enables unbundling of credentials (e.g., for modules instead of degrees),
- enables stackability,

- new forms of study and new business models are possible,
- new potential students or customer groups can be reached.

The advantages for **employers** are:

- simple and quick verification of digital credentials,
- link to evidences of tasks performed and/or the results of assessments,
- potential to consult data on HE skill/knowledge/competence supply and trends,
- option to access additional information about the credential and the acquired knowledge, skills and competences,
- encourages lifelong learning,
- opportunity to document in-service/continuing professional development training in compatible credential format,
- transparent solution,
- the credential's content (meta-data) is searchable.

(Sources: (Riksen & Kerver, 2016), own research).

2.3 Unbundling

Unbundling means that products and services that were being offered or sold together are now being offered in parts. In Higher Education, all modules of a study programme leading to a degree were traditionally organized and offered by the same institution. Upon successful completion, that institution awarded the degree.

Open learning recognition could potentially lead to unbundling in higher education. As an example of how higher education institutions can embrace the trend towards unbundling in higher education, consider the “curiosity-driven education” approach of the Code University in Berlin, Germany. Students work on challenging projects, seek out learning resources online, define the competencies and skills that they will acquire in the project through a learning agreement with their professors, and are accompanied by university lecturers in their personal development and learning processes. They are being empowered to become digital pioneers and entrepreneurs of their studies. They develop the self-confidence to accept unknown challenges and new solutions (Code University of Applied Sciences, 2018).

3 Technology in OEPass

This chapter discusses the requirements of an ideal system of recognition and verification of credentials in open education at national or European levels in terms of technologies. The basis of our approach is visualized by (Grech & Camilleri, 2017).

Figure 4 outlines how the approach of OEPass fits into the existing higher education landscape. The two components in the right column, “Ledger” and “Learning Passport”, are new. The key focus of OEPass is on the Learning Passport. For this reason, the ledger is also of relevance.

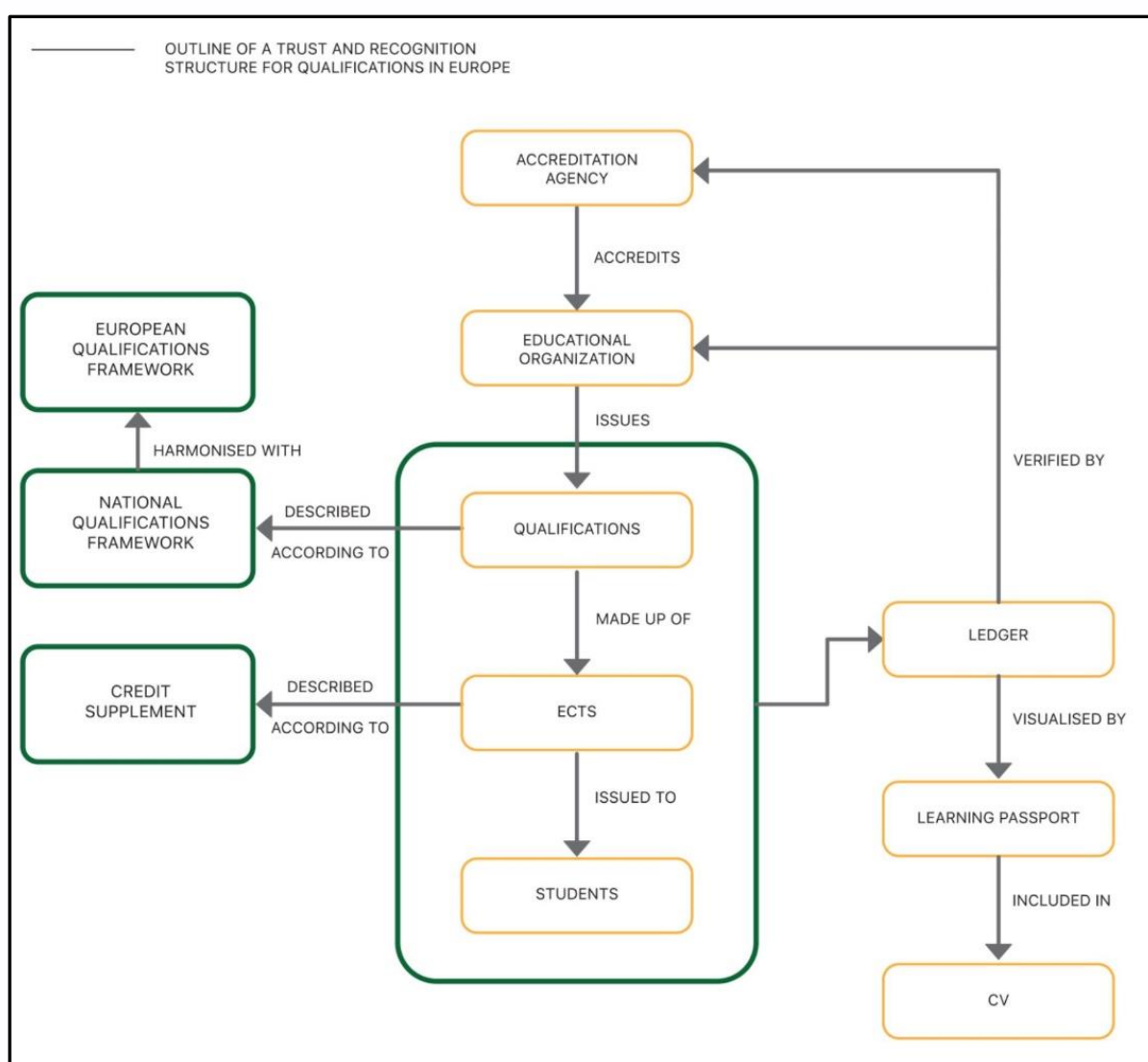


Figure 4: Trust and Recognition Structure for Qualifications (Grech & Camilleri, 2017).

The Learning Passport is envisioned to be an official document that contains the description of all the learning a person has done. The student will have a lifelong Learning Passport to store and display digital credentials in terms of ECTS or ECVET from various educational providers, just like Backpack does for the Mozilla Open Badges. We aim to create an open system

for issuing, verifying and sharing micro-credentials. Digital credentials in the Learning Passport can be notarized and verified on a Blockchain and be shared in external credential wallets or other e-portfolios.

The Learning Passport is a proposal that will provide all necessary information for transferability and recognition of credits utilizing the established higher education structures such as ECTS and EQF. This has an IT component (the meta-data standard) and a qualitative component (procedures and requirements for recognition).

In order to align the Learning Passport with existing trust and recognition systems in Europe, a standardized way is required to store individuals' learning experiences. OEPass addresses this with a meta-data standard (Section 3.1). In OEPass, the ledger refers to a Blockchain solution, which enables the use of the Learning Passport and related metadata in existing systems. Although such a solution is not in the core focus of the project, the technology and existing solutions are discussed in the following chapters. Further, we will discuss additional needs for integrating the Learning Passport and ledger with institutional and administrative (even governmental) systems.

3. 1 Meta-Data Standard

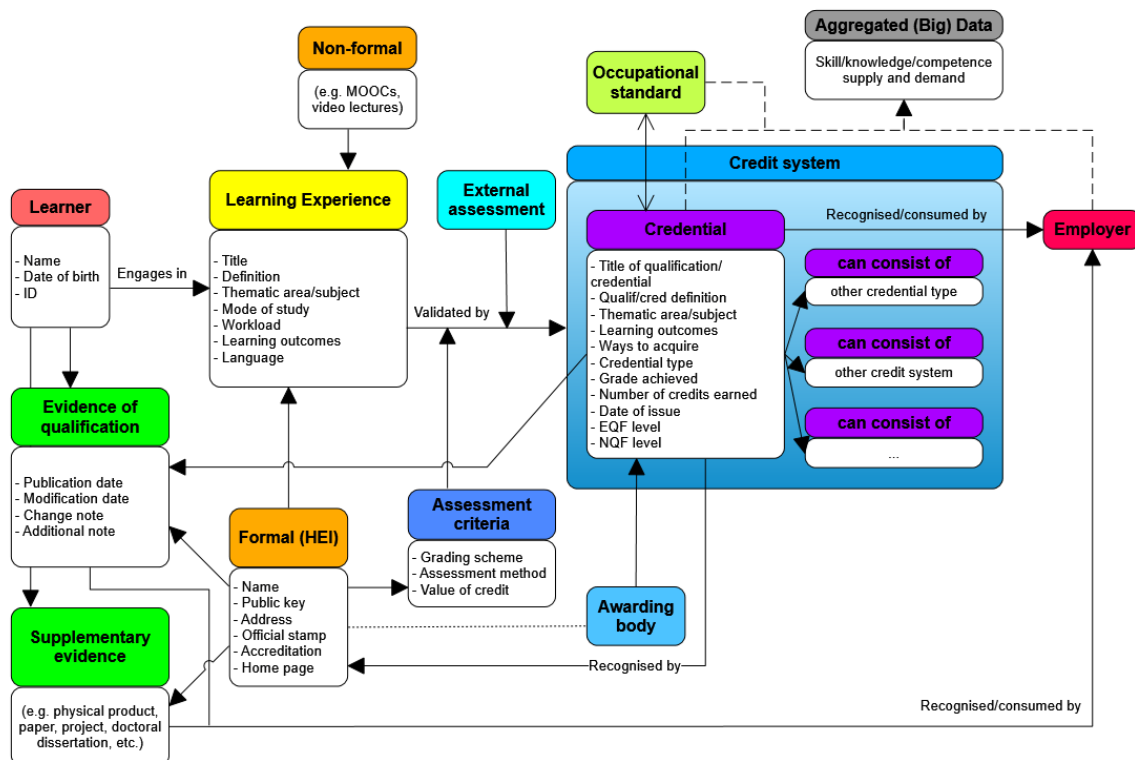


Figure 5: MicroHE Meta-Data Standard (Illustration by Ildiko Mazar).

