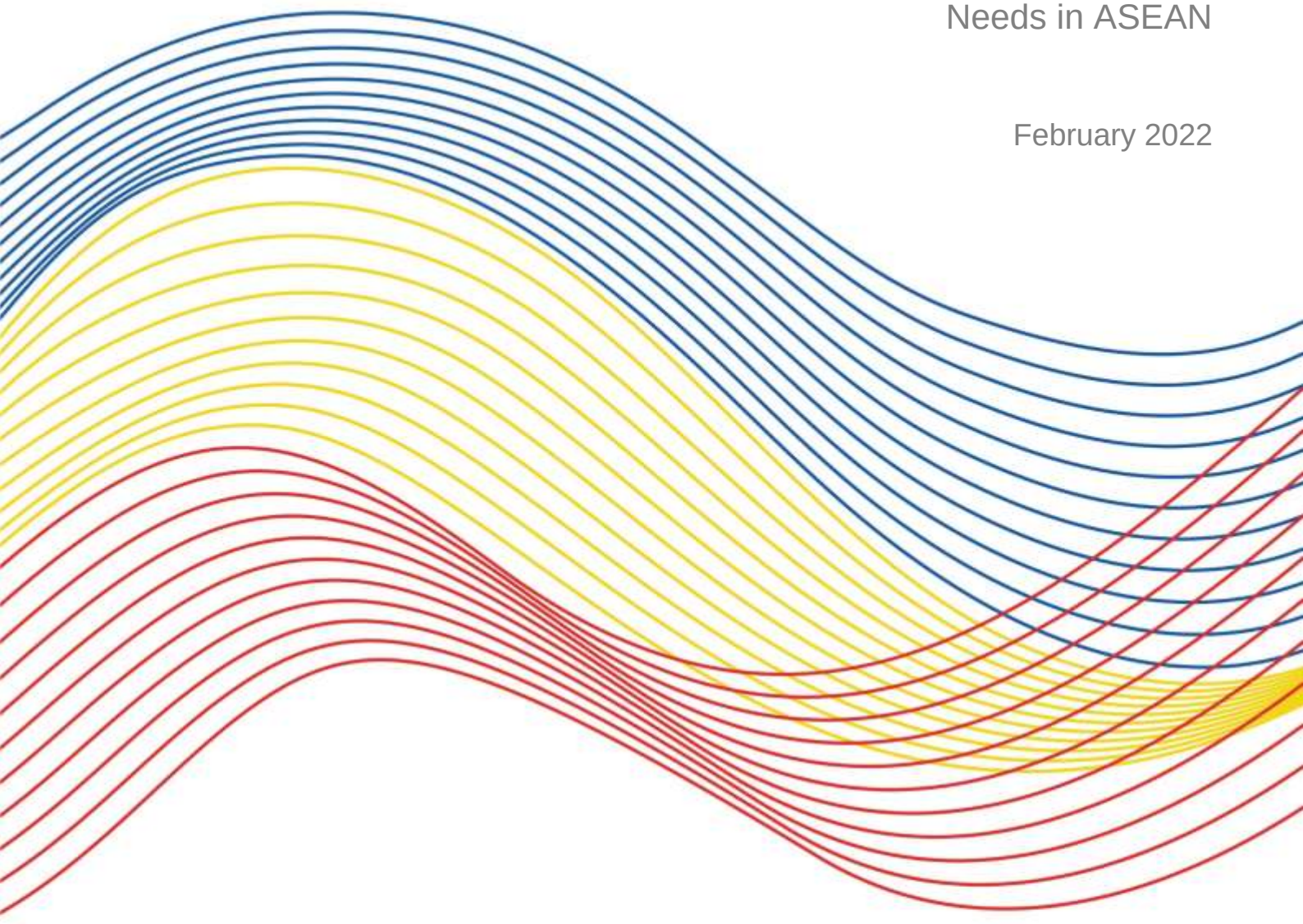
Digital Credential Recognition

Mapping and Identification of Digital Credit Transfer System Needs in ASEAN

February 2022



Mr. Anthony F. Camilleri

Dr. Sintho Wahyuning Ardie

SHARE – Support to Higher Education in the ASEAN Region – is a European Union (EU) Grant funded project with an overarching objective to strengthen regional cooperation, enhance the quality, competitiveness and internationalisation of ASEAN higher education institutions and students, contributing to an ASEAN Community. The main aim of SHARE is to enhance cooperation between the EU and ASEAN to create an ASEAN Higher Education Space.

SHARE Project Management Office
ASEAN Secretariat
Heritage Building
70 Jl. Sisingamangaraja
Jakarta 12110
Indonesia
Phone: +62 (21) 726 2991
E-mail: info@share-asean.eu
Website: www.share-asean.eu

Table of Contents

Executive Summary 1
1 Introduction 5
1.1 Terms of Reference 5
1.1.1 What do we Mean by Credential Recognition? 5
1.2 Types of Digital Credentials 7
1.3 Models and Types of Recognition 9
2 Global Standards for Digital Credentials 11
2.1 European Learning Model 11
2.2 ELMO 13
2.3 The Comprehensive Learner Record (CLR) 14
2.4 Open Badges 14
3 Applications of Digital Credential Recognition 18
3.1 Management of Student Mobility 18
3.1.1 Erasmus Without Paper 18
3.2 Digital Credentialling 20
3.2.1 Digital Credentials Consortium 20
3.2.2 Europass and European Digital Credentials for Learning 20
3.3 Transfer of Credentials between institutions 22
3.3.1 EMREX 22
4 Digital Credential Recognition in the ASEAN+3 region 25
4.1 National or Regional Digital Credentials Initiatives 25
4.2 Digital Credentials Issuing and Recognition in ASEAN HEIs 27
5 Success Factors for Digital Credential Recognition 30
6 Conclusions and Recommendations for Digital Credential Recognition 33
6.1 Develop a Regional, Full-Lifecycle Approach to Digital Credential Recognition. 33
6.2 Pursue Alignment with EU Standards for Mobility and Credentialling 33
6.3 Use Inter-Institutional Agreements to Regulate Recognition in the short-term 34
6.4 Establish a Credential Recognition Centre of Excellence 34
6.5 Consider open and self-sovereign data management paradigms 35
Annex 1: Focus Group Discussion on Digital Credit Transfer Systems 37
Annex 2: Actors in Digital Credentialling 41
Badgr 41
Accredible 41
Hyland 42
Digitary and Parchment 42
Azure AD Verifiable Credentials 44

Table of Figures

Figure 1: Student Journey showing all applications of Credential Recognition for different types of mobility 6
Figure 2 Methods for Digital Signing and Verification of Documents 8
Figure 3: Envelope and Content of a Digital Document 9
Figure 4: Explanation of the types of claims that can be expressed by European Digital Credentials for Learning 11
Figure 5: Depiction of the European Learning Model and its relationship with learning opportunities and credentials 12
Figure 6 Sample code from the elmo schema.xsd 13
Figure 7: Open Badge full life cycle according to the Open Badge spec (IMS Global, 2018). 15
Figure 8: Screenshot of the Erasmus Dashboard 19
Figure 9 Europass portal's homepage 21
Figure 10 : Data content and verification checks of a sample Europass Digital Credential visualised in the EDC Viewer 22
Figure 11: Graph of the Network Effect and Indication of Critical Mass 31
Figure 12: Functions of a Centre of Excellence 34
Figure 13 Digitary CORE works around a triangle model of issue, share and verify 43

Executive Summary

This study, carried out during June-September 2021, gives an overview of digital credential recognition, its implementation globally and within the ASEAN region. It also gives recommendations on deployment of systems for digital documents and enhancing their recognition throughout the region. The study is a result of a literature review, the testing of different digital credential recognition systems as well as workshops and interviews with relevant stakeholders in ASEAN as well as Europe.

The focus of this study is on credentials for student mobility, which includes credentials for credit transfer between institutions within the context of a single programme, for mobility between institutions after completion of a programme as well as for mobility between academia and the labour market after graduation. Digital credentials are defined as digital documents, which make claims about persons, which contain data machine-processable data.

The digital recognition of such credentials implies the ability of a verifier to receive such a document, to check its authenticity, process it according defined formats and schemas, and make an educated recognition decision on that basis.

Digital credentials are all reliant on data standards to convey information. The European Learning Model (ELM) is an open-source standard used to describe information about learning opportunities, qualifications, credentials and accreditation, and is promulgated by the European Commission throughout the EU Education Area. It is used to power educational services in the Europass platform, as well as to exchange this data between countries. The ELMO format is produced by a group of countries and is intended specifically for Higher Education data interchange between countries, in particular for sharing transcripts of records between countries. The Comprehensive Learner Record is an analogous standard to the ELM, with a more US focus. Open Badges are an open-source standard that is used to created digital documents encoded into images – these are mainly used as records of achievement in non-formal education use-cases.

Document transfer in this area is done via three different categories of software. Student Mobility software allows for institutions and students to exchange mobility learning agreements, and then, at the end of a mobility programme, to exchange a transcript of records between the institutions. The most common initiative for this is Erasmus without Paper (currently being rebranded into the European Student Card Initiative) which allows for this interchange between over 3000 universities in Europe. Digital Credentialing software allows for the award of credentials to students. Students store these credentials in their own wallets, and may share them for the purposes of recognition with their own institution, with other educational organisations or with employers. There are currently multiple public and private providers of digital credentials globally. Of note are the European and MIT-led initiatives, each of which are developing open ecosystems of standards and software around digital credentials. Within ASEAN+3, significant initiatives have been noted in Japan via the RECSIE system, Indonesia via the implementation of blockchain credentials into ICE-network, and in Singapore via the OpenCerts system. OpenCerts in particular is considered a global reference project in using blockchain technology to secure credentials. Transfer of credentials between institutions is regulated by a third type of software, which creates interchange networks between organisations – an example of this is the EMREX system, also in Europe that facilitates exchange of credentials between different universities' student information systems.

Our research with representatives of SHARE partner universities from throughout the ASEAN region, indicates that the use of digital documents to regulate mobility and/or recognition is still not common, and where it exists, is limited to paper-analogues such as PDF, rather than involving the exchange of true computer-readable documents.

This said, the policies of governments in Indonesia, Philippines, Vietnam and Singapore increasingly support digital credentialling, albeit at very different stages of development. In Malaysia and Thailand, pockets of expertise exist in specific, usually private, institutions, while Cambodia, Myanmar and Laos have yet to develop anything in the area.

Taken as a whole, the region has yet to overcome challenges to the adoption of digital credential recognition. These are related to the technological capacities of institutions in terms of technical and human resources, lack of infrastructure and knowledge of e-signatures, institutional cultures built around paper credentials, lack of government support for digitisation and a lack of common standards for digital credential recognition across the region. Despite these, the development of a digital credential system is still seen as an important priority, and even more so during the current pandemic.

To guide further development of systems, the study identifies a set of implementation success factors based on the case studies mentioned above – with success being defined as the ability to reach critical mass whereby the user base is enough for the network to be self-sustaining. Successful digital mobility and digital credentialling systems are governed by public authorities or multi-stakeholder groups and are based around open standards and software. The systems are not built as separate software packages but are ecosystems of software, with different providers each connecting different applications to the network. The systems are typically backed by extensive documentation, developed over several years of testing and piloting, and are continually reviewed and updated based on institution and user feedback. Finally, they are often integrated into wider projects on the digital labour market, rather than focusing solely on a narrow educational use case.