The OEPass project is developing the meta-data standard jointly with the MicroHE project.

The meta-data standard¹¹ extends the existing ESCO data standard so that it cannot only be used for entire qualifications, but also for short learning programs and the micro-credentials they award. The proposed meta-data standard is independent of the underlying technology. However, OEPass considers a Blockchain solution to enable its use in existing trust and recognition systems in Europe.

The European Commission is developing and rolling out a “European Digital Credentials Infrastructure” as part of the New Europass, see <https://ec.europa.eu/futurium/en/europass/europass-digital-credentials-infrastructure>.

3.2 Blockchain

“Ledgers are tools by which one can determine the owner of an asset at any point in time. They perform this function by serving as a central authoritative list of transfers of the asset in question.

In a system or society that has agreed to use a ledger to determine ownership of a particular asset, all that is required to transfer ownership between two parties, is to make an entry in the ledger indicating that this has happened.” (Grech & Camilleri, 2017, p. 16).

“Simply put, a Blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community” (Grech & Camilleri, 2017, p. 16). Blockchain is a technology that enables time-stamped verification of a transaction without the need of a central authority. This makes it ideal for issuing verifiable digital credentials.

For the purposes of accountability and verification, higher education institutions are by law required to keep records of the credentials they issue. Traditionally, this has been done both in paper and electronically through a database maintained by (and at) the issuing institution.

¹¹ For details on the MicroHE meta-data standard, please visit the websites <https://microcredentials.eu/consultation/> <https://github.com/MicroCredentials/MicroHE>

3.2.1 Digital Certificates using Blockchain technology

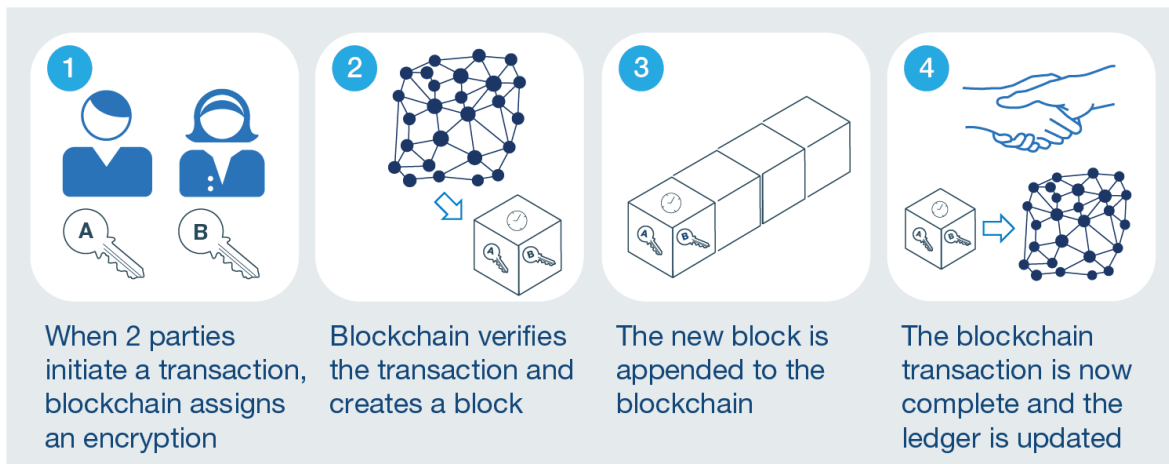


Figure 6: How to create a blockchain transaction (by McKinsey&Company).

Blockchain technology is ideal as a new infrastructure to secure, share, and verify learning achievements (Smolenski, 2016). In the case of certifications, a Blockchain can keep a list of issuer and receiver of each certificate, together with the document signature (hash) in a public database (the Blockchain) which is identically stored on thousands of computers around the world.

Despite the above listed disadvantages and challenges, digital certificates that are secured on a Blockchain could still hold significant advantages over 'regular' digital certificates, in that:

- they cannot be forged – it is possible to verify with certainty that the certificate was originally issued and received by the same persons indicated in the certificate;
- verification of the certificate can be performed by anyone who has access to the Blockchain, with easily available open source software – there is no need for any intermediary parties;
- because no intermediary parties are required to validate the certificate, the certificate can still be validated even if the organisation that issued it no longer exists or no longer has access to the issued record;
- the record of issued and received certificates on a Blockchain can only be destroyed if every copy on every computer in the world hosting the software is destroyed;
- the hash is merely a way of creating a 'link' to the original document, which is held by the user. This means that the above mechanism allows for the signature of a document to be published, without needing to publish the document itself, thus preserving the privacy of the documents.

3.2.1.1 Ideal Characteristics for Recipient

Blockchains address the following ideal requirements for a certificate from a recipient's perspective:

- **independence:** the recipient owns the credential, and does not require the issuer or verifying third party to be involved after receiving the credential;
- **ownership:** the recipient may prove ownership of the credential;
- **control:** the recipient has control over how they curate credentials they own. They may choose to associate credentials with an established profile they own, or not;
- **verifiability:** the credential is verifiable by third parties, like employers, admissions committees, and verification organisations;
- **permanence:** the credential is a permanent record.

3.2.1.2 Ideal Characteristics for Issuer

Blockchains address the following ideal requirements for a certificate from an issuer's perspective:

- the issuer may prove they issued the credential;
- the issuer may set an expiration time on the credential;
- the issuer may revoke the credential;
- the credentialing system is secure and imposes minimal ongoing burden to remain so.

3.2.1.3 Other Characteristics

For the actual credential to have meaning and utility, a third-party verifier, such as an institution receiving the credential as part of an application must be convinced of a certificate's veracity. The following are standard requirements:

- **integrity:** the content hasn't been tampered with; that is, it matches what the issuer originally intended.
- **authenticity:** confidence that the issuer is who the certificate claims, and has not been forged.

3.2.1.4 Challenges to Blockchain Use

Blockchain is not in itself a panacea to all potential disadvantages of credential systems. In particular, the design of a system would need to take into account:

- How to create a balance between full user control and ownership over data, and protecting the user from mistakes such as password loss.
- How to manage permissions for a ledger – who should have access to do what under what conditions?
- What kind of blockchain to use to reach a balance between security and efficiency (in particular as regards energy and storage costs)?
- Interoperability between systems – no global standard currently exists for educational certificates, let alone blockchain certificates.
- How to reconcile the immutability requirement of blockchains with the requirements for the GDPR.

integrity, hashes of each block on these consortium chains are in turn stored on a public blockchain involving proof-of-work. Credentials will be stored on the consortium blockchain in anonymous form using a Universal Unique Identifier.

Qualification data (like for example versioned and time-stamped module descriptions) are stored off-chain in a qualification database. Evidence linked to a credential is stored off-chain in an evidence database. This could be a project work a student has created as part of an assessment in open learning, like a video, a website or a computer program. To prevent tampering and falsification, hashes of the off-chain data are stored on the consortium blockchain. The Learning Passport can be interpreted as the view of an individual on all the qualifications and credentials associated with that specific person, i.e., the individual's wallet. Likewise, the database that an institution maintains about all the credentials it has issued is that institution's wallet.

In this Learning Passport community, each educational institution who is a consortium member "maintains his or her own copy of the information and all members must validate any updates collectively. The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form. Entries are permanent, transparent, and searchable, which makes it possible for community members to view transaction histories in their entirety. Each update is a new "block" added to the end of a "chain." A protocol manages how new edits or entries are initiated, validated, recorded, and distributed. With blockchain, cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole." (Grech & Camilleri, 2017, p. 16).

Issuing Credentials

Education providers will issue digital credentials using their institutional wallet, as described in the previous section. There will also be a paper representation of the digital credential containing a link to the digital form.

Verifying Credentials

Verifying credentials should be possible through verification services via web interface or app. As the user interface of Learning Machine (<https://www.learningmachine.com/>) illustrates for the digital credentialing solution Blockcerts, such a verification can be made both user-friendly and secure through open source code and open standards.

Evolution of Standards and Technologies

We envisage that a consortium of education institutions will operate the Learning Passport and the underlying infrastructure. Institutions wishing to issue credentials to the Learning Passport will have to become members of the consortium. To join, they will have to prove that they pass certain quality standards (which have yet to be defined).

The consortium will take responsibility for discussing, developing, approving and implementing new standards and technologies.

Data Protection

Data protection issues are of great concern in the digital era. Information on the blockchain is publicly searchable and cannot be deleted, so it is important that any personal information be stored in anonymised form using a separate Universal Unique Identifier for each credential.

3.4 Integration and APIs

OEPass foresees the need for many technological developments in the near future for enabling a successful adoption of the Learning Passport. This requires both development of new applications on top of the Learning Passport as well as integration to existing systems deployed at universities. Although such solutions are not the focus of OEPass, the potentials relating to them will be discussed next.

3.4.1 Front End Integration: Applications

Developing and maintaining applications is not within the scope of the OEPass project. Therefore, the OEPass project welcomes outside collaboration. To provide front-end and back-end integration and applications, the OEPass project collaborates with the Blockchain start-up company 0xcert (<https://0xcert.org/>) that is using non-fungible tokens on the Ethereum blockchain according to the ERC721 standard. This will be sufficient to demonstrate the functioning of the Learning Passport and of the meta-data standard.

For a start, we envisage the following applications and functionalities:

- Learning passport as a web service and as an application
- Social Media and Career Network integration
- Europass integration
- Verification services

3.4.2 Back End Integration: Campus IT Systems

HEIs and other education providers wishing to make their credentials digitally available via the Learning Passport will have to update their IT systems to provide sufficient information via the meta-data standard so that other institutions can make an informed decision about recognising the credential towards their degrees.

Education providers from outside the higher education world will most likely also have to review their procedures and standards regarding teaching and learning, quality management, ID verification, assessments and fraud prevention. They will have to provide compatibility to the higher education system through a “credit supplement” that describes the workload, the learning outcomes, the level of learning, the issuer, the assessment and the grading scale.

4 Recognition

4.1 Standards and Guidelines for Recognition

The OEPass project envisages automated systems of credential recognition as a long-term goal strengthened through the project and its counterpart MicroHE. In order to ensure such recognition, it is not only necessary to provide suitable (innovative) technology (see previous sections) but also to fulfil the standards that are required for formal recognition by the relevant authorities, mainly HEIs. The Learning Passport will thus be designed in alignment with the standards and guidelines of the European Higher Education Area. The major reference for the project thus are the European Standards and Guidelines (ESG, 2015), the European Area of Recognition Manual (Nuffic, 2012; The EAR HEI and STREAM projects, 2016) and the ECTS Users' Guide of the European Commission (European Union, 2015). Additionally, the national and European qualification frameworks (NQF and EQF) play a major role for the taxonomies behind the credential, linked to other initiatives such as ESCO. The most relevant stakeholders to be included in the further development and evaluation of standards and guidelines for (open) micro learning are thus the European Commission as well as the members of the ENIC-NARIC networks, which are national authorities responsible for recognition of qualifications, who increasingly also work on applying their standards to the field of open and flexible education. From project partner countries, this would be, for example, the *Central Office for Foreign Education in the Secretariat of the Standing Conference of the Ministers of Education and Cultural Affairs in the Federal Republic of Germany* as the German ENIC-NARIC Centre (<https://www.kmk.org/zab/zentralstelle-fuer-auslaendisches-bildungswesen.html>).

Several authorities on national and European level as well as independent initiatives have already worked on the incremental development of standards for the recognition of open learning, with a focus on applying the European Standards and Guidelines. As part of the PARADIGMS project the Dutch NARIC Nuffic recently published a policy paper focussing on the evaluation of MOOCs that suggests several criteria for the assessment of a MOOC certificate which could be applied to the context of micro-credentials in general (PARADIGMS, 2018). The OEPass consortium is going to publish a concept paper outlining the potential criteria for micro-credentials based on the Nuffic recommendations.

4.2 Automated Credential Recognition

There are several possible use cases for credential recognition, among them:

- Learning agreement
- Stackability
- Curriculums that integrate prior or open learning
- Recognition of prior learning

Learning agreement

Ideally, the decision about recognizing an open learning credential will be made before the student takes that course, and the student and the institution sign a corresponding learning agreement.

Stackability

Institutions may choose to define learning pathways (or curriculums) through which they define beforehand that some specific courses combined will be awarded with a summative credential or degree.

Curricula that integrate prior or open learning

Higher education institutions might also decide to accept certain pre-qualifications as equivalent to some (usually entry-level) modules of their curriculum. Examples include:

MIT has signed agreements with (currently) 14 universities from around the world. They recognize MIT's edX online credential "MicroMasters in Supply Chain Management" as equivalent to between 20 and 42 ECTS credits of their own curriculum.

Some Bachelor's curricula in midwifery or physiotherapy in Germany recognize a vocational education in that field as equivalent to the first two or three semesters of the curriculum.

Recognizing Credentials from the Learning Passport towards an HE degree

For a higher education institution to recognize open learning credentials as credit towards an HE degree, a responsible person has to make an informed decision by evaluating the information and evidence about the learning that the credential attests and comparing it to the learning outcomes of the module that it will be credited to (graded or non-graded). The initial decision about recognizing a certain credential as ECTS credit towards a specific module must always be done by a responsible person or committee. It cannot be automated.

Automation can only kick in for all subsequent recognition requests about that course, i.e., to ensure consistency once a recognition decision has been taken about a specific credential.

Recent studies have tried to provide guidance on the recognition of online learning (Kiron Open Higher Education, 2017; Rampelt, Niedermeier, R wert, Wallor, & Berthold, 2018; Witthaus et al., 2016) and of foreign degrees (The EAR HEI and STREAM projects, 2016).



Quality Criteria of Credentials	OpenCred	Oops a MOOC	EAR Manual	
The credential should provide information on...				
C1 Identification of Credential & Institution	Informative certificates / badges acknowledging learning	2. Verification of the certificate [Authenticity]		Transparency
C2 Identification of the Learner	Identity Verification of the Learner	7. Identification of the participant [Identification]		
C3 Learning Outcomes		4. Learning outcomes	5. Learning Outcomes	
C4 Workload of Learning		5. Workload (volume)	2. Workload	
C5 Level of Learning		3. Level of the study programme [Level]	1. Level of a Qualification	
C6 Quality of Learning	Quality Assurance	1. Quality of the study programme [Quality]	3. Quality	
C7 Assessment of LOs / Rules to earn	Supervised assessment Award of Credits	6. The way study results are tested [Testing]		
	Partnership & Collaboration		4. Profile	
The medium should be ...				
M1 Distinct			(Substantial and non-substantial differences)	Trust
M2 Authentic	(Informative certificates /badges acknowledging learning)	(2. Verification of the certificate [Authenticity])	(Authenticity)	
M3 Accessible				
M4 Exchangeable			(Credits, grades, credit accumulation and credit transfer)	
M5 Portable			(Purpose of Recognition)	

Table 3: Quality Criteria of Credentials. (Kiron Open Higher Education, 2017; Rampelt, Niedermeier, Röwert, Wallor, & Berthold, 2018; Witthaus et al., 2016) and of foreign degrees (The EAR HEI and STREAM projects, 2016).

5 Identification of meta-data standards used for recognising and verifying open credentials

This section contains a review of existing standards, which are used to describe open learning opportunities and/or credentials. Only standards, which have a significant usage basis within Europe have been considered for inclusion within the section.

5.1 EUROLMAI & CWA 16133: Guidelines on a European Learner Mobility model

Maintained by:	European Committee for Standardization (CEN)
Used for:	Exchange of learning mobility information
URL:	https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PRO-JECT:31329&cs=16608C34D25336BA4D2F76D2AC9B38753

EuroLMAI defines a model for the recording and exchange of learner achievement information among student management information systems, as well as the aggregation of information by third party suppliers. The data model describes assessments, primarily Diplomas, Diploma Supplements and Transcripts of Records for higher educations.

The model proposed within this CEN Workshop Agreement (CWA) is not intended to define the representation of the entire spectrum of Learner Mobility information. The scope of the standard is restricted to the definition of the electronic representation of official, institutionally attested achievement information for learners engaged in formal learning processes, in order to facilitate its recording and subsequent exchange within the European Education Area. Achievement Information structured and presented in compliance with this standard may of course be used for other purposes – for instance, providing descriptions of achievement to enrich a learner-owned report, in terms of an e-portfolio. However, guidance on the specification and organisation of information for purposes other than the representation of formal achievement reports is outside the scope of this standard. The EuroLMAI model has been developed as:

- a lightweight standard taking into consideration existing and emerging educational practice processes and the relevant European policies;

- an easy-to-implement standard in order to ensure a rapid uptake by stakeholders of learning, education and training throughout Europe (Higher Education Institutions, learners, employers, service providers, etc.).

5.2 ELMO

Maintained by:	EMREX Network
Used for:	Exchange of student data, including credentials between Higher Education Institutions
URL:	https://github.com/emrex-eu/elmo-schemas

The ELMO XML format is a basis for the exchange of result information between Higher Education Institutions who are included within the EMREX network. ELMO is based on the CEN [5] standard EN 15981-2011 EuroLMAI. The ELMO format is also being used as the format for the European Commission's Erasmus without Paper Initiative.

5.3 Learning Object Metadata

Maintained by:	IEEE/IMS
Used for:	Describing learning objects at any granularity level
URL:	https://standards.ieee.org/project/1484_12_1.html

The IEEE LOM standard defines a set of meta-data elements that can be used to describe learning resources. This includes the element names, definitions, datatypes, and field lengths. The standard is known as a multi-part standard and defines both a conceptual model for the meta-data and an XML binding. The standard includes conformance statements for how meta-data documents must be organised and how applications must behave in order to be considered IEEE-conformant.

5.4 Schema.org

Maintained by:	Schema.org community
Used for:	Course catalogues and learning opportunities
URL:	https://schema.org/Course

Schema.org is a collaborative, community activity with a mission to create, maintain, and promote schemas for structured data on the internet, on web pages, in email messages, and beyond.

Schema.org vocabulary can be used with many different encodings, including RDFa, Microdata and JSON-LD. These vocabularies cover entities, relationships between entities and actions, and can easily be extended through a well-documented extension model. Over 10 million sites use Schema.org to mark up their web pages and email messages. Many applications from Google, Microsoft, Pinterest, Yandex and others already use these vocabularies to power rich, extensible experiences.

Founded by Google, Microsoft, Yahoo and Yandex, Schema.org vocabularies are developed by an open community process, using the public-schemaorg@w3.org mailing list and through GitHub.

The schema.org 'course' standard provides for a description of an educational course, which may be offered as distinct instances at which take place at different times or take place at different locations, or be offered through different media or modes of study. An educational course is a sequence of one or more educational events and/or creative works, which aims to build knowledge, competence or ability of learners.

5.5 Open Badges

Maintained by:	IMS Global
Used for:	Issue of credentials, especially non-formal credentials
URL:	https://www.imsglobal.org/activity/digital-badges

Open Badges are information-rich visual records of verifiable achievements earned by recipients. The Open Badges standard describes a method for packaging information about accomplishments, embedding it into portable image files as digital badges, and establishing resources for its validation and verification. In other words, Open Badges contain detailed metadata about achievements such as who earned it, who issued it, the criteria required, and in many cases even the evidence and demonstrations of the relevant skills. The data is all inside!