The study finds that digital credential recognition in the region can be significantly boosted by leveraging on existing global standards, software and networks. In the short-term an initiative led by a university-consortium could bring significant benefits from student mobility. This could be expanded to more user cases, and be applied to more institutions with time.

We find that given the state of development of digital credentials globally, and the inherent advantages of these for users, the time is right to initiative a regional initiative for digital credentialling with in ASEAN. There is no need to develop ASEAN-specific data-standards and software, since the mobility and credentialling processes are close enough to those used in Europe and are aligned closely enough to be able to adapt these to local use. We recommend that using the European Learning Model as a basis, such a consortium would start with digitising credit transfers between institutions for mobility, and then move on to award of credentials to students, transfer of programme credentials between institutions and finally transfer of credentials to third parties such as employers.

Such a system should prioritise student data portability, and user-ownership of their own data, while using decentralised paradigms of technology and governance to mitigate the need of creating a centralised management authority. Critical to supporting such a development would be the creation of an ASEAN Centre of Excellence in Digital Credential Recognition. Such a Centre would monitor global developments, make recommendations on standards and software for use in the region and localise these. It would assist in capacity building of educational organisations and training of key staff.

Finally, it would manage the backbone of the network connecting institutions together, and manage its growth.

Through such an approach, institutions in the ASEAN region have an opportunity to make a generational change in the management of credential recognition in a comparatively short period of time, bringing efficiency gains to institutions and improving credential-portability and recognition for students.

CHAPTER 1

CHAPTER 1

1 Introduction

1.1 Terms of Reference

This study is to map the implementation of digital credential recognition by universities and organisation in the ASEAN region. The study will also explore the implementation of digital credential recognition conducted in other universities and organisations outside of the ASEAN region, particularly in Europe. The outcome is to identify the best practices and lessons learned in digital credential recognition and how this digital solution can facilitate the recognition and support the mobility of learners, which later can be applied to enhance the SHARE CTS Platform.

1.1.1 What do we Mean by Credential Recognition?

Broadly speaking, a credential can be described as **any document that makes claims about a person.** Thus, on enrolment, students may be present identity credentials, as well as credentials which prove their prior learning. A student card is a credential which proves that a student is a member of a specific institution, while a transcript of records is a credential which attests to a person's academic performance.

Recognition requires a credential to be:

a. presented to a verifying party for a particular purpose;
b. accepted as authentic by the verifying partying;
c. accepted as appropriate for the purpose for which it was presented by the verifying party.

The focus of this study is on credentials for student mobility, which is categorised in three types of mobility, namely:

- credit transfer between institutions within the context of a single programme;
- mobility between institutions after completion of a programme;
- mobility between academia and the labour market after graduation.

Within this context, the study addresses a set of use cases, namely:

- creation of transcripts of student records within an institution, i.e., recording the results of each student for various modules, based on assessments and the transfer of this document between institutions;
- issuance of digital records of achievement based on these transcripts to students, and signing or securing these credentials so that they cannot be easily tampered with
- retrieval of credentials by students from their institution, or storage of those credentials by a student, and to sharing of them with third parties such as employers
- preparation and exchange of credentials entitling students to participate in student exchanges, and further to have their learning recognised by their home institutions

The diagram on the next page shows an idealised student journey encompassing all of these steps.

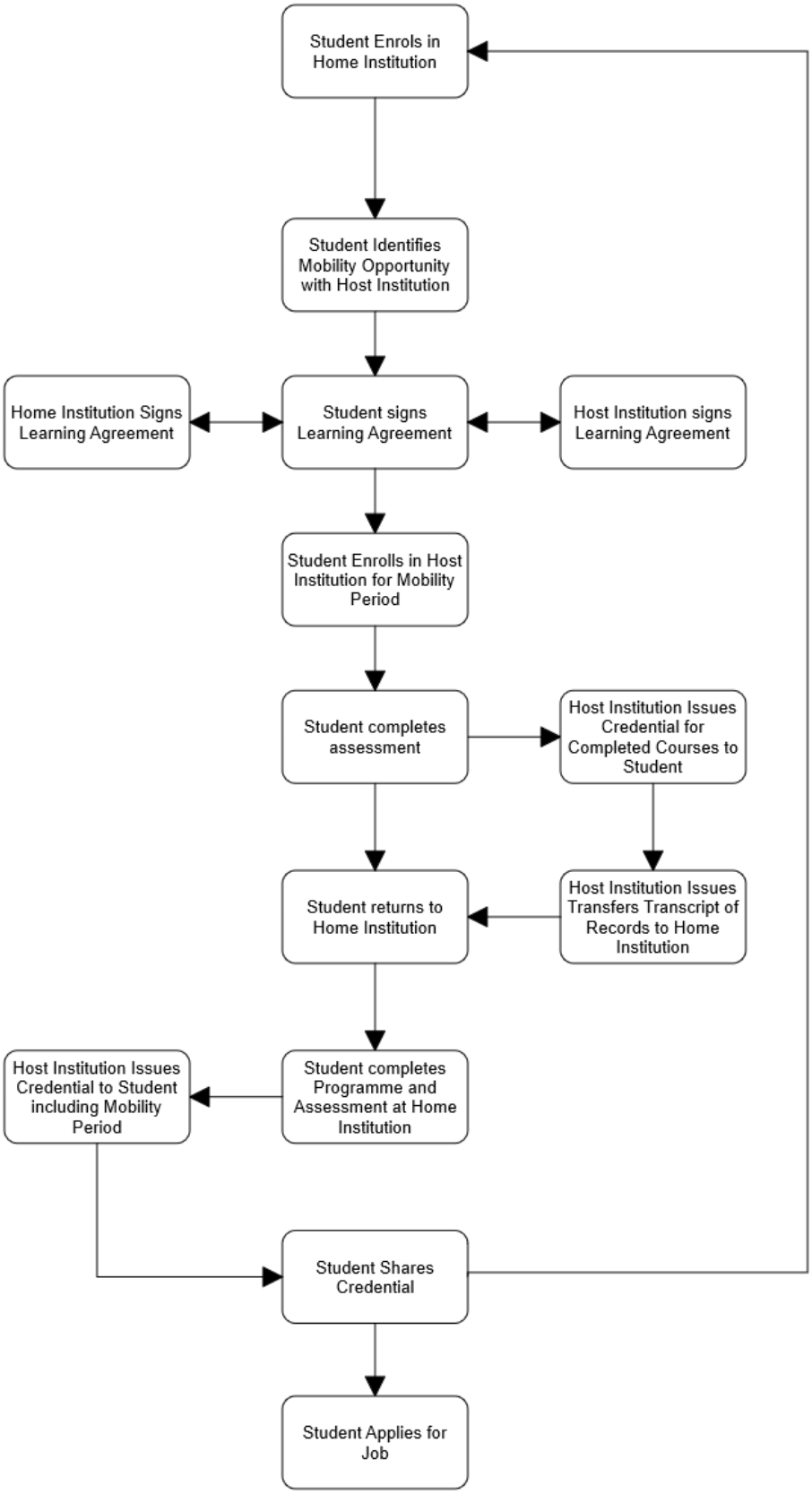


Figure 1: Student Journey showing all applications of Credential Recognition for different types of mobility

1.2 Types of Digital Credentials

At a high-level, digital documents may take three forms.

Digital Reproductions

At the most basic level, credentials may consist of reproductions of paper documents. These are usually scanned versions or photographs of paper certificates. For many low-security applications, these are considered to be equivalent to paper documents. These are typically not considered 'true' digital certificates and are not further discussed in this study.

Unsigned Digital Documents

Unsigned digital documents consist of digital documents which contain data. These include documents with a 'visual layer' such as PDF or Word documents, but often can include pure machine-readable formats such as XML or JSON. They hold many advantages over paper certificates in that they require less time and far fewer resources to issue, maintain and use. In particular, their issue can be automated, as can their processing, allowing e.g., for the validity of their content to be verified by algorithms allowing for use cases such as automatic processing of mobility or job applications. Digital certificates hold additional advantages in that they can easily be issued multilingually, and in many systems they may be revoked by the issuer.

Unsigned digital documents are however extremely easy to edit, forge and reproduce at scale and as such their use is not recommended for any trust-based applications. Thus, typically they are not held or shared directly by users, as a verifier can have no guarantee that the user has not modified the document. Rather, they require the issuer to maintain a registry of documents which can be accessed by a third party, whereby they may verify the veracity of any specific document. Should the registry fail, the certificates themselves become worthless since unlike paper certificates, they hold no intrinsic value without the registry. Furthermore, these registries are prone to large-scale data-leaks or sophisticated data tampering operations (hacking).

Digitally-Signed Documents

Digitally-signed documents are both computer-readable and tamper-evident. The security of the document 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.

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.

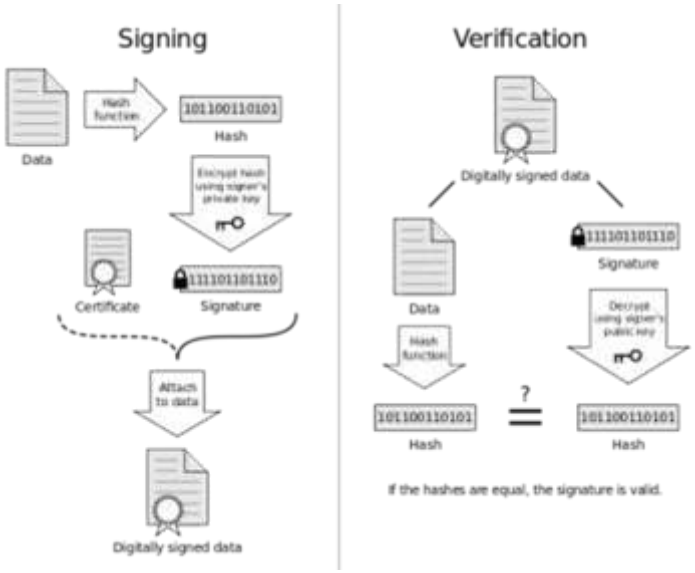


Figure 2 Methods for Digital Signing and Verification of Documents

Critically, where a document that has been digitally signed is modified after issue, this becomes immediately visible to a verifier, analogous to how breaking a wax seal on a document gives instant recognition that the document has been tampered with. The institution issuing the credential no longer needs to be responsible for verifying the document after issuing - it becomes self-verifiable. Since a registry is not required to verify the digital document, the recipient of a credential can store the credential themselves, and they can directly share it with a third party such as an employer or an educational institution. This gives them much better control over their data, and allows them, rather than the issuing organisation to determine who can access it under what conditions.

However, digital signing of documents has yet to become commonplace, because 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. Furthermore, correctly implementing signature protocols adds a large degree of complexity to any system, increasing price and often decreasing ease of use. Digital signatures also 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 can be abused – often through the use of exploitative pricing models. While distributed ledger (blockchain) technologies potentially solve many of the issues around digital signatures, their implementation is still in nascent phases and in most cases are not ready for production environments.

1.3 Models and Types of Recognition

Recognition of digital documents is often described in terms of a metaphor around of an envelope.