Verifiable digital credentials such as Open Badges are an increasingly important means for educational institutions, employers, and other learning organizations to recognize a learner's skills, competencies, and achievements.

Designed based on learner-agency principles, Open Badges put learners in control of their credentials by enabling them to claim and display the badge on any platform. Open Badges are also portable rather than tied to one specific system (e.g., badging platform, learning management system, social media site). Open Badges contain rich metadata that provides information about the issuing organisation, the recipient, and evidence that substantiates the earning of the badge.

Optional extensions to the standard allow Open Badges to include detailed information about assessments and additional information about an issuer's accreditations relating to the credential. These elements help validate the rigor of the badge to audiences who review the credential, which may include fellow students, instructors, academic advisors, career center staff and others within the institution, as well as potential employers and peer networks. In these ways, badge owners can own, display, store, and share their Open Badges across an open digital credentialing ecosystem.

5.6 Qualifications Meta-data Schema (QMS)

Maintained by:	European Commission
Used for:	Exchange of qualification information
URL:	https://ec.europa.eu/esco/portal/escopedia/Qualifications_metadata_schema

To facilitate that all European Member States and other actors have a common view on the attributes that all qualifications share such as information about awarding bodies, EQF level, description of learning outcomes, etc., the European Commission developed a detailed 'metadata schema'. The schema is both human- and machine readable, the latter allowing IT

systems, search engines and web portals (such as the LOQ portal¹² or the ESCO Service Platform¹³) to access and interpret information on qualifications.

Member States and other stakeholders wishing to publish information on their qualifications in ESCO and the LOQ portals need to structure their data according to this meta-data schema.

5.7 MicroHE Meta-data Standard

Maintained by:	MicroHE consortium
Used for:	Exchange of information on qualifications and micro-credentials
URL:	https://github.com/MicroCredentials/MicroHE

The success of a growing number of HE unbundling initiatives suggests that in the long-term we may anticipate an increase in the quality and quantity of micro-credentials on offer within the European Higher Education Area (EHEA). In parallel with that trend, micro-credential recognition by different educational organisations and employers should also be expected to improve.

Since the EHEA is already coordinating and harmonising its Member States' and education providers' efforts in qualification documentation (see chapter 5.6 above), the MicroHE meta-data standard was naturally building on these existing foundations and was developed as an extension of the ESCO QMS. The MicroHE meta-data standard is therefore an attempt to create a new, or additional, European Qualifications Framework (EQF) schema within the EQF pillar in ESCO that proposes a set of standard meta-data for documenting micro-credentials, and specifically on how to record, store and transfer them via computer systems.

As the volume and stackability aspects of micro-credentials in HE were found to resemble the diversity and adaptability of non-formal learning experiences, the OEPass partnership selected the MicroHE meta-data schema to provide the basis of the OEPass ontology and Learning Passport development.

¹² <https://ec.europa.eu/ploteus/en>

¹³ <https://ec.europa.eu/esco/portal/document/en/7c597e8c-0825-4914-abcf-3c7a2f7d779c>

6 Proposition of an appropriate meta-data standard for the learning passport

6.1 Requirements for an Appropriate Standard

An appropriate metadata standard for promoting the recognition of open education should meet the following criteria:

- Addressing all levels of education: open education can take place at any level of education from primary to higher, including continuing education. Therefore, any recognition standard should also meet these aims.
- Aligned with European recognition instruments: within the context of processes such as the Bologna and Copenhagen processes, the Lisbon Recognition Convention and through the work of the European Commission's Education Council, the past two decades have seen a multitude of tools for recognition and portability emerge across Europe – any standard used must take full account.
- Captures Formal and Non-Formal Learning: the standard should be able to capture formal (accredited) learning as well as non-formal learning offered by other entities.
- Applicable to the Whole Course Lifecycle: it would be inconvenient for institutions to use different standards to describe the same information within different stages of the course lifecycle. Therefore, a standard that can be used at all stages from programme design through to award of credentials is preferred.
- Interoperable: the ideal standard should take account of other standards existing in the field and provide for easy mapping between them.
- Free & Open-Source: the standard should be fully available in its entirety.

6.2 Assessment of existing standards

To consider a meta-data standard for Open Recognition, we provide the following assessment of the standards identified against these criteria:

6.2.1 EUROLMAI & CWA 16133

On the plus side, these standards provide a framework for interoperability, which is strengthened by their publication by a standardization body, they are closely linked to European Recognition instruments, and they can be utilised at various phases of the course lifecycle.

However, both standards fail a number of the tests. In particular they are:

- Focused on tertiary education and specifically formal education,
- “closed” standards, requiring payment to access.

6.2.2 ELMO

By effectively providing an XML schema based on EUROLMA and CWA, ELMO shares all the advantages of the mentioned standards, and additionally, since it is fully open, mitigates the closed nature of those standards by providing a fully open access solution. ELMO's primary however is still focused on tertiary and formal education.

6.2.3 Learning Object Metadata

Learning Object Metadata is focused on describing learning objects, as such, providing support for the early stages of the course lifecycle, but not providing sufficient language or concepts, which are useful for credentialisation. LOM is extensible, but out of the box is also not linked with European Recognition instruments.

6.2.4 Schema.org

Similarly to LOM, schema.org supports the early stages of the course lifecycle by allowing description of courses, but does not provide sufficient language or concepts which are useful for credentialisation. Schema.org is also extensible, but out of the box is also not linked with European Recognition instruments.

Neither standard provides support for description of accreditation, but they are fully open access and invest significant resources in promoting interoperability.

6.2.5 Open Badges

Open Badges meets all the requirements in terms of open access, ability to apply to formal, non-formal, and applicability to the entire course lifecycle at all levels of education. While it is extensible, it does not provide support for accreditation concepts or for a link to European Recognition Instruments out of the box.

6.2.6 Qualifications Metadata Schema

Having been designed by the European Commission, the Qualifications Metadata Schema is designed specifically to express the concepts outlined in European Recognition instruments. It is applicable at all levels of education, and provides extensive support for accreditation concepts, but does not provide support for non-formal education or for the credentialisation stage of a course lifecycle.

The QMS is fully open and published as linked open data to enhance interoperability.

6.2.7 MicroHE Meta-data standard

The MicroHE Metadata standard was specifically designed to extend and enhance the QMS into new areas. As such, it extends the concepts in the QMS to the entire course lifecycle, allows for recording of non-formal education, and provides better support for recording micro-credentials.

Given this, the **MicroHE Standard** provides the best basis on which to build an ontology for recognition of open learning.

7 Proposition of an ontology for recognition of open learning

An open learning experience can come from either traditional formal education, e.g. higher education (HE), or non-formal sources, such as massive open online courses (MOOCs) or video lectures. A third party, for example a hiring employer or a university processing an admission application should be able to determine the value of learning outcomes irrespective of their source or formality of acquisition. In HE the course content, assessment and achievement administration is already well enough established (demonstrated by the success and widespread use of the Diploma Supplement¹⁴) to ease recognition processes. Non-formal learning providers should also be able to utilise vocabularies like qualification levels and ECTS and standards and classification like ISCED-F¹⁵ codes or ESCO skills and competences¹⁶ to describe their learning offerings to support informed decision making about learning outcomes.

¹⁴http://ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Communique_AppendixI_V_952782.pdf

¹⁵ https://ec.europa.eu/education/international-standard-classification-of-education-isced_en

¹⁶ <https://ec.europa.eu/esco/portal/skill>

Following the identification of the appropriate meta-data standard and an in-depth analysis of the Diploma Supplement, the OEPass partnership mapped the relationships between the main classes and properties and developed the Open Learning Passport¹⁷, a user-friendly, flexible online document describing a wide range of learning experiences. As non-formal learning has many shapes, forms and sizes, this ontology had to be transparent enough for issuers to know exactly what information and data may be expected by third parties to recognise the comprehensive value of the credential.

7.1 Learning Experience

Non-formal learning providers are encouraged to record the following information about their learning provision:

- Title of the learning experience (i.e. course or lecture)
- Short and abstract description of the experience
- Designation of the subject/thematic area (preferably from a controlled vocabulary, such as ISCED)
- Indication of mode of study (e.g. online, face-to-face, workplace, practice, etc.)
- Workload, i.e. the duration of the learning experience in hours, weeks or years – workloads should ideally be expressed in (or converted to) ECTS credit points (60 ECTS credits are the equivalent of a full year of study or work¹⁸)
- Free text description of learning outcomes: at minimum statements which indicate what a learner should have achieved in respect of both knowledge and skills at the end of a given course or programme, optionally including references to standard vocabularies such as ESCO
- The indication of the language of study

7.2 Information identifying the awarding body

Non-formal learning credential issuers should identify themselves, and – where applicable – their (and/or their programmes') accreditation status in as much detail as possible, as that could allow third parties to access information that may be a crucial aspect of recognition decision making. OEPass identified the following pieces of data to be part of the Learning Passport:

- Official name of the learning provider
- Public key (or identifier) of the institution
- Official address
- Digital version of the institution's official stamp/seal (if available)
- Information related to the accreditation, quality assurance and regulation of the institution – if applicable

¹⁷ <https://oepass.eu/outputs/learningpassport/>

¹⁸ https://ec.europa.eu/education/resources-and-tools/european-credit-transfer-and-accumulation-system-ects_en

- Home page of learning provider

7.3 Information identifying the holder of the credential

It is not only the learning credential and the issuing organisation that need to be accurately documented to facilitate credential recognition. Properly identifying the credential owners is crucial to make sure that third parties, i.e. consumers, can validate the authenticity of a quality credential.

Non-formal learning providers are, therefore, urged to document not only the names of their credential holders, but also unique identifiers, such as e.g. personal IDs, dates of birth, etc., that can be cross-checked by third-party administrators such as admission officers or HR personnel.

7.4 Credit system

The relatively simple transaction of a **Learner** engaging in a **Learning Experience** that is provided by a formal or non-formal **Awarding Body** has to be seen in a more complex system of assessment, evidencing and credentialisation. That is where the OEPass ontology provides an important visual aid to depict how learning is validated (either by the awarding body or by external assessment) with the use of assessment criteria, and how it is documented in a commonly understandable language and computer-readable credential meta-data.

An open credential, as suggested by OEPass, can be described by a long list of (mostly optional) data fields like qualification/credential title, definition, subject area, qualification level, grade achieved, etc. As mentioned before, non-formal learning can have many shapes, forms and sizes, so the OEPass ontology and Learning Passport facilitates the documentation of credential stacking, where a distinct credential can form part of a larger or include smaller components of other open credentials.

When the Learning Passport online form was developed based on the ontology, special attention was paid to provide a user-friendly mechanism to document and display the stackability aspect of credentials. The online form, that was tested by credential issuers and recognition decision makers throughout two pilot phases, also provides an intuitive flow of documentation starting with a set of basic data that can be expanded if necessary/required as the user moves along the process to record more specific information about e.g. learner authentication, achievement grades, links to credential and learning outcome evidences, etc.

8 Policies and Regulations

We envisage three courses of action for European policy-makers to foster the introduction of OEPass (or a comparable standard or initiative) as a standardized format to document micro learning. In the following, we will briefly introduce each scenario and discuss the advantages and disadvantages of each one.

Incremental change

The first scenario is one of incremental change. In this scenario, national and/or European policy-makers would foster the use of OEPass as documentation for micro learning through project funding in combination with formal requirements. When choosing funding schemes policy-makers should vote for a combination of the development of micro-learning opportunities, the use of a standardized documentation in form of OEPass and the recognition of micro-credentials. Especially funding large European consortia to pilot implementing micro-credentials and OEPass could fulfil these requirements. Optionally, large-scale piloting projects can be funded with accompanying research to learn about and better understand the internal processes and the challenges for universities to use OEPass. Additionally, specific funding for the development of micro-credentials in which OEPass is the basis for documentation could foster the micro-credential market in Europe. In the end, policy-makers could make it a general requirement for any type of European funding for micro-credentials to use OEPass as standard documentation.

Pro's:

- Policy-makers can start fostering the development of micro-credentials, the use of OEPass and recognition of micro-credentials without a time-consuming formal standardization process. Funding as described above is easy to implement for policy-makers.
- Although concerted action on a European level would be more impactful, single European countries could start funding such projects.
- By fostering not only a standard documentation but also the development and recognition of micro-credentials, the number of micro-learning opportunities for students in Europe will increase. This in turn might motivate more students to make use of micro-learning opportunities.
- Starting with a piloting phase can help to quickly reveal challenges in the implementation of OEPass on a larger scale.
- Higher education institutions are given a choice instead of being formally required to use OEPass for any of their micro-credentialing activities. In combination with a piloting phase, open discussions about the challenges, pro's and con's of OEPass can be held.

- Consequently, acceptance of HEIs might be higher than for regulation.

Con's:

- The effect of funding single projects might be too small to truly foster OEPass as a standard documentation for micro learning.
- Might not be accepted as the way to document micro-credentials.

Learning Passport through Blockchain technology

The second scenario is the introduction of OEPass as documentation for micro-learning through blockchain technology. Many actors in the European higher education system are currently learning about digital opportunities to safely issue, store and eventually recognize credentials, especially through blockchain technology. The use of blockchain technology for issuing credentials has many advantages, especially in terms of data security and protection from fraud. For micro-credentials, however, blockchain technology is valuable far beyond security reasons as it technologically enables automated stacking of security-proof credentials. As one of the basic ideas of the European higher education system is to provide stackable “pieces of learning”, e.g. ECTS, certified learning within the Bologna framework consists of building blocks and rules which can be put together to pieces, such as a module or a full degree. Blockchain technology now provides the opportunity to automatically stack certified learning to the next greater “piece” of certificate. This will be especially valuable for more open and flexible models of studying in terms of micro-learning and micro-certificates.

The introduction of a new technology might thus provide an open window for a broader push for micro-credentials and a common standard to document micro-learning in a national or the European higher education system. National or European higher education institutions could only participate in issuing and automated recognition of micro-credentials on a national or European Blockchain infrastructure if they complied to OEPass as the standard for documentation.

This third scenario combines the advantages of the two above-mentioned: A piloting phase with a small number of universities or a consortium could allow for a testing phase and uncover challenges. Beyond a pilot, however, it is closely connected to the Bologna system if it is embedded in a broader initiative to foster blockchain for issuing credentials in Europe. As such, it could help advance the European higher education system in total.

Pro's:

- A broader transition to blockchain can open and push the discourse for micro-credentials more broadly.
- Policy-makers can start fostering the development of micro-credentials, the use of OEPass and recognition of micro-credentials without a time-consuming formal standardization process. Funding as described above is easy to implement for policy-makers.
- Although concerted action on a European level would be more impactful, single European countries could start funding such projects.

- Starting with a piloting phase can help to quickly reveal challenges in the implementation of blockchain for micro-credentials and OEPass on a larger scale.

Con's:

- Blockchain still provides many challenges in terms of feasibility for large higher education systems.
- This path is only feasible if the use of OEPass is embedded in a broader Blockchain initiative.
- Introducing a new technology and new forms of credentials and their documentation at the same time provides a lot of complexity upfront.

Learning Passport through European Policy Instruments: Bologna process, Europass and ESCO

The third scenario is a formal standardization of the Learning Passport as part of the Bologna process beneath of short-cycle degrees. In this scenario, European policy-makers would establish OEPass as the standard documentation of micro-learning in Europe.

Pro's:

- Quick spreading of one European standard to document micro-learning.
- As part of Bologna, it could possible increase recognition of micro-credentials in Europe and student demand for micro-learning opportunities.

Con's:

- Protracted path.
- OEPass as a product would have to be close to final to introduce it as part of Bologna.

9 Blockchain Questions and Answers

Why a blockchain solution for digital credentialing?

Blockchain brings many possibilities that other technologies do not have. Many technological advantages of blockchain are recognized as foundational as opposed to disruptive which means it has a huge potential to reinvent our current social and economic systems. Verification of a certificate itself should have a significant impact for both higher education and lifelong learning. Discussing different conventional technical solutions (information systems, databases) in broader sense is possible, of course, but it may also be out of scope in this project. That would require a lot of effort and we do not have enough technical resources in the scope of this project. For a high quality output, we would need a technological roadmap for a completely new platform. There would be only little value in just describing a simple database solution. However, standardizing stackable learning outcomes (open credentials, micro-credentials) and putting them in a database is already a valuable project output as itself. This off-chain database may be applied in other technological solutions as well, and it is not dependant of blockchain.

Conventional technological solutions have also an increased possibility for human error due to amount of different third party members. For example, different data breaches are often unintentional. Blockchain-based solution would leverage transparency and MyData-principles with high level of privacy and cryptography.

The basic characteristics of blockchain are quite simple and compact (decentralization, immutability, pseudonymity, self-sovereignty, equitability); standards and policies in its practical implementation (proof-of-concept) are complex. Objective characteristics of technology creates explicit boundaries for discussions. It also makes the scope of the project compact, but still possibly allowing a big impact for the future. However, it is important to notice that blockchain brings up many other major challenges (as addressed below) that need to be discussed before its broader implementation.

Are Open Badges an alternative?

Standardization of learning outcomes (short learning programs, micro-credentials) allows a possibility to use different Open Badges in parallel, if needed. Open Badges is “an organic” solution, without many advantages (e.g. trust) that blockchain-based verification of certificates would bring. Using standardized and stackable micro-credentials as Open Badges is also possible. However, Open Badges and blockchain-based solutions may co-exist together, as they serve a little different purposes. Open badges can provide as just another way to display the learning outcomes but most definitely do not provide the full scale end to end functionality that a blockchain based solution is capable of.

Are Recognition Management Databases an alternative?

This is possible, but scalability within EU in HEIs and in context of open learning would probably diminish without creating an expensive platform supporting many functionalities and advantages (e.g. security, transparency, immutability, MyData) that blockchain-based solution would bring. The possibility to have a self-sovereign identity in totality for a learner where they are in charge of their personal data without the interference of a third party can only be realized with a blockchain solution.

What if the link to the course description (= credit supplement) changes?

How do you ensure that the course description database will be accessed externally? If it changes, do I get a new hash for the new course description?

New hashes to new learning descriptions should be provided, and accepted on voluntary basis. Individual should be able to keep an old description if wanted (if the original transaction is truly valid, the course has actually been completed, there are no human errors or frauds in the process, etc.). Old descriptions of learning should be accessible at all times as well. Therefore, these descriptions should be “a living document” that holds up in time (with backups and high level of security). Updating hashes to new learning descriptions should be voluntary; otherwise, MyData-principles are not met. Individuals must trust that the content of their records is permanent.

What happens if someone loses the public/private key to their wallet?

Reclaiming lost public\private keys is still a hugely contested issue among the blockchain community. The Blockchain Intelligence Group, a private entity has listed biometric tools such as fingerprint scanning, retinal scanning and facial detection as the most viable tools to solve this conundrum. However, the government regulators (in this case Education Ministries) and industry stakeholders (in this case universities and accreditation bodies) need to make a central decision on this issue since performing a large scale biometric undertaking on this scale may be a daunting task.

How do we deal with fraud and errors?