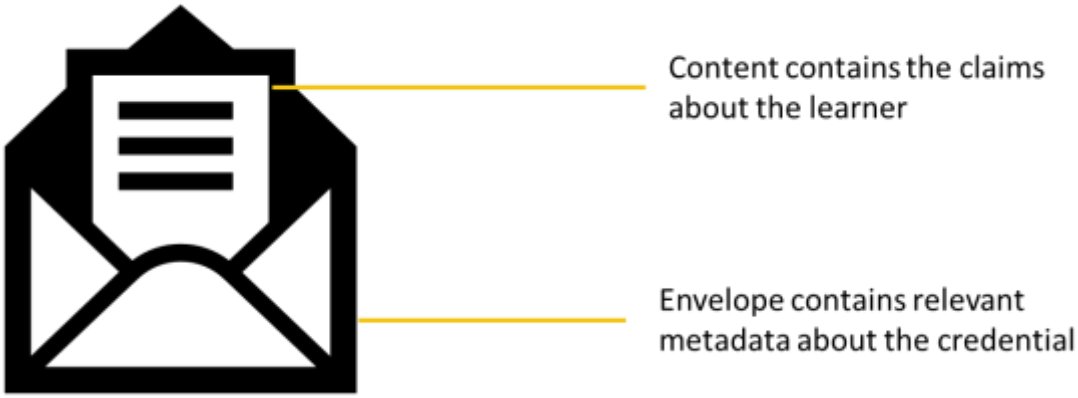


Figure 3: Envelope and Content of a Digital Document

When a digital document is created the 'content' of that document is encoded in a digital format, according to a content standard that is specific to that domain such as a template for a learning agreement or a template for a credential. That content is in turn sealed in an envelope which (a) secures the document, (b) provides information about the content inside, and (c) indicates who issued the credential. The envelope tends to be the domain of a different set of standards covering e-signatures, time-stamping, verifiable claims and attestations etc.

Delivering an envelope from one party to another requires a postal system. Similarly, delivering a digital document from one party to another requires a mechanism to transport the envelope and the content between computer systems. This is the realm of a third set of standards for communication between systems, and may include standards such as e-mail, DID interchange formats, REST APIs etc.

While with educational policy, 'recognition' typically applies to the recognition of learning, such as in the recognition of study periods abroad, that recognition cannot take place if the content cannot be received, read and verified by a verifier. Therefore, within digital systems recognition includes:

- the ability of a verifier to receive a digital document via a network, according to a commonly agreed format with the issuer/sharer;
- the verification of the authenticity of the document either by reference against a registry, or by verifying a digital signature;
- the processing of the content of the document according to the formats and schemas laid out by a data standard/model;
- the resulting status 'educational recognition' that is conferred upon the contents or holder of a credential as a result of that processing

In this study, 'digital credential recognition' is understood in the comprehensive sense, encompassing all of the above steps.

CHAPTER 2

2 Global Standards for Digital Credentials

2.1 European Learning Model

The European Learning Model standard is designed to provide a single format to describe certificates of attendance, degrees and diploma supplements, employer recommendations and any other kind of claims that are related to learning. Consequently, the widening use of this data model can help education and training providers to offer more meaningful descriptions of their learning opportunities and issue data-rich machine-readable credentials to their (prospective) learners. At the same time, the widespread use of the standard can also support **employers and job seekers** to communicate effectively, and better match knowledge and skill supply with demand on the labour market.

More specifically, as illustrated by the figure below, the European Learning Model – and digital credentials that use this data model to provide information about a person's learning – can describe claims related to:

- **Activities** (e.g., participation in classes and non-formal learning events),
- **Achievements**, including **qualifications** (e.g., professional certificates, university diplomas and other learning achievements),
- **Assessments** (e.g., examination results and transcripts of records), and
- **Entitlements** (e.g., right to enroll in learning opportunities, or to undertake an occupation)

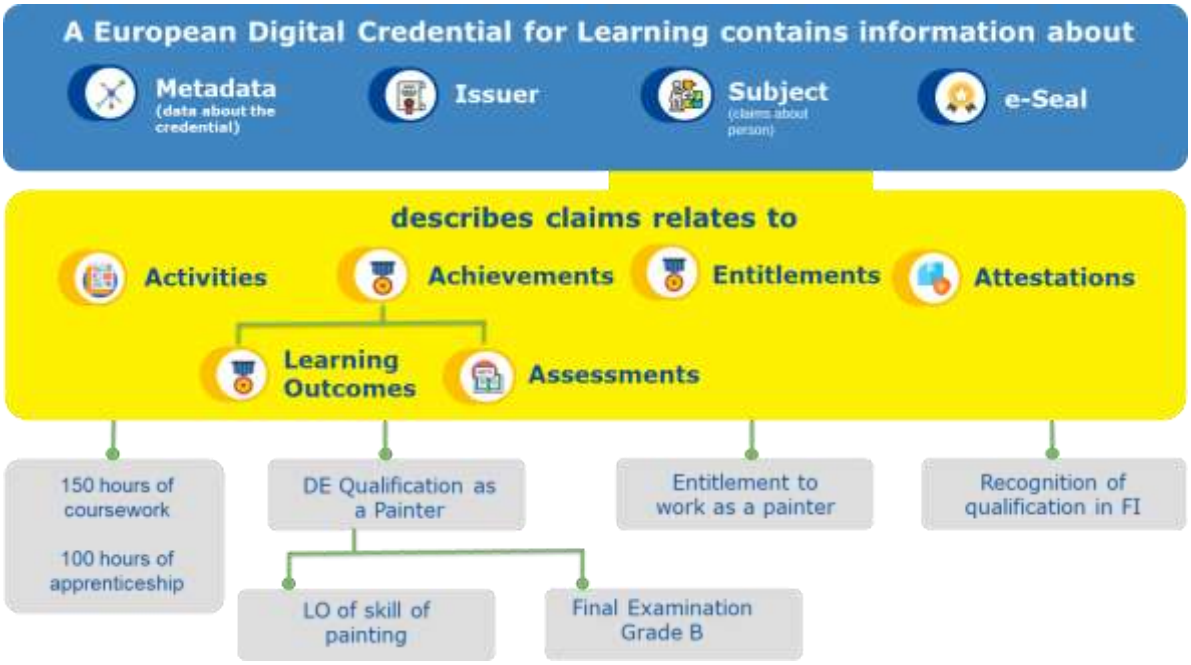


Figure 4: Explanation of the types of claims that can be expressed by European Digital Credentials for Learning

The initial development stage (between February 2019 and July 2020) involved a wide range of stakeholder representatives from 18 European countries[1]. Their invaluable support and feedback helped shape the Europass Learning Model into its current state and allowed the early versions of the credential 'Issuer' and 'Viewer' tools to capture and display credential content that resembled the look and feel of their original counterparts, while at the same time serving the precise needs and requirements of real digital credential implementers.

[1] Austria, Croatia, Cyprus, Czech Republic, Estonia, France, Germany, Greece, Italy, Luxembourg, Malta, Norway, Portugal, Romania, Slovakia, Slovenia, Spain, The Netherlands

Since the launch of the public preview of the EDCI in July 2020, the list of early adopters has been gradually growing with the involvement of vendors (c.a. 60) and university alliances, increasing the impact, potential and the appeal of the EDC initiative.

While European Digital Credentials for Learning describe **concrete** facts and details about a person's learning, the European Learning Model also allows the description of **prospective** learning, or learning opportunities, and a highly **conceptual** description of learning, that we call "specifications". The above-mentioned claims, i.e., achievements, activities, assessments, and entitlements, are all building on learning opportunities, and have their corresponding specifications as shown on Figure 5. By this design, specifications can help scaffold learning opportunities (that can also be described by specifications) and connect them with personalised credentials.

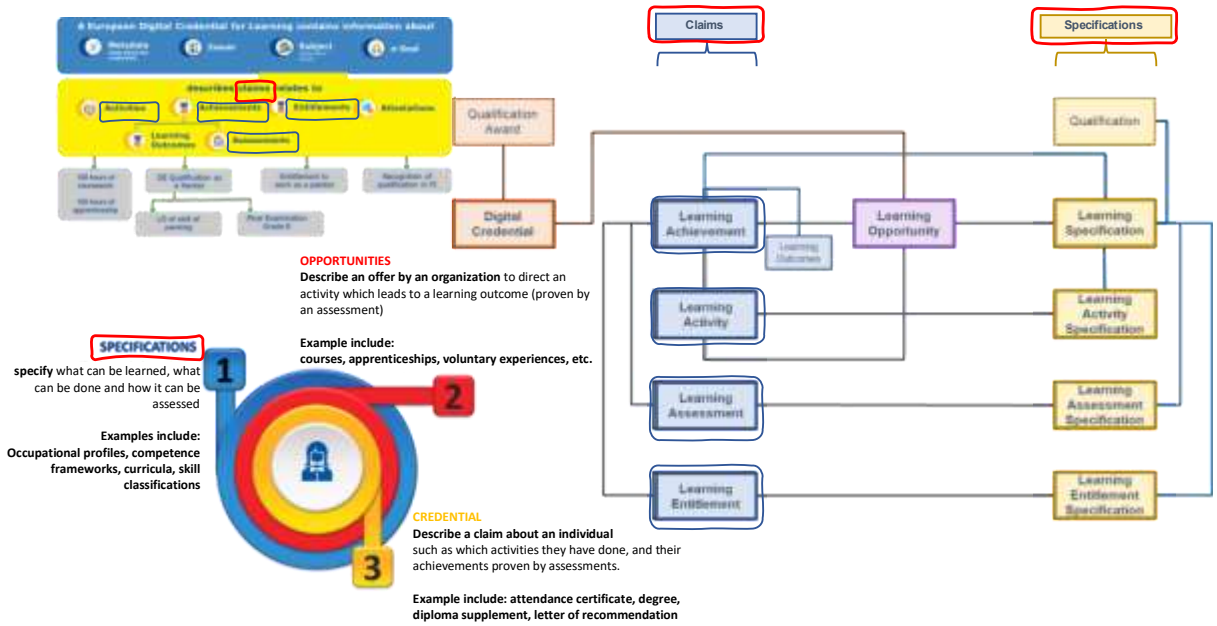


Figure 5: Depiction of the European Learning Model and its relationship with learning opportunities and credentials

The European Learning Model is an extension of the W3C Verifiable Credentials data model, and integrates widely known and used open standards, including

- ESCO to identify and describe knowledge, skills, qualifications and occupations,
- ISCED-F to reference thematic areas related to learning opportunities and credentials and
- qualification frameworks used across Europe, such as the EQF and 43 NQFs.

The European Learning Model is also aligned with the EMREX initiative mentioned in chapter 2.2.

2.2 ELMO

The Emrex User Group (EUG) is an **independent, international network** which unites various actors, including universities, public institutions and national consortia, that are interested in **enhancing student data portability**. As such, the network acts as a global platform for connecting expertise, sharing knowledge and enhancing collaboration to expand the EMREX footprint and help unlock the full potential of student data and open up data flows globally. The purpose of EMREX, with its electronic data exchange solution, is to empower individuals to control their own student data and exchange throughout their lifespan, across borders for various purposes.

```
<xs:element name="elmo">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="generatedDate" type="xs:dateTime">
                <xs:annotation>
                    <xs:documentation>The datetime when the file was generated. It SHOULD contain the timezone
                        suffix. Example values: &quot;2015-08-01T12:00:00+02:00&quot;, &quot;2015-08-01T10:00:00Z&quot;.
                    </xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="learner">
                <xs:annotation>
                    <xs:documentation>This describes the student whose achievements we will be describing. One EMREX
                        ELMO element may contain multiple reports, but all of the reports are always
                        describing exactly one student.
                    </xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="citizenship" type="europass:countryCode">
                            <xs:annotation>
                                <xs:documentation>The ISO 3166-1-alpha-2 code of the country the student is a citizen of.
                                    E.g. &quot;PL&quot;.

                                    For server implementers: If this is not known then you MUST skip the element
                                    altogether (instead of, for example, providing an empty value).
                                </xs:documentation>
                            </xs:annotation>
                        </xs:element>
                        <xs:element maxOccurs="unbounded" minOccurs="0" name="identifier">
                            <xs:annotation>
                                <xs:documentation>For server implementers: Please read thought the list of predefined identifier
                                    types below and try to provide all of those you can get. We are aware that
                                    some of those will be difficult to get (especially for the foreign students).

                                    For client implementers: If a given identifier is present you can use
                                    it for any purpose you want. However, you should expect them to be NOT present
```

Figure 6 Sample code from the elmo schema.xsd

The EMREX XML format is used for formatting students' Transcripts of Records. Most of the elements described in the schema are marked as optional (this is solely to support some uncommon edge cases), but they are strongly recommended.

The EMREX ELMO format is loosely based on the "ELMO" schema used in various sources under the namespace of "http://purl.org/net/elmo". However, the original ELMO XSD schema seems to be unsupported by its authors and the EMREX ELMO format is no longer compatible with those XSDs.

2.3 The Comprehensive Learner Record (CLR)

The IMS Global Comprehensive Learner Record Standard (CLR) is a technical specification designed to support traditional academic programs, co-curricular and competency-based education as well as employer-based learning and development—in any domain where it's important to capture and communicate a learner's and worker's achievements in verifiable, digital form. Designed to be used, curated, and controlled by the learner, the IMS CLR is a modern and web-friendly interoperable learner record structured for easy understanding yet flexible enough to support a wide range of use cases to meet the needs of learners and workers, registrars and employers.

The CLR Standard is part of IMS's digital credentials portfolio of standards that also includes Competencies and Academic Standards Exchange (CASE®) and it leverages the Open Badges standard and is compatible with the W3C Verifiable Credentials and the Credential Engine Registry. CLR has onboard verifiability, but for an added degree of permanence, implementers may choose to authenticate ownership with a blockchain solution.

The CLR standard is recommended by AACRAO, the American Association of Collegiate Registrars and Admissions Officers. The CLR v1 is a specification launched in 2020 and the following products are already IMS CLR certified: AEFIS v3.66, ELocker & Gradintelligence, Open Credential Publisher, SmartResume and Territorium

2.4 Open Badges

Open Badges labels itself as the world's leading format for digital badges. Open Badges is not a specific product or platform, but a type of digital badge that is verifiable, portable, and packed with information about skills and achievements. Open Badges can be issued, earned, and managed by using a certified Open Badges platform. The Open Badges specification is a free and open specification available for adoption.

The IMS Open Badges specification describes a method *for packaging information* about accomplishments and recognition embedding it into *portable image files* as digital badges and establishing *resources for its validation and verification*. The current stable and latest version is 2.0, which was released in October, 2018.

The specification indicates a set of use cases which represent the badges full-life cycle as it is presented in the next figure:

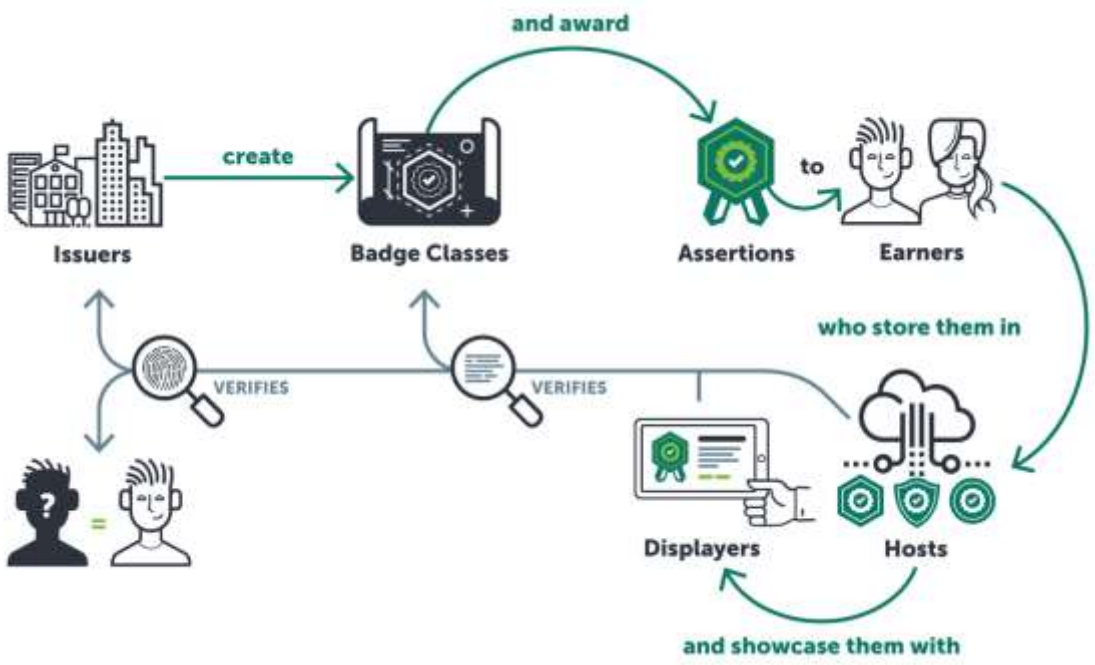


Figure 7: Open Badge full life cycle according to the Open Badge spec (IMS Global, 2018).

1. Creating a BadgeClass: Organization acting as Issuers can create BadgeClass objects to build a catalogue of badges that may be available to earn from the issuer. Those Badge classes may include information about the achievement including how to earn it or learn more about the issuer and achievement itself.
2. Organizations can Issue badge Assertions to recipients: With a catalogue of badges (BadgeClasses) prepared, organizations can issue those badges to recipients by creating Assertion objects. The Assertion is the representation of an awarded badge and may include evidence and supporting information on how the recipient became eligible for it.
3. Earners will be able to store their awarded badges in Badge hosts, which will implement main features for importing (see 5 below) and displaying Open badges.
4. Displaying Open Badges: Typically, when an Open Badge is displayed, the Assertion and related objects are displayed on a screen in human-readable format. Supporting this enables the recipient to showcase their earned achievements and choose to allow others to view those.
5. Importing Open Badges: Badge Hosts must support the function of importing Open Badges. This involves a process by which an Assertion and related objects are validated for format and integrity. Import of Open Badge data normally results in the subsequent display of that data.

IMS Open Badges supports the process of badges sharing or exchanging using the following technologies:

- Download baked badge image file: Badge Baking is the process of taking an Assertion and embedding it into the badge image, so that when a user displays a badge on a page, software that is Open Badges-aware can automatically extract that Assertion data and perform the checks necessary to see if a person legitimately earned the badge. The BadgeClass (IMS Global) image must be in either PNG or SVG format to support baking.
- Social media integrations.
- Copy URL to JSON assertion.
- Retrieve HTML to display the badge.

The following products are IMS Open Badges certified Acclaim by Credly, Accredible v.1.27.0, AEFIS, Badgr v3 by Concentric Sky, Hyland Credentials v1.0, Moodle v3.10 and 3.11.

CHAPTER 3

CHAPTER 3

3 Applications of Digital Credential Recognition

The standards described in the previous chapter form the foundational basis for the development of concrete applications across multiple use cases. These are described in next chapters.

3.1 Management of Student Mobility

Study mobility between Higher Education Institutions entails a whole set of processes that facilitate such mobility. Oftentimes in this process communication is needed between the sending (or home) HEI and the receiving (or host) HEI. In general, one can describe the mobility flow as follows (sometimes steps are repeated/ordered somewhat differently):

1. Sending HEI nominates the student at the receiving HEI;
2. Learning agreement needs to be worked out and signed by three parties (student, sending HEI, receiving HEI) before departure;
3. Student arrives at the receiving HEI and upon receiving HEI needs to confirm the date of arrival;
4. Learning agreement might change. If so, it needs to be signed by three parties (student, sending HEI, receiving HEI);
5. Student departs from the receiving HEI and upon receiving HEI needs to confirm the date of departure;
6. Receiving HEI sends Transcript of Records to sending HEI

3.1.1 Erasmus Without Paper

The Erasmus Without Paper (EWP) initiative uses the latest digital technology to pave the way to manage mobilities more efficiently. This allows Higher Education Institutions to exchange information in the context of student mobility swiftly and securely. In doing so EWP supports replacing paper-based workflows by digital ones.

EWP consists of two chief components:

- The Erasmus Without Paper Network that interconnects a multitude of student information systems (whether individual universities or third-party providers which represent multiple institutions) using APIs (i.e., connectors between the Network and the users)
- The Erasmus Dashboard that provides a web solution for exchanging student data electronically for HEIs lacking the required SIS software.

It is the technological framework that is being used to form the European Student Card Initiative, which in the period from 2021-2028 will be used to manage all Erasmus student mobilities in Europe – nearly 1 million student mobilities per year.

The main principle behind EWP is that an institution keeps using your existing system for managing student mobility and that this system is connected to the EWP network. Instead of printing a PDF or a paper copy of e.g., an Inter-Institutional agreement or a Learning Agreement, a student is able to sign the "documents online" and send them directly via a software system to your partner institution which will also digitally sign them.

The network allows different ways of connecting:

- for institutions that use commercial mobility software which has been developed for various national markets in Europe, connectors to the network are provided;
- for institutions that have developed their own mobility software, a set of APIs are provided that allow them to build their own connections to the network;
- for institutions that do not have their own mobility software, a new system known as the Erasmus Dashboard is provided

The Erasmus Dashboard is used by nearly 3000 institutions in Europe to manage their mobilities. It is a free-to-use tool providing institutions with the basic functionality needed to manage the mobility processes of Erasmus+. and lets you manage the Online Learning Agreements.