Although intrinsically secure, blockchain is still evolving as a technology on an everyday basis. Just like any other incumbent digital technology it has had its share of security breaches. The DAO (Decentralized Autonomous Organization) hack of 2016 exposed the hidden vulnerabilities of the technology. As blockchain offers a decentralized and verified system that helps to foster trust and transparency in transactions, it makes fraud hard to commit largely. This however, does not address the problem of entry of bad data in the first place. These transaction end points are the problem areas. In the clear absence of legal precedent in the case of blockchain technology, such errors or possible crimes would become hard to investigate.

UK's National Fraud Intelligence Bureau (NFIB) has tried to shed some light on the issue by defining blockchain as just one part of an anti-fraud ecosystem. Together with other technologies such as security biometrics, tougher regulations such as know-your-consumer rules and data protection laws form the other part of this ecosystem.

Redundancy, Resilience?

It is evident that a distinct level of authority and hierarchy is needed in this solution. Trusted institutions should be able to reset a password to a wallet. This should be done using high-level security protocols (verifying individual's identity with official identity document, or via bank account, biometrics). The same applies in case of an individual who wants to be "forgotten"; we need clear protocols with these cases.

E.g. what if an individual is granted a non-valid certificate (individual accepts a transaction and he/she is not willing to rewrite it later)? What if this happens on a large scale? Should the trusted institution have the power to delete or rewrite individuals' hashes in these cases? There is a need for a regulatory authority for these kind of actions. However, different third party members with such power are against the basic principles of blockchain that is based on peer-to-peer transactions and user consensus. There has to be some kind of a balance between a network (user-generated dystopia) and hierarchy (control and bureaucracy). Transactions must be based on consensus and transparency must be guaranteed, but some kind of an administrative backdoor is needed in case of possible frauds and errors. Because blockchain is a foundational technology, these mechanisms must be taken into account before implementing any large-scale solutions.

Here is one suggestion to handle these problems: in this solution, only the institution that has granted a certificate is able to delete or rewrite it. However, an individual institution is not able to delete accounts or rewrite errors without permission (consensus) of other institutions on the blockchain. Individuals are also able to control their own data; in possible conflict situations, transparency of transactions allows them to show what has happened and when.

- Regulatory layer (consensus of trusted institutions)
- Grants permissions for individual institutions to delete accounts and/or rewrite errors
- No extra 3rd party member needed
- Trusted institutions
- Resetting lost passwords (strict security protocols)
- Deleting accounts, rewriting errors (permission from other institutions needed)
- Learners
- Consensus for transactions
- Visible transaction history mitigates conflicts

What are the risks of long transaction times?

If every university will participate, how scalable is it, how long will the transactions take?

There is a constant race for "the most effective" blockchain solution. As technology evolves, transaction times are getting faster and transaction costs are getting lower (in our case, the amount of transaction costs is the most relevant question).

One of the most important questions is also who handles the mining (i.e. calculates transactions) in blockchain? For example, the computing power of most blockchains is based on private individuals who are doing the actual mining with their computers and they are rewarded with coins. The value of each coin is based on speculative market (a lot of hype, risk of bubbles). If the value of a coin drops, the miners will take their computing power elsewhere. What would be the long-standing solution with handling transactions? How easy it would be to copy the content of a blockchain to another blockchain in the future?

However, blockchain without fully decentralized mining is possible. One solution is that only trusted institutions in blockchain do the mining. As described above, there could be two layers of actors in blockchain: a) trusted institutions and b) learners. On this solution:

- the actual validation of transaction is done by every actor in blockchain (institutions and learners),
- mining is done *only* by institutions.

It could be automated that the institution with the best internet connection during the time of transaction could do the mining. To get rid of a problem of free-riding, transaction costs could be divided evenly between institutions (according to the ratio of how many % of total transactions/learners each institution bring to the ecosystem, of course). This blockchain solution is based on smart contracts, meaning that blockchain is able to handle actual algorithms on-chain (scenario X triggers action Y, etc.).

Estimation of the infrastructure needs transaction costs and running costs?

There are estimates that some blockchain solutions bring transaction costs as low as 0.001 dollars/transaction. Therefore, if one micro-credential is 2-30 ECTS, costs of transaction per student remains minimal. It is possible that some amount of extra infrastructure is needed for universities.

What is the relation between “Learner’s Wallet”, “Learning Passport”, and “Credit Supplement”?

Diploma or Credit supplement has been defined by EU Commission as a ‘document that accompanies a higher education diploma, provides a standardized description of the nature, level, context, content and status of the studies completed by its holder’. It is produced by the higher education institutions according to standards agreed by the European Commission, the Council of Europe and UNESCO. The Diploma Supplement is also part of the [Europass framework transparency tools](https://europass.cedefop.europa.eu/), (<https://europass.cedefop.europa.eu/>). The supplement is designed as an aid to help (but not guarantee) recognition – it is not a CV or a substitute for the original qualification.

It has the following sections of information:

- the holder of the qualification
- the qualification
- its level and function
- the contents and results gained

- certification of the supplement
- details of the national higher education system concerned (provided by the National Academic Recognition Information Centres (NARICs), <https://www.enic-naric.net/>)
- any additional relevant information.

Graduates in all the countries taking part in the [Bologna Process](#) have the right to receive the Diploma Supplement automatically, free and in a major European language.

The Learning Passport combines information, which the different actors in an unbundled learning system are requested to provide in order to put open learning recognition into practice. The passport consists of the three sections. The first section is designed to gather information about the learning module and about the institution, which provides it. The second section regards primarily activities that the learner was engaged in. In the last section, the Learning Passport gathers information about the institution that has assessed Learning from OER modules and awarded certification. The Learning Passport could meet great variety of needs in regards to unbundled learning scenarios such as to accommodate open learning recognition, stretching leading from specification of learning outcomes to recognition of credit.

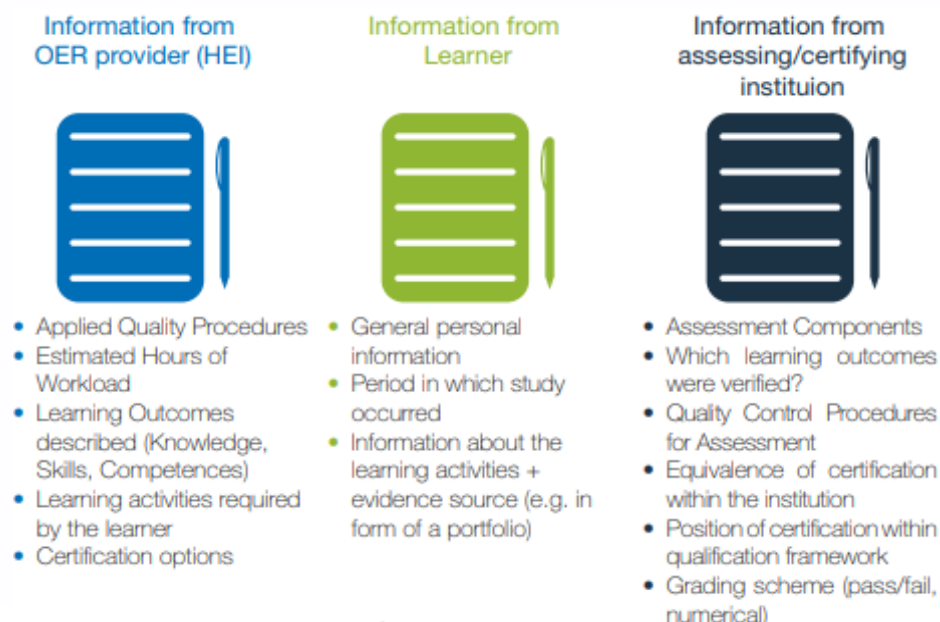


Figure 8: Basic Outline of the Learning Passport.

The Learner's wallet is an element of the blockchain-based solution to provide learners and institutions a unique identity wallet, which is owned and accessed by them through public/private keys. The wallet can be either held by institutions where it can be used to collect, display and share tokens from any accrediting authority (such as ECTS, ECVET) or it can be held by a learner where it can be used to collect, display and share tokens from any credential blockchain. Users can in turn share their wallet with external parties such as future employers.

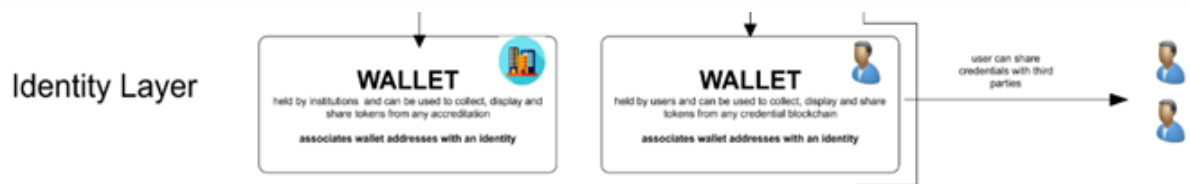


Figure 9: Identity Layer.

The Credit/Diploma Supplement would be embedded into one of the blocks on the consortium blockchain depending upon where they originate from (ECTS, ECVET). The learner's passport is basically a way to define/display the learner's wallet. It would be the information behind the digital wallet.

10 Appendix

Appendix 1: Stakeholders for Consultation and Collaboration

National Level

- National Authorities (e.g. ministries)
- National ENIC-NARIC Centres
- Higher Education Institutions
- Providers of MOOCs, OERs and other online or on-site learning
- National Accreditation Governing Bodies

Examples for Germany:

Akkreditierungsrat, <http://www.akkreditierungsrat.de/>

The Accreditation Council has the task of deciding on the accreditation of study programs (program accreditation) and the accreditation of quality management systems (system accreditation) based on expert opinions. The implementation of so-called alternative procedures, with which new paths in quality development are to be tested, also requires the approval of the Accreditation Council. While responsibility for the accreditation decisions has now passed to the Accreditation Council, the implementation of the evaluation procedures in programme and system accreditation remains in the hands of the accreditation agencies authorised for this purpose. The accreditation of an agency is subject to its EQAR registration by the Accreditation Council.