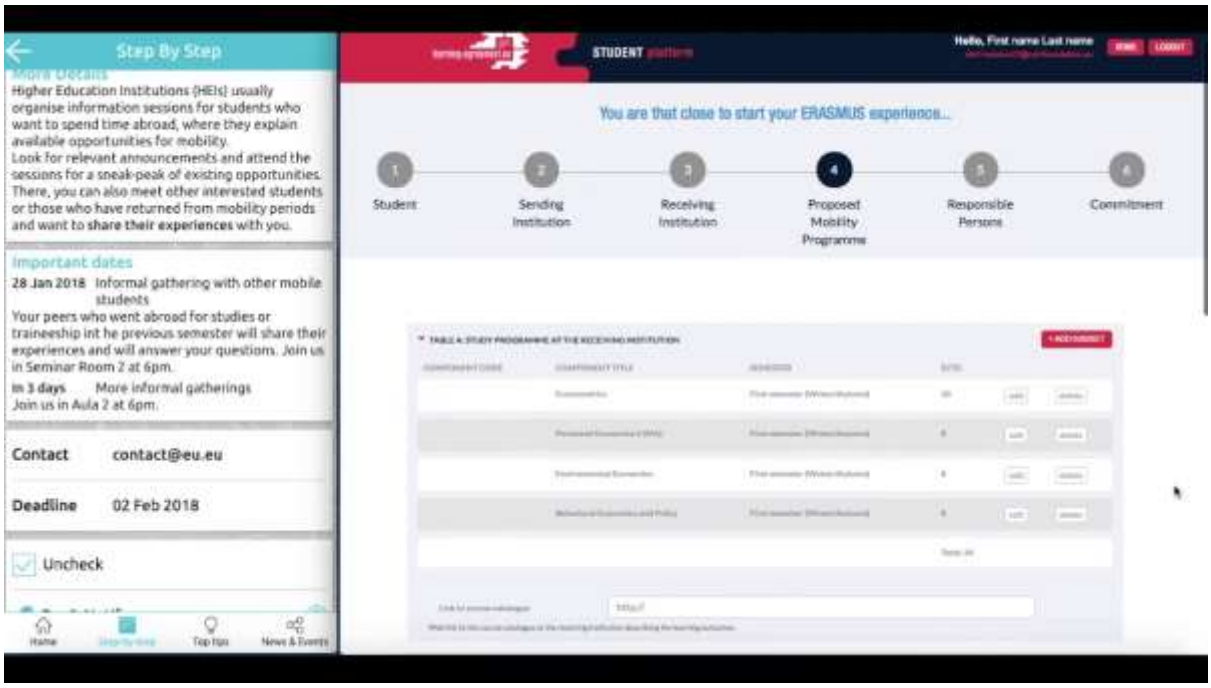


Figure 8: Screenshot of the Erasmus Dashboard

It consists of components handling:

- Online Learning agreement (OLA): the online tool for creating, negotiating and updating learning agreements in a machine-readable format;
- Inter-Institutional Agreement Manager: a tool that allows creating, negotiating and updating Inter-Institutional Agreements in a machine-readable format

It also connects to the European Commission's Erasmus+ Mobile App, allowing one to communicate with the incoming and outgoing students directly via the App.

These services have recently been consolidated into the European Digital Student Service Infrastructure.

3.2 Digital Credentialling

There are tens of providers globally that provide digital credentials services. This chapter outlines some of the more significant initiatives based on the level of maturity of their technology, market recognition, adoption and ability to meet use cases. The section is complemented by a description of further private credentialling providers included in Annex 2.

3.2.1 Digital Credentials Consortium

The Digital Credentials Consortium (DCC) was founded in 2018 by a group of leading universities with expertise in the design of verifiable digital credentials: Delft University of Technology (NL), Georgia Institute of Technology, Harvard University (USA), Hasso Plattner Institute, University of Potsdam (Germany); Massachusetts Institute of Technology, McMaster University (Canada), Tecnologico de Monterrey (Mexico), TU Munich (Germany), UC Berkeley (USA), UC Irvine (USA), University of Milano-Bicocca(Italy), University of Toronto (Canada).

The DCC is designing an infrastructure for digital credentials of academic achievements which is expected to become a standard for issuing, storing, displaying, and verifying digital academic credentials. It focuses on a stronger privacy-by-design and privacy-by-default with attention to regional legal frameworks such as the GDPR. In addition, it provides more reliable revocation mechanisms and credential lifecycle management, more direct learner's ownership over his lifelong learning record and a higher level of consistency between the machine-readable data of a credential, its human-readable visual representation, and its necessary output formats—paper or digital.

DCC work is primarily concerned with use-cases in higher education, but this work can be taken as a broader effort to bridge post-secondary and lifelong learning, connecting traditional institutions of higher education, non-formal education providers, as well as the workplace, through interoperable standards. There is a collaboration with technology companies, online learning platforms and IT vendors to create a vital ecosystem of options to choose from. Furthermore, they also expect to liaise with employers to integrate verification services into their hiring workflows.

This effort is entirely driven by institutions committed to open source and open standards and they are actively working with standards groups to complement existing efforts.

3.2.2 Europass and European Digital Credentials for Learning

Europass is one of the 12 flagship actions of the European Skills Agenda adopted by the European Commission on 1 July 2020. With the launch of the new Europass platform the Commission has taken a significant step in delivering on the ambition of the Skills Agenda and making lifelong learning a reality for all.

The new Europass offers a range of **online 'e-Portfolio' tools and information** for people of all ages, at all stages of their lives, to manage their learning and career such as:

- a personal profile for people to record all their skills, qualifications and experiences,
- tailored suggestions of jobs and courses for Europass users based on their interests and skills,
- updated tools for creating CVs and cover letters and
- information on learning and working in Europe.

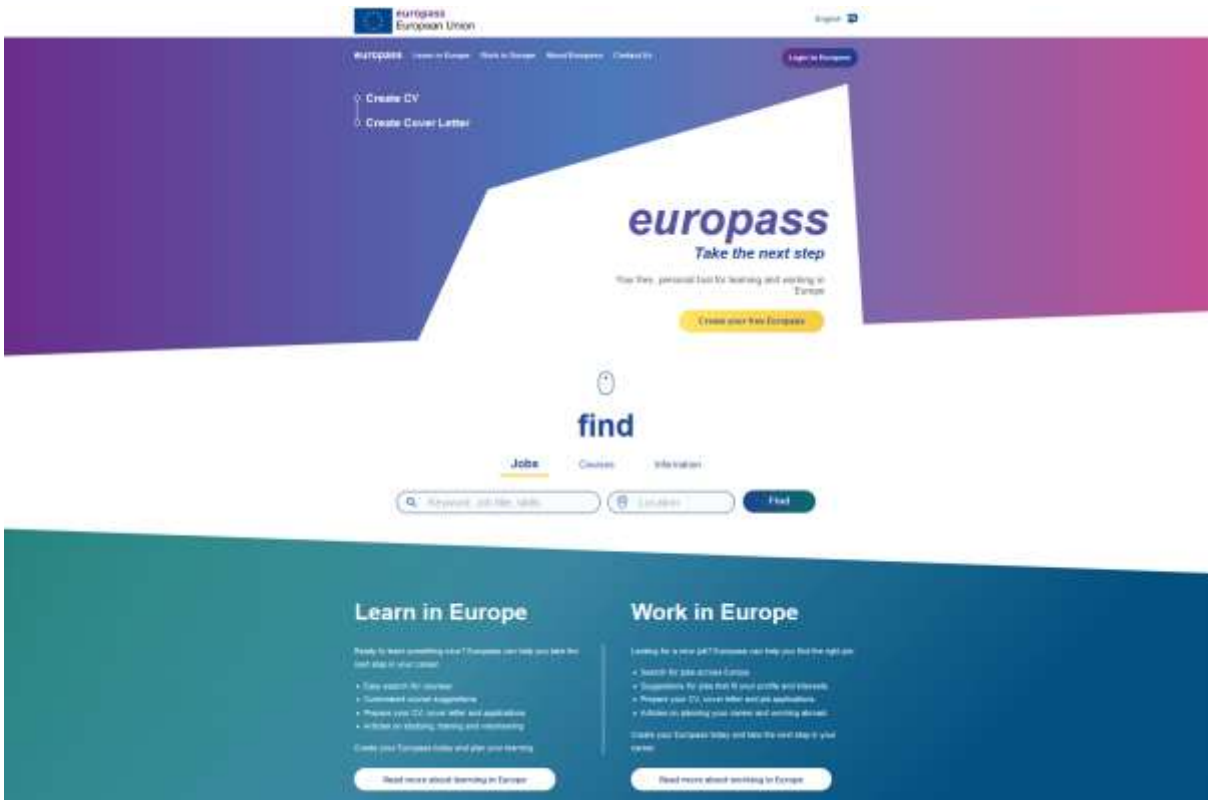


Figure 9 Europass portal's homepage

As part of the new Europass, the Commission has also developed tools and mechanisms to allow the issuing, storage and sharing of Europass Digital Credentials, which are **authentic, tamper-evident digital credentials** (e.g. qualifications, diplomas, certificates) that can support 'paperless' processes and easier recognition and understanding of qualifications across the EU.

The ambition of offering citizens course and job recommendations that are truly aligned with their goals, as well as their prior knowledge, experiences and current country of residence, can only be realised through using a multilingual platform and open (global) standards.

Europass Digital Credentials (EDCs) for Learning are electronically sealed digital records given to a person to certify the learning they have undertaken. They can be awarded for formal education, training, online courses, volunteering experiences and more. The European Commission has developed the Europass Digital Credentials Infrastructure (EDCI), launched in November 2021, as a component of the new Europass platform to support efficiency and security in how credentials such as qualifications and other learning achievements can be issued and recognised across Europe. At the time of writing this report there are over 2.5 million Europass wallets registered and ready to receive and store EDC format compliant digitally-signed credentials.

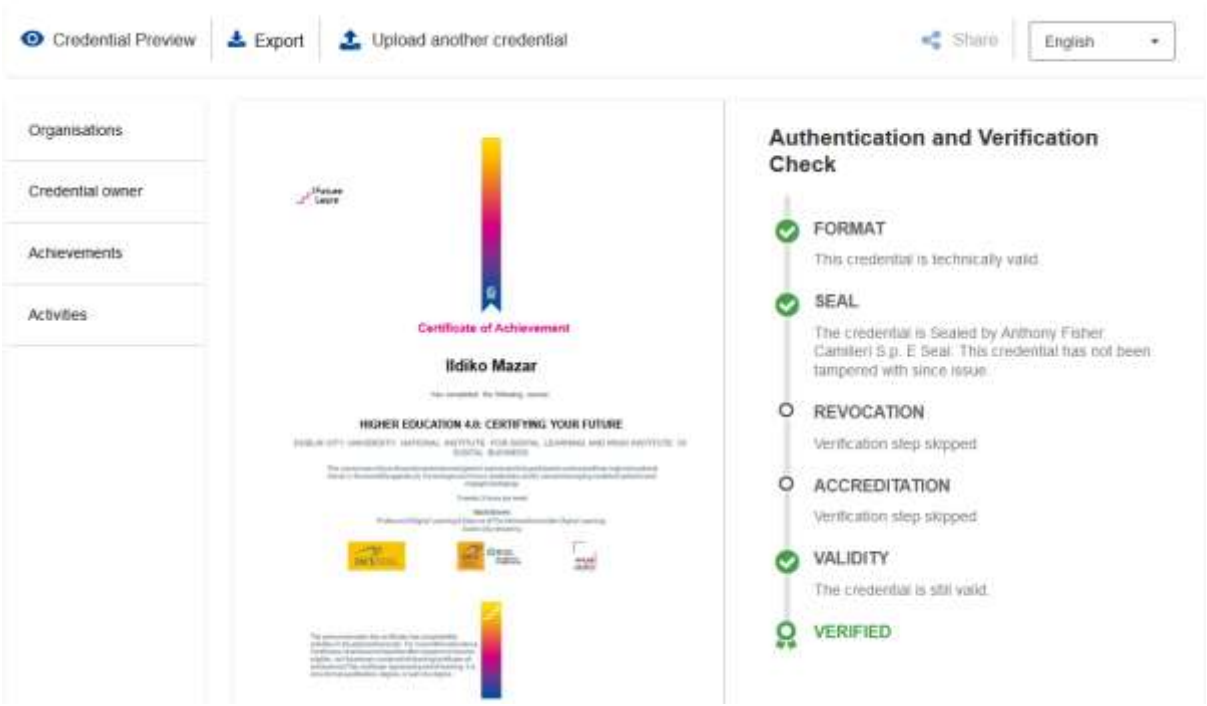


Figure 10 : Data content and verification checks of a sample Europass Digital Credential visualised in the EDC Viewer

3.3 Transfer of Credentials between institutions

3.3.1 EMREX

EMREX is both a network of institutions and a system of transfer of credentials between those institutions. The network is made up on nine national credentialling services or universities in Europe, that have interconnected their systems for the purposes of transferring these documents between themselves. It includes members from Norway, Finland, Sweden, Denmark, Italy, Germany, Netherlands, Belgium, Denmark, Spain, UK and Croatia.