European Level

ENIC-NARIC Networks, <http://enic-naric.net/>

The ENIC Network (European Network of Information Centres)

To implement the Lisbon Recognition Convention and, in general, to develop policy and practice for the recognition of qualifications, the Council of Europe and UNESCO have established the ENIC Network (European Network of National Information Centres on academic recognition and mobility). The Council of Europe and UNESCO jointly provide the Secretariat for the ENIC Network. The ENIC Network cooperates closely with the NARIC Network of the European Union.

The Network is made up of the national information centres of the Parties to Lisbon Recognition Convention. An ENIC is a body set up by the national authorities. While the specific competences of ENICs may vary, they will generally provide information on:

- the recognition of foreign diplomas, degrees and other qualifications;
- education systems in both foreign countries and the ENIC's own country;
- opportunities for studying abroad, including information on loans and scholarships, as well as advice on practical questions related to mobility and equivalence.

The NARIC Network (National Academic Recognition Information Centres)

The NARIC network is an initiative of the European Commission and was created in 1984. The network aims at improving academic recognition of diplomas and periods of study in the Member States of the European Union (EU) countries, the European Economic Area (EEA) countries and Turkey. The network is part of the Community's Lifelong Learning Programme (LLP), which stimulates the mobility of students and staff between higher education institutions in these countries.

All member countries have designated national centres, the purpose of which is to assist in promoting the mobility of students, teachers and researchers by providing authoritative advice and information concerning the academic recognition of diplomas and periods of study undertaken in other States. The main users of this service are higher education institutions, students and their advisers, parents, teachers and prospective employers.

The NARICs were designated by the Ministries of Education in the respective countries, but the status and the scope of work of individual NARICs may differ. In the majority of States, institutions of higher education are autonomous, taking their own decisions on the admission of foreign students and the exemption of parts of courses of study programmes that students may be granted based on education undertaken abroad. As a result, most NARICs do not take a decision, but offer on request information and advice on foreign education systems and qualifications.

DG EAC, https://ec.europa.eu/info/departments/education-youth-sport-and-culture_en

The Directorate General for Education and Culture (DG EAC) is the executive branch of the European Union responsible for policy on education, culture, youth, languages, and sport. DG EAC also supports these issues through a variety of projects and programmes, notably Creative Europe and Erasmus+.

European Quality Assurance Register for Higher Education (EQAR), <https://www.eqar.eu/>

In most European countries, higher education institutions or study programmes are subject to regular external review by a quality assurance agency. The European Quality Assurance Register for Higher Education (EQAR) is a register of such agencies, listing those agencies that have demonstrated their substantial compliance with a common set of principles for quality assurance in Europe. These principles are laid down in the Standards and Guidelines for Quality Assurance in the European Higher Education Area.

EQAR aims to provide the public with clear and reliable information on quality assurance agencies operating in Europe, and the register is therefore web-based and freely accessible.

European Association for Quality Assurance in Higher Education (ENQA), <http://www.enqa.eu/>

The European Association for Quality Assurance in Higher Education (ENQA) is an umbrella organisation, which represents quality assurance organisations from the European Higher Education Area (EHEA) member states. ENQA promotes European co-operation in the field of quality assurance in higher education and disseminates information and expertise among its members and towards stakeholders in order to develop and share good practice and to foster the European dimension of quality assurance.

European Students' Union (ESU), <https://www.esu-online.org/>

The European Students' Union (ESU) is the umbrella organisation of 45 National Unions of Students (NUS) from 39 countries. The aim of ESU is to represent and promote the educational, social, economic and cultural interests of students at the European level towards all

relevant bodies and in particular the European Union, Bologna Follow Up Group, Council of Europe and UNESCO. Through its members, ESU represents around 15 million students in Europe.

European University Association (EUA), <http://www.eua.be/>

The European University Association (EUA) is the representative organisation of universities and national rectors' conferences in 47 European countries. EUA plays a crucial role in the Bologna Process and in influencing EU policies on higher education, research and innovation. Thanks to its interaction with a range of other European and international organisations EUA ensures that the independent voice of European universities is heard, wherever decisions are being taken that will affect their activities.

European Association of Institutions in Higher Education (EURASHE), <https://www.eurashe.eu/>

According to its statutes, the mission of EURASHE is to promote, within the European Higher Education Area (EHEA), the interests of professional higher education and of relevant higher education institutions that are recognised or financed by the public authorities of an EHEA member country.

European Centre for the Development of Vocational Training (CEDEFOP), <http://www.cedefop.europa.eu/en>

Helping develop the right policies to provide the right skills. Cedefop is one of the EU's decentralised agencies. Founded in 1975 and based in Greece since 1995, Cedefop supports development of European vocational education and training (VET) policies and contributes to their implementation. The agency is helping the European Commission, EU Member States and the social partners to develop the right European VET policies.

International Level

Postsecondary Electronic Standards Council (PESC), <http://www.pesc.org>

PESC leads the establishment and adoption of open data standards across the education community by serving as an open standards-development and open standards-setting body producing PESC APPROVED STANDARDS. PESC members believe that fostering open, transparent collaboration across educational communities to solve common, industry-shared problems brings much needed clarity and coherence to the education ecosystem.

Appendix 2: ESCO, ISCO and EQF

ESCO is the multilingual European classification of **S**kills, **C**ompetencies, qualifications and **O**ccupations (ESCO, 2013, p. 2). "It identifies and categorizes all of those which are relevant for the EU labour market and education and training, in 25 European languages. The system provides occupational profiles showing the relationships between occupations, skills, competences and qualifications" (ESCO, 2013, p. 2) – an ontology, taxonomy or a classification.

"By introducing a standard terminology for occupations, skills, competences and qualifications, ESCO can help education and training systems and the labour market to better identify and manage the availability of required skills, competences and qualifications" (ESCO, 2013, p. 2).

"Jobseekers can use ESCO to describe their skills, competences and qualifications when de-

veloping their CV, which can then go through various automated or machine matching processes. They can also compare their skills, competences and qualifications against job vacancies using ESCO terminology, to identify the skills they are lacking” (ESCO, 2013, p. 4).

Connecting ESCO and ISCO: “ESCO’s occupations pillar is structured in a hierarchical way and linked to [the International Standard Classification of Occupations or] ISCO, developed by the International Labour Organisation (ILO). This allows statistical data [acquired] through the use of ESCO to be comparable at international level” (ESCO, 2013, p. 12).

Connecting ESCO and EQF: The EQF aims to increase the comparability of levels of qualifications across borders. However, qualifications do not always keep pace with the evolution of knowledge, skills and competences needed by the labour market. “Employment services do not share the same IT and classification systems to manage information on the supply and demand of jobs” (ESCO, 2013, p. 2). EQF is incorporated into ESCO. “In addition, National Qualifications databases developed by the Member States and referenced to the EQF will, in the future, feed into ESCO” (ESCO, 2013, p. 16).

Connecting ESCO, ISCO and EQF: “The ESCO classification is composed of modules that contain elements such as occupations, knowledge, skills and competences, qualifications, and the International Standard Classification of Occupations (ISCO) hierarchy. When combined and interrelated, these modules make up the whole [ontology/] classification” (ESCO, 2017c). “The qualifications pillar of ESCO is developed in a way that is consistent with the EQF. This will allow building on the results achieved during the work on the EQF, including National qualification databases” (ESCO, 2018b).

“ESCO has been developed in an open IT format and is available for use free of charge by everyone and can be accessed [through an online] portal” (ESCO, 2017b). “ESCO can be used by developers as a building block for different types of applications that provide services such as auto complete, suggestion systems, job search algorithms and job matching algorithms.

The ESCO classification is published in SKOS-RDF format and soon will be published in CSV and XML formats, in order to enable users to integrate it into their applications and services” (ESCO, 2017c).

ESCO is available as Application Program Interface (API), other important APIs are for example Google Translate. “The web-based service API is designed to support interoperable machine-to-machine interaction over the World Wide Web” (ESCO, 2018a) - “a software component facilitating the interaction with other software components.” “ESCO will offer access to the classification through APIs” (ESCO, 2018a). “with a set of services and functionalities published in the Web that allow other applications to access the ESCO classification” (ESCO, 2018a).

“The Commission services have set up a process to continuously improve the ESCO classification and keep it up-to-date when new versions are released” <https://ec.europa.eu/esco/portal/howtouse/6af39243-1e25-484b-af62-ad223a9c48b8> (ESCO, 2017c). The Commission will regularly review the continuous improvement process itself, in order to make it as efficient as possible. “The ESCO Maintenance Committee will continue playing an important role on the continuous improvement of the ESCO classification. The ESCO Maintenance Committee will include custodians of national and international classifications, ESCO implementers and cross-sectoral domain experts” (ESCO, 2017a).

Appendix 3: EQF

“The [...] [European Qualifications Framework] (EQF) has been a trigger for a shift to learning outcomes. The linking of national qualifications frameworks (NQFs) to the EQF [...] [was] expected to be completed in 2014, thus signalling that the learning outcomes approach has been broadly accepted as the basis for future European cooperation in the area of education and training. The introduction of the EQF, and the rapid development of NQFs, is increasingly influencing the writing of curricula and qualification standards, focusing on what a learner is expected to know, understand and be able to do. Increasingly we observe that this shift influences the way teaching and training is organized and assessment is carried out” (ESCO, 2018b).

“EQF makes qualifications more readable and understandable across different countries and systems in Europe and is a translation tool that helps communication and comparison between qualifications systems in Europe” (European Communities, 2008). Its eight common European reference levels are described in terms of learning outcomes: knowledge, skills and competences (van den Broek & Buchem, 2017). This allows any national qualifications systems, national qualifications frameworks (NQFs) and qualifications in Europe to relate to the EQF levels. “Learners, graduates, providers and employers can use these levels to understand and compare qualifications awarded in different countries and by different education and training systems” (European Commission, 2018).