Each country has two roles in the EMREX network:

1. providing students with application(s) that allow them to fetch their result from another HEI, either in the same country or from abroad.
2. Provide national client(s) with functionality to fetch assessments (results from courses, qualification) from the databases containing this information.

Because EMREX is a decentralised system, there is no major component that each country can reuse. The EMREX project does provide some modules, plugins and examples that can be used and built upon, however there are a couple of issues that cannot be solved in a general way:

1. **Authenticating a student**: Each country has their own way of authenticating a student in their system. In Norway there are Feide and ID-Porten, Finland has Haka, Sweden has Swamid and so on. Therefore, the EMREX project cannot make a complete login module and distribute this, as each country solves this in different ways.

2. **Fetching results for a student**: Each country/HEI has their own student information systems. Some countries have national data sources that can provide this information. Therefore, there is not one unified way of fetching results from these systems. The EMREX-system is dependent on connecting to an existing solution that can fetch results for a given HEI. The preferred solution is to build a REST service for each student information system involved, that provides ELMO formatted data.
3. **Storing results for a student**: Each country/HEI has their own student information systems. So, there is no standard way of storing the result data the EMREX fetches into the existing student system. When the EMREX clie0nt returns a set of results for a student, these must be stored in some local system, as EMREX does not store the data in itself.

The EMREX code is open source and can be downloaded from the EMREX GitHub account.

CHAPTER 4

4 Digital Credential Recognition in the ASEAN+3 region

4.1 National or Regional Digital Credentials Initiatives

5.1.1. RECSIE, Japan

RECSIE (Research Consortium for the Sustainable Promotion of International Education) was established in January 2014 as a non-profit organization in Japan aiming to make contributions to the internationalization of Higher Education Institution (HEI), and promoting a research agenda on HEI internationalization that goes beyond the borders of any individual universities. The core objective of RECSIE is to collaborate with universities around the world for enhanced student mobility and to nurture the global talent of students through cultural diversity. RECSIE joined the Groningen Declaration Network in early 2020 as the first member from Japan. Starting its research on international digital credential platforms by late 2019, RECSIE has taken up the digitalization initiative for Japan's higher education community and launched its partnership with Digitary to build the Japanese National Network on September 2020. The Japanese National Network is the first of its kind, being a national online platform as well as a national credential wallet for students of Japan's post-secondary education. The network itself is under continuous improvement and is planned to offer six important benefits related to academic credentials, including:

1. Language support in both Japanese and English.
2. An around-the-clock service allowing students to access the Network at any time of the day, any place, and any device.
3. Secure access to view and share official documents in digital format including transcripts and credentials.
4. A platform to increase productivity and efficient services of higher education institutions in Japan, while enabling them to preserve the independence and brand value of their digital documents.
5. Automatization of student records as well as the exchange of documents both nationally and internationally through a secure and trusted network.
6. The opportunity for Japanese higher education institutions to advance into a post COVID-19 model through more efficient utilization of academic record portfolios, micro credentials, Massive Open Online Courses (MOOC) and many more.

RECSIE is welcoming more universities to participate in this partnership, following Shibaura Institute of Technology, International Christian University, Nanzan University, and Toyo University as its current four leading universities. The National Network is believed to have a strong impact on the realization of UNESCO's Tokyo Convention which promotes the mobility of students and talents in the Asia Pacific region.

5.1.2. ICE-Institute, Indonesia

The adoption of digital credentialing is just about to emerge in Indonesia, starting with the rapid development of online learning in the country. By 2014, Indonesia had begun promoting online learning through Indonesian MOOCs (Massive Open Online Courses) called SPADA Indonesia, which is the Indonesian Online Learning System established by the government. The government's initiative was soon followed by private sector initiatives such as Indonesia-X and HarukaEDU.

These private online learning platforms offer free courses with fees for accessing the exams and also obtaining certificates. Online courses are also offered by foreign HEIs providing virtual courses in Indonesia. Thus, it becomes increasingly important to provide routines and systems that can ensure that the online education being implemented meet the specified quality standards.

Indonesian HEIs are further encouraged to boost online courses by the national policies Regulation No. 51/2018 and No. 7/2020. Regulation No. 7/ 2020 enables online education to exist with the transfer of credentials among HEIs in the country. This national policy also introduces a new framework for quality assurance to cover not only accreditation in institutions and/or study programs in the conventional and distance education settings, but also accreditation in courses and blocks in an online or unbundled university setting. ICE (Indonesian Cyber Education) Institute was created as part of the scheme to ensure quality of online education regardless of level (institution, study program, course, or block).

ICE is a national center for quality assurance of online education in Indonesia which was officially launched in July 2021. The main function of the ICE-Institute is to facilitate quality assurance of online education in Indonesia, specifically the registration of e-learning courses from Indonesian universities, as well as online courses from international universities and global MOOC platforms. A course which has passed the quality assessment done by the ICE-Institute will be given a registration number which is unique for each institution, study program and course. The assessed and registered course will then be uploaded in ICE-Institute's marketplace where it will be delivered online in Indonesia and also transferred to HEIs across countries. The unique registration number it owns shows the institution, study program, and course's quality and legal status as assessed by ICE-Institute. This quality assessment is done not just for HEIs within the country but also international HEIs offering their services in Indonesia. At the moment, there are 13 Indonesian universities, two global MOOCs (edX and RELO), one professional association, (AFEBI) and a job hiring platform (Kalibrr) which have joined ICE-Institute. ICE-Institute currently uses private blockchain services for digital credentials, specifically from Accredible. The utilization of digital credentials by ICE-Institute open possibilities for wider adoption of digital credentials in the country.

5.1.3. OpenCerts, Singapore

OpenCerts is an initiative of digital credentialing in Singapore which was jointly developed by SkillsFuture Singapore (SSG), Government Technology Agency (GovTech), Ngee Ann Polytechnic (NP), and Singapore's Ministry of Education (MOE) in 2018. This blockchain-based platform powered by Ethereum enables secure and reliable digital certificate issuance and verification. OpenCerts utilizes a decentralised ledger which ensures that each digital certificate on its platform is equipped with a unique cryptography code. Through the use of this distinct code, forgery and other forms of fraud, such as tampering, could be detected easily. There are three key elements of OpenCerts which are the open source scheme for educational credential publication, the set of tools used to generate cryptographic

codes for the protection of credentials, and the OpenCerts website itself which is the platform used to verify the authenticity of OpenCerts files.

Currently, there are 18 institutions in the OpenCerts registry maintained by SSG, including Nanyang Technological University (NTU) and National University of Singapore (NUS). Certificates issued by institutions under the SSG registry can be viewed on a wallet called Skills Passport. Digital certificates for N, O and A Levels; ITE qualifications; diploma and degree qualifications from polytechnic institutes, LASALLE College of the Arts, Nanyang Academy of Fine Arts, autonomous universities, and the National Institute of Early Childhood Development; as well as from the Singapore Workforce Skills Qualifications (WSQ) are being uploaded into the Skills Passport. Skills Passport serves as a single digital repository for education and training certificates which allows employers to easily identify the qualifications of employees and job candidates. This online wallet helps to highlight individuals' skills, developed during their educational journey or through other life experiences. On the other hand, the Skills Passport could also be used to discover the skill area of an individual which needs further improvement as it becomes apparent when their achieved skills are spotlighted in one repository. Through these benefits, users can then make further decisions and plan their next steps accordingly.

4.2 Digital Credentials Issuing and Recognition in ASEAN HEIs

As an effort to elaborate the status of digital credentials issuing and recognition in ASEAN HEIs, the SHARE Programme held a Focus Group Discussion (FGD) on Digital Credit Transfer Systems, attended by over 50 representatives from SHARE partner universities across the ASEAN region on August 12, 2021. The results of this FGD are expected to provide general figure about digital credentialing development in the region.

It appears that most HEIs in ASEAN are not yet issuing digital credentials as the majority of the FGD participants stated that their institutions do not have a digital credential system. Most of these institutions still utilised PDF versions of credentials or at the most provided credentials that can be checked in the institution's website. However, in terms of digital systems of credit transfer these institutions mentioned several credit transfer platforms which they have utilised and which they believe to be digital systems for credit transfer, including the SHARE AECTS platform, the AUN credit transfer, UMAP credit transfer, and the Erasmus+ credit transfer. Nevertheless, paper-based documents or digital documents in the form of PDFs are still utilised for the digital credit transfers, with institutions citing challenges such as difficulties in transferring university stamps or e-signatures into a digital system.

The existence of national regional/ national policies or projects on digitisation which are relevant to credentialing should encourage the development of digital credentials in ASEAN HEIs. Increasing amounts of online learning as well as digital credentialing is supported by Government Regulation No. 7/2020 in Indonesia. Following this regulation, a blockchain based-digital credential powered by Accredible was introduced by ICE-Institute in Indonesia to enable the transfer of credentials among HEIs in the country. The National Public Key Infrastructure in the Philippines has been initiated, but is still pending the development of applications for a digital wallet system to support it. Policies and funding from the government to develop digitisation have been initiated in Vietnam, but institutions are still in the process of adopting true digitisation. Institutions in Malaysia and Thailand have had some experience with digital credentials, with some private universities in Malaysia utilising digital badges or micro-credentials, supported by a government regulation on micro-credentials.

In other countries including Cambodia, Myanmar, and Laos, policies on digital credentials have yet to be developed.

Although the status of digital credentialing is diverse among the ASEAN HEIs and seems to lag behind those in Europe and in the US, most of the representatives of SHARE partner universities supported the idea of increased digitisation of credentialing in the region, citing advantages such as increased ease for employers to access learner transcripts, improving the credit transfer process between universities, minimizing bureaucracy, and lowering costs. Nevertheless, some challenges in implementing digital credentials were identified during the FGD. Some of the challenges are related to:

1. **Technological capacities of institutions**, both in infrastructures and human resources to implement such a system.
2. **Security** is another issue, whereby institutions are still hesitant about the possibility of fraudulent digital credentials.
3. **Difficulties in shifting the tradition of utilising paper-based credentials** was also mentioned as one of the challenges, especially since paper-based credentials are still the most widely accepted credentials by universities and employers who are often unaware of digital credentials and do not require this for employment purposes.
4. **Policy issues**, including the lack of government policies and funding for digitisation, with some governments mandating the use of paper-based credentials such as paper transcripts with official university seals.
5. **Different educational standards** among ASEAN HEIs leads to difficulties in a common system implementation for digital credential recognition in the region.

Despite the above-mentioned challenges, the development of a digital credential recognition system is still seen as an important priority, even more so during the current pandemic. In order to ensure the success of a digital credential system, it is imperative to establish a standard information exchange on grading and learning outcomes between institutions. Support from various stakeholders is also indispensable, including government support in terms of relevant policies and funding for digitisation initiatives, institutional willingness to accept a shift to digital credentials, as well as training to support human resources and technological competency. In this regard, the SHARE program can be the bridge to introduce these concepts to ASEAN institutions, including government bodies and employers so that all stakeholders in the process are aware of the need for developing a digital credential system.

CHAPTER 5

5 Success Factors for Digital Credential Recognition

Multiple technologies are used for credentialling globally. These include client-based systems, cloud-based systems, unsigned credentials, systems based on public key infrastructures, decentralised ledgers and more. Each of the systems tend to claim technology-based advantages which give them an edge of the others.

While there is a clear global trend towards more secure systems with a greater emphasis on user identification, the wide variety of implementations globally implies that no technology has a breakout advantage over the others in facilitating adoption.

In all cases, the *accessibility* of the technology rather than the feature set is a major factor in facilitating adoption. Accessibility depends on price, openness of the standards and code, maturity of the software products, ease of use and availability of documentation.

The cases described in this document share most of the following features, providing a transferable template for implementation. Successful systems tend to;

- be governed either by public authorities or by multi-stakeholder groups which are responsible for defining standards across a network, and include the users/clients of those standards as well as experts and software vendors;
- offer a large portion of their code under open-source licenses, as well as offer some degree of openness to access the standards;
- have undergone several years of testing, piloting and initial implementation;
- include a strong element of user self-sovereignty and decentralisation, such as those offered by distributed ledger technologies;
- have very well-developed documentation resources;
- support the connection of multiple applications supporting the same standards to a network, rather than using a single centralised application;
- have an ecosystem of different providers that can support the implementation of creation, transmission or verification of digital documents;
- offer out of the box implementations, as well as the option to create highly customised systems based on the standards;
- implement processes for continual review and improvement of their standards and applications;
- have reached a point of critical mass whereby the size of the user base is enough for the network to become self-sustaining.

Furthermore, several of the most successful digital recognition systems are integrated into wider projects on the digital labour market. For example, the SkillsFuture System in Singapore accepts digital credentials from OpenCerts, while In Europe, Digital Credentials for Learning are integrated into the Europass e-Portfolio system, and use data from the ESCO Skills taxonomies. The ICE in Indonesia is also in the process of implementing such a connection with labour market data with a connection with Kalibrr.

A network effect is the phenomenon by which the value of a network increases with the number of users. The adoption of a product by an additional user can be broken into two effects; an increase in the value to all other users ("total effect") and also the enhancement of other non-users' motivation for using the product ("marginal effect").

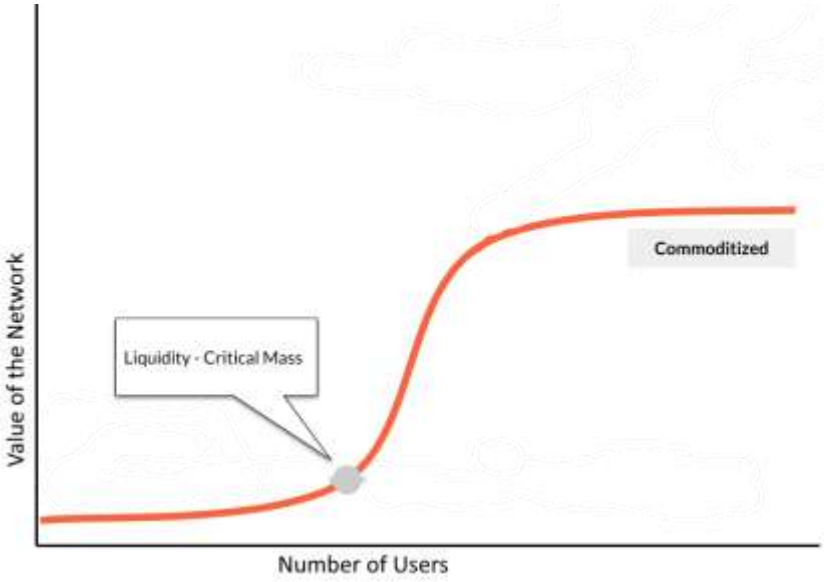


Figure 11: Graph of the Network Effect and Indication of Critical Mass

Within digital credentialling this implies that the value of any solution is **strongly correlated** with its overall interoperability with the market. Establishing a new network has significant risks – as early users will not receive significant value, and may not realise the value at all if the system does not reach critical mass. Thus, early adoption requires significant incentives and support, and needs to have a source of funding that will cover early losses from investment.

Once a system reaches critical mass, the network becomes self-sustaining, and growth tends to go through a spurt phase, before plateauing as the network achieves saturation levels. A typical example of this is the Erasmus Without Paper Network. For over 5 years it was in an early stage, with less than 20 members, and financed through EU-funded research projects. As it reached a critical mass, it quickly added another 3000 institutions in the space of two years, and is set to grow into every higher education institution in Europe within the next 2 years. At this point, the network will reach saturation levels and further growth will not be possible.

The difficulty and investment required for a network to reach critical mass, indicates that establishing a new network for digital credential recognition should be a last-case scenario, if no other options are available. Our overview of digital credential recognition in Asian countries seem to indicate no process-level divergences from global norms in mobility and credential award. Thus, success is more easily achieved by joining or extending an existing network of institutions, already collaborating around a set of standards.

CHAPTER 6

6 Conclusions and Recommendations for Digital Credential Recognition

6.1 Develop a Regional, Full-Lifecycle Approach to Digital Credential Recognition.

Our overview of digital credential systems globally indicates that this is a sector that is experiencing both rapid development and rapid growth. Projections indicate that digital credential will become the norm well before the end of the decade. They bring significant advantages to institutions and employers in terms of lower overheads for issuing and recognising credentials, and bring additional advantages to students in terms of added privacy and portability. Given all of this, we believe the time is right for an initiative to develop a regional approach to digital credential recognition encompassing issue, storage, exchange and recognition of digital credentials across the ASEAN region.

Fully realising the potential of credential recognition implies following the full lifecycle of credentials from design through to usage by students later in life. The various processes which are included within this lifecycle involve different actors, administrative procedures and software packages.

Given this, a stepwise approach to implementation is advised. Taking SHARE's specific focus on mobility, we recommend, in order of priority, the implementation of:

- Credit Transfer between institutions, for the regulation of mobility periods;
- Award of credentials to students, in the form of secure digital certificates;
- Transfer of programme credentials between institutions, as part of course enrolments;
- Transfer of credentials to third parties for purposes of employment, immigration etc.

All processes can be realistically implemented in a 3-5 year time period, depending on the desired level of urgency.

6.2 Pursue Alignment with EU Standards for Mobility and Credentialling

While individual initiatives for digital credentialling may exist in certain ASEAN countries (Japan, Indonesia and Singapore in particular), these initiatives are disparate and do not contain an international or mobility element. Taken together, they currently do not add up to a regional approach to digital credentialling. Given this, three options for alignment present themselves:

- Alignment with EU standards and software
- Alignment with US-based standards and software
- Creation of a new regional approach to standards

The existence of the SHARE program, as well as our analysis of the SHARE manual indicates an ongoing alignment of mobility procedures to EU processes and procedures. Given the costs and difficulties implied in creating a specific set of ASEAN standards and software for digital credentialling due to network effects, we recommend complementing the existing SHARE activities with the application of existing EU based technical standards and open sources software packages such as the European Learning Model, Europass infrastructure and EDSSI infrastructure.

6.3 Use Inter-Institutional Agreements to Regulate Recognition in the short-term

The conversations held with stakeholders during this study, as well as an analysis of policy documents, indicates that at present there are no plans at national or trans-national levels for an overarching credential-recognition framework within the ASEAN region. Given this, we recommend using a network of institutional agreements within the framework of an association or a consortium to create a 'credential recognition network'.

Such institutional agreements should be based on a standardised template, which would cover the method of communication, the format of the credentials as well as the rules for making educational recognition decisions. Agreements should not deviate significantly from standard clauses, so as to achieve a goal of open recognition amongst members of the network, with predictable outcomes for students trying to utilise the network.

Critically, any universities acceding to the network must be required to make changes to institutional policies and strategies which would allow for the recognition of the digitally-supplied content, and which reflect the terms of the agreement – avoiding the issue of 'unimplementable' agreements.

The SHARE network of institutions could choose to form such a recognition network through modification of existing inter-institutional agreements by adding some digital specifications.

6.4 Establish a Credential Recognition Centre of Excellence

The majority of institutions and countries in the ASEAN region have not begun digitisation credentialisation processes or are in very early stages of such developments. While digital credential recognition is very much an evolving field, there are also established best practices in selecting, capacity-building for, managing and maintain such systems.

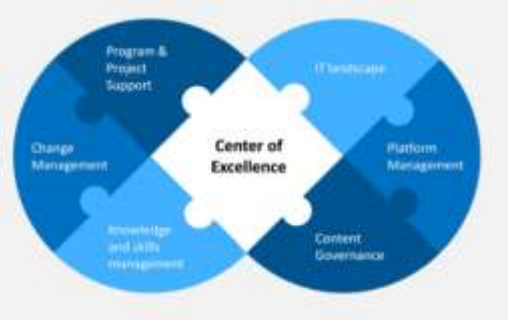


Figure 12: Functions of a Centre of Excellence

To this end, the establishment of a centre of excellence for digital credentialling in ASEAN region, would significantly accelerate implementation of such solutions. Amongst tasks that could be performed by such a centre are:

- Monitoring global developments in global credential recognition and recommending standards and technologies for use in credential recognition across the region;
- Localising products by customising/extending data models and providing for local language versions of products;
- Capacity building of educational organisations and training of key staff on issues linked to credential recognition
- Providing centralised software tools and services which facilitate interoperability between institutions and systems

The implementation of such a system would allow for the dissemination of best practices throughout the region and promote interoperability by reducing fragmentation of approaches. While many institutions globally have taken a journey from paper-based credentials to partially digitised systems, and finally to fully digitised systems, the Centre of Excellence could help institutions jump from paper

straight to fully digitally signed document workflows, in significantly less time, creating a generational change in document management.

6.5 Consider open and self-sovereign data management paradigms

Systems for digital documents around the world are slowly converging around principles for data management and self-sovereignty. In particular, this means that in choosing any system, attention should be paid to:

- Allowing users to hold and control access to their own documents;
- Ensuring that documents are verifiable without extensive dependencies on third parties – implying that systems are secured via systems for digital signature;
- Ensuring documents can always be transferred from one system to another without restriction.

ANNEX 1

Annex 1: Focus Group Discussion on Digital Credit Transfer Systems

As part of the study on "Mapping and Identification of Digital AECTS Needs in ASEAN" the SHARE Programme held a Focus Group Discussion (FGD) on Digital Credit Transfer Systems on August 12, 2021, attended by over 50 representatives from SHARE partner universities across the ASEAN region. Mapping and identification on digital credentialing implementation in the participant's respective countries and institutions were conducted through an in-depth discussion and interactive poll.

In-depth Discussion

In-depth discussion about the implementation of digital credentials in the participants' respective countries and institutions was held in three breakout rooms. The following five questions were addressed in the breakout rooms:

Question 1: Do institutions in ASEAN already issue 'true' (diploma-style) digital credentials? If so, what standards and technologies are used?

In all three breakout rooms, the majority of participants shared that their institutions do not have a digital credential system. Most of these institutions only utilised PDF versions of credentials or, at the most, provided credentials that can be checked in the institution's website. They also cited barriers such as unreadiness in terms of the technological infrastructure to implement digital credentials.

Question 2: Do institutions in ASEAN currently use any digital systems for credit transfer between institutions?

In terms of digital systems of credit transfer, the institutions mentioned several credit transfer platforms which they have utilised and which they believe to be digital systems for credit transfer, including the SHARE AECTS platform, the AUN credit transfer, UMAP credit transfer, and the Erasmus+ credit transfer. However, the majority of institutions are still utilising paper-based documents or digital documents in the form of PDFs for credit transfer, citing challenges such as difficulties in transferring university stamps or e-signatures into a digital system.