Annexe 4: Initiatives for Digital Credentials

The following is a list of different European Initiatives for digital credentials:

- Open Badges on the Blockchain - Open University UK, Knowledge Media Institute
Introduction of OpenBadges data related to the OpenLearn web access into a set of Ethereum Smart Contracts, allowing storing the certificates from different sources in the same place.
<http://kmi.open.ac.uk/review/pdf/kmi-review-issue-10-2017.pdf>
<https://openbadges.org/about/>
- UNIC's Blockchain Initiative for academic certificates - University of Nicosia
Use of Bitcoin blockchain technology to issue electronic PDFs verifiable through UNIC's website verification tool or by replicating UNIC's open-source instructions (available at block.co).
<https://block.co/blockchain-certificates/>
- Blockchain in education pilots - Government of Malta
Implementation of a nation-wide pilot project for academic credentialing and professional certifications using Blockcerts open standards, defined by the Malta Qualifications Framework (MQF) and adapted to the European Qualifications Framework (EQF).
<http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/>
<https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/September/15/PR172070.aspx>

- Recipient-owned credentials - The University of Melbourne
Issuance of a Teaching Certificate using the Learning Machine issuing system based on Blockcerts open standards.
<http://newsroom.melbourne.edu/news/university-melbourne-issue-recipient-ownedblockchain-records>
- Infrastructure to issue digital certificates - Aristotle University of Thessaloniki PKI
Issuance of Qualified Certificates for e-Signatures following European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
<https://pki.auth.gr/index.php.en>
- Digital Badge Academy - Sussex Downs
Use of Digitalme's Open Badge Academy to showcase skills in a "digital and verifiable way" through endorsements by experts, educators and peers.
<https://www.openbadgeacademy.com/sussexdowns>
- HfdCert - Stifterverband and German Recotr's Conference
teachers and students with teaching duties register on a newly developed certification platform and submit evidence of their activities in the field of digital teaching and learning.
<https://hfdcert.de/>
- Teacher's badges - Oulu University, partners, and the Ministry of Education of Finland
Creation of a new system to be applied across educational sectors which will consist of a shared structure, model, and awarding criteria for badges to recognise the competences of teachers.
<http://www.digital-competences-for-teachers.eu>
<http://www.oppiminenonline.com/>
- Digital Certificates Project - MIT Media Lab Learning Initiative and Learning Machine
Development of a system to ensure the management, ownership, transferability, longevity and trust of certificates through tools, software and strategies related to the bitcoin blockchain technology.
<http://certificates.media.mit.edu/>
- Blockchain for education - Fraunhofer Institute for applied information technology
Creation of a platform to facilitate certificates management through smart contracts in the Ethereum blockchain.
<https://www.fit.fraunhofer.de/en/fb/cscw/blockchain.html>
- Edubadges - SURF
Issuance of micro-credentials that cover both formal and non-formal learning and exploration of the use of blockchain in combination with the Edubadges infrastructure.
<https://www.surf.nl/en/innovationprojects/customised-education/edubadges-and-microcredentialing.html>
<https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/whitepaper-onopen-badges-en-micro-credentials.pdf>
- Lifelong learning competencies on the blockchain - VDAB & GO!
Linkage of competencies to individuals through a "bring-your-own-standards" blockchain-based online platform, through which future employers will be able to consult

candidates' diplomas but also their skills.


<https://medium.com/wearetheledger/bring-your-own-standard-426da33034ca>

- Badgr - Concentric Sky
Use of a free and open source achievement recognition and tracking system to issue, organise, and share Open Badges offered as a service or as an open source.
<https://badgr.com/>
- Digital Badges - Acclaim
Issuance of badges compliant with the Open Badge Infrastructure (OBI) metadata, allowing users to store and share their badges in their profile or in other OBI-compliant badge wallets.
<https://www.youracclaim.com/>
- Credentials Dashboard – Accredible
Issuance of certificates and badges that are verified in the platform through third parties or by using blockchain technology.
<https://www.accreditable.com/>
- IndiaChain – Government of India, Niti Ayog
Implementation of a blockchain-based solution linked to IndiaStack, a government identification database.
<http://indiastack.org/>
<https://www.newsbtc.com/2018/02/06/indiachain-governments-blockchain-basedcertification-for-education-degrees/>

11 References

- Code University of Applied Sciences (2018). Lernkonzept. Retrieved from <https://code.berlin/de/concept/>
- Connecting Credentials (2016). Glossary of Credentialing Terms. Retrieved from <http://connectingcredentials.org/resources/quality-dimensions-connected-credentials/>
- The EAR HEI and STREAM projects. (2016). The European Recognition Manual for Higher Education Institutions: Practical guidelines for credential evaluators and admissions officers to provide fair and flexible recognition of foreign degrees and studies abroad (2nd edition). Retrieved from <http://www.enic-naric.net/ear-manual-standards-and-guidelines-on-recognition.aspx>
- The Economist (2017). Lifelong learning is becoming an economic imperative. *The Economist*. Retrieved from <https://www.economist.com/news/special-report/21714169-technological-change-demands-stronger-and-more-continuous-connections-between-education>
- ESCO. (2013). *European Classification of Skills/Competences, Qualifications and Occupations : the first public release*. Luxembourg: Publications Office of the European Union. Retrieved from http://europa.eu/citizens-2013/sites/default/files/content/publication/DGEMPL_ESCO_EN_Accessible.pdf
- ESCO (2017a). Continuous improvement workflow for ESCO: European Skills, Competences, Qualifications and Occupations. Retrieved from <https://ec.europa.eu/esco/portal/document/en/f834e202-0ebf-461a-9249-a00e91d86e94>
- ESCO (2017b). European Skills, Competences, Qualifications and Occupations (ESCO). Retrieved from <https://data.europa.eu/euodp/de/data/dataset/european-skills-competences-qualifications-and-occupations>
- ESCO (2017c). How to implement ESCO: Using ESCO. Retrieved from <https://ec.europa.eu/esco/portal/howtouse/6af39243-1e25-484b-af62-ad223a9c48b8>
- ESCO (2018a). ESCO API. Retrieved from https://ec.europa.eu/esco/portal/escopedia/ESCO_API
- ESCO (2018b). European Qualifications Framework (EQF). Retrieved from https://ec.europa.eu/esco/portal/escopedia/European_Qualifications_Framework_%2528EQF%2529
- ESG. (2015). Standards and guidelines for quality assurance in the European Higher Education Area (ESG). Brussels, Belgium. Retrieved from <https://enqa.eu/index.php/home/esg/>
- European Commission (2018). Showing and using skills. Retrieved from <http://ec.europa.eu/social/main.jsp?catId=1217&langId=en>
- European Communities. (2008). *The european qualifications framework for lifelong learning (EQF)*. Luxembourg: Office for Official Publications of the European Communities. Retrieved from http://ecompetences.eu/wp-content/uploads/2013/11/EQF_broch_2008_en.pdf
- European Union. (2015). *ECTS User's Guide 2015*. Retrieved from https://ec.europa.eu/education/ects/users-guide/docs/ects-users-guide_en.pdf
- Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. (EUR 28778 EN). Retrieved from http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf

- Kiron Open Higher Education (2017). Quality Handbook. Retrieved from https://kiron.ngo/wp-content/uploads/2017/11/2017-11-01_Quality-Handbook-V1.pdf
- Nuffic. (2012). *European Area of Recognition Manual*. Retrieved from http://eurorecognition.eu/manual/EAR_manual_v_1.0.pdf
- PARADIGMS (2018). Oops a MOOC!: Dealing with eclectic learning in credential evaluation. Retrieved from <https://www.nuffic.nl/en/publications/find-a-publication/oops-a-mooc.pdf/view>
- Rampelt, F., Niedermeier, H., Röwert, R., Wallor, L., & Berthold, C. (2018). Digital anerkannt. Möglichkeiten und Verfahren zur Anerkennung und Anrechnung von in MOOCs erworbenen Kompetenzen. (Arbeitspapier 34). Berlin.
- Riksen, D., & Kerver, B. (2016). *Whitepaper on Badges and Microcredentials*. Retrieved from <https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/whitepaper-on-open-badges-en-micro-credentials.pdf>
- SUNY (2018). Micro-credential Definition - SUNY. Retrieved from <http://system.suny.edu/academic-affairs/microcredentials/definitions/>
- Van den Broek, E., & Buchem, I. (2017). White Paper on Open Badges at Policy Levels. Retrieved from http://www.openbadgenetwork.com/wp-content/uploads/2017/09/O5-A2_Policy-White-Paper_DUO_FINAL.pdf
- Witthaus, G., dos Santos, A. I., Childs, M., Tannhäuser, A.-C., Conole, G., Nkuyubwatsi, B., & Punie, Y. (2016). *Validation of Non-formal MOOC-based Learning: An Analysis of Assessment and Recognition Practices in Europe (OpenCred)*. EUR 27660 EN, doi:10.2791/809371.
- World Economic Forum (2016). The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. Retrieved from http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf



This technological roadmap describes what is required to create a system for issuing, verifying and sharing micro-credentials in terms of ECTS. It proposes the creation of a Learning Passport that allows students to store credentials from different educational providers all in one place and selectively share them with educational institutions and employers.

The switch from paper-based to digital credentials offers advantages to learners and employees, to educational institutions and to potential employers. A system of universally recognized and stackable micro-credentials for smaller units of learning below degree level (both online and offline) enhances student mobility and employability and enables truly flexible learning paths. It has the potential to take life-long learning to a new level.



Co-funded by the
Erasmus+ Programme
of the European Union