Question 3: Are there any regional/national policies or projects on digitisation which are relevant to credentialling?

The responses from the three breakout rooms were very diverse on this issue. In some countries such as the Philippines and Indonesia, there have been national policies that support digitisation of credentials. This includes the National Public Key Infrastructure in the Philippines which has been initiated, but still pending the development of applications or a digital wallet system to support it. In Indonesia, the government has created regulations on digital credentials, but they are not yet implemented by all institutions. Vietnam has had a similar experience whereby there have been developments of policies and funding from the government to do digitisation, but institutions are still in the process of adopting true digitisation. On the other hand, institutions in Malaysia and Thailand have had some experience with digital credentials, with some private universities in Malaysia utilising digital badges or micro-credentials, supported by a government regulation on micro-credentials. Whereas in other countries including Cambodia, Myanmar, and Laos, policies on digital credentials have yet to be developed.

Question 4: Do institutions think there is a need for increased digitisation of credentialling? How important is this compared to other priorities? Do they see this in terms of extra services for students, or extra convenience for the institution?

Many of the participants supported the idea of increased digitisation of credentialling, citing advantages such as increased ease for employers to access learner transcripts, improving the credit transfer process between universities, minimizing the bureaucracy, and lowering costs. However, the participants also cited several concerns in implementing digital credentials, such as the development and maintenance of a digital credential platform, the technological capacities of institutions, the financial support required to develop such a system, as well as ensuring the security of digital credentials. Despite these challenges, the development of a digital credential system is still an important priority, even more so during the current pandemic. In order to ensure the success of a digital credential system, it is imperative to establish a standard information exchange on grading and learning outcomes between institutions. Once developed, a digital credential system can also help support the ASEAN Economic Community, however governmental support is essential as this is a multi-stakeholder process which needs ample preparation and significant investments.

Question 5: What barriers are stopping institutions from adopting digital credentialling?

The participants gave several remarks on why it is difficult for institutions to adopt digital credentialling. Some of the barriers are related to technological challenges, whereby institutions lack the technology and human resources to implement such a system. Security is another issue, whereby institutions are still hesitant about the possibility of fraudulent digital credentials. The participants also mentioned that it is still difficult to overcome the tradition of utilising paper-based credentials, especially since this is still widely accepted by universities and employers, who are often unaware of digital credentials and do not require this for employment purposes. The participants also cited policy issues, including the lack of government policies and funding for digitisation, and with some governments mandating the use of paper-based credentials such as paper transcripts with official university seals. Additionally, as there are different educational standards among ASEAN higher education institutions, it is very difficult to implement a common system for digital credential recognition in the region.

Interactive Poll Results

An interactive online poll was conducted to obtain quantitative information on the level of interest for digitalization of credentials in the participating institutions and the challenges they face in doing so. The results of this poll are presented below:

1. Does your institution already issue 'true' (diploma-style) digital credentials? (39 respondents)
   - Yes : 5%
   - No : 95%
2. Does your institution currently use any digital systems for credit transfer between institutions? (40 respondents)
   - Yes : 5%
   - No : 55%
   - SHARE platform : 30%
   - Other platform : 10%
3. If your institution uses any digital systems for credit transfer between institutions, which processes do you digitize? (38 respondents)
   - Finding an Opportunity : 53%
   - Learning Agreement : 79%
   - Credit Transfer : 61%
   - Diploma Award : 24%
4. Are there any regional/national policies or projects on digitisation which are relevant to credentialing? (33 respondents)
   - Yes : 21%
   - No : 79%
5. Does your institution think there is a need for increased digitization of credentialing? (34 respondents)
   - Yes : 97%
   - No : 3%
6. How important is increasing digitization of credentialing in your institution compared to other priorities? (36 respondents)
   - Low : 8%
   - Mid : 56%
   - High : 36%
7. How does your institution see digitization of credentialing? (31 respondents)
   - It is an extra service for students : 55%
   - It is an extra convenience for the institution : 84%
8. What barriers are stopping your institution from adopting digital credentialing? (36 respondents)
   - Lack of Knowledge/Skills about digital credentialing : (3.61)
   - Lack of Policy Instructions / Standardization : (3.03)
   - Lack of Technical Infrastructure : (2.89)
   - Costs : (2.06)
   - No Demand : (0.64)

ANNEX 2

Annex 2: Actors in Digital Credentialling

This annex introduces some of the most important private digital credentialling companies. The selection is based on existing or emerging market share within the Higher Education segment.

Badgr

Badgr helps organizations to create learning ecosystems to support skills-based digital credentials, stackable learning pathways, and portable learner records. It was founded in 2015, its headquarters are based in Oregon, USA and Microsoft, Starbucks, Mozilla, AI Singapore, SAP, CISCO networking academy, Arizona State University and more than 2400 organizations spanning 160 countries compose the Badgr client base.

Badgr allows LMS integration, as Blackboard or Canvas and helps to create skill-based credential systems that organize user's learning experiences by building stackable credential pathways that incorporate professional certifications and ach0ievements from third-party organizations. As its support independent skills definitions and connect its client-designed badges to real-time labour market information and job opportunities. Badgr was one of the first two platforms to be IMS Global Open Badges 2.0 certified 2.0 compliant across all three implementation roles of Issuer, Host, and Displayer.

Accredible

Accredible was founded in 2013 with a mission to make all learning verifiable and quantified – it has main offices in USA and UK and employees working remotely from Canada, the US, Egypt, South Africa, the UK, the Netherlands, etc. Accredible currently serves to more than thousand renown organizations like Google Cloud, IEEE, McGraw- Hill Education, Slack, Harvard and Berkeley Universities.

Accredible provides a comprehensive digital badge and certificate platform with a full-service digital credentialing solution for creating and managing credentials and their integration with the organizations' legacy systems. It maintains and delivers a SaaS product that allows the issuing organization to design badges and certificates that can be dynamically updated with information about the certification, the recipient, the organization, or any custom information. Credential records, crucial for professional certifications, are always accessible, verifiable, and updated automatically when they lapse, so that valid credentials can be trusted. Furthermore, it has several verification features including the Verification Check, which 3rd parties can use to verify the legitimacy of the information they are seeing when looking at a user's credential. And the verification directory is another verification option, only available to Plus Plan issuers, which provides a central place for 3rd parties to come to verify any credential from the registered organizations.

Accredible data privacy policy is certified to comply with GDPR and other national privacy frameworks. Badges issued via Accredible also conform to the IMS Global Open Badges 2.0 standard.

Hyland

Hyland's business solutions[2] offered to Higher Education Institutions around the world can facilitate that all the data gathered by departments across an institution is accessible through a singular, configurable interface. One of the solutions from this palette is the verifiable blockchain-based Hyland Credentials, that makes the issuing of records easy and efficient, using a digital format that is fully compliant with internationally-recognised open standard, such as those of DCC and Europass mentioned in chapters 3.2.1 and **Error! Reference source not found.** respectively.

Initially incubated by MIT and evolving in alignment with the W3C, Blockcerts.org is the open standard Hyland is built on to issue and verify blockchain-based official records. Blockcerts are a new type of record that individuals own for a lifetime and can easily share with anyone they choose.

Hyland has designed its digital credential solution based on the premise that blockchain technology can combat fraud, mitigate risk and relieve administrative burdens associated with exchanging information and content. They assert that when used to issue official records as part of a holistic content and process management strategy, the power of blockchain only grows.

Thanks to the use of the open standard and blockchain technology, Hyland Credentials offers its users the following safeguards and benefits:

- Credential recipients own their records via key control, provided by the Blockcerts mobile app;
- Records can be verified across blockchains using the Blockcerts Universal Verifier;
- Records can be aggregated across various institutions, forming a lifelong record of learning and achievement;
- All content and personal data is stored off chain for maximum privacy;
- Records are standards-compliant JSON files, compatible with virtually any back-end system;
- The entire ecosystem is open-source, vendor-independent and aligned with other data standard.

Digitary and Parchment

Digitary (an online platform for certifying, sharing, and verifying academic credentials) and its parent company, Parchment (a platform and network for the secure issuing and exchange of academic credentials), both believe that digital credentialing processes should ultimately serve and empower credential holders, i.e., learners themselves.

[2] Connecting cross-campus processes is supported by solutions addressing (1) Enrollment management, (2) Business office, (3) Student life services, (4) Advancement and athletics, (5) Digital credentials, (6) Senior administration and (7) Information technology

Both parties share a common mission to help turn credentials into opportunities by digitally enabling schools and universities involved in issuing and recognising academic credentials. And while Digitary and Parchment strive to accelerate the transition of organisations towards issuing academic credentials digitally and securely, making credentials more actionable for learners – more effective at accessing enrolment or employment opportunities – is their ultimate motivation.

As part of its product portfolio, Digitary offers institutions a standards-based technology, called Digitary Certified Online Record Exchange (CORE), to issue cryptographically signed, legally valid, digital academic records. The Digitary CORE is a secure cloud platform that helps learners access and share online their digitally signed academic documents (such as transcripts, diplomas, certifications, digital badges, graduation/degree verifications and other sensitive documents) with employers, education providers, governments and other third parties.

Figure 13 Digitary CORE works around a triangle model of issue, share and verify

With Digitary CORE:

- Institutions can issue digitally certified degree certificates, transcripts, diploma supplements and other sensitive documents online;
- Education Providers can reduce credential fraud by using secure digital technologies;
- Education Providers can reduce costs and streamline processes by enabling self-service for learners and employers;
- Learners can access their digitally certified academic records online;
- Learners can securely share their records with third parties, quickly and easily;
- Employers and other credential viewers that are authorised by credential owners can quickly and easily verify learners' academic records.

Digitary documents comply with relevant security standards in each of the geographical regions where they have partners. These include XAdES-A and PAdES-LTV from the European Technical Standards Institute.

Digitary also provides the maximum level of security and legal validity of documents and data by adhering to these standards. Digital signatures are produced on FIPS 140-2 Level 3 cryptographic hardware devices, which are issued to officials of vetted organisations.

Digitary works with a range of universities around the world, each of which has their own Student Information Systems. Digitary uses modern technologies such as web services and XML data standards to allow easy data export from these Student Information Systems.

Azure AD Verifiable Credentials

Azure AD verifiable credentials provides a platform to digitally generate, present and verify customized verifiable credentials that an organization' employees, contractors, vendors, or customers can use in multiple scenarios. Azure AD verifiable credentials is now used by Keio University, Japan; the National Health Service (NHS) in the UK, the Flanders Government of Belgium

It is based on the use of DIDs (**decentralized credentials)** user-generated, self-owned, globally unique identifiers rooted in decentralized systems like ION (**Identity Overlay Network)**. They possess unique characteristics, like greater assurance of immutability, censorship resistance, and tamper evasiveness. These attributes are critical for any ID system that is intended to provide self-ownership and user control.

Microsoft's verifiable credential solution uses DIDs to cryptographically sign as proof that a relying party (verifier) is attesting to information proving they are the owners of a verifiable credential. While **DID User Agent/Wallet: Microsoft Authenticator App** enables real people to use decentralized identities and Verifiable Credentials.

Microsoft collaborates with members of the Decentralized Identity Foundation (DIF), the W3C Credentials Community Group and currently the Azure Active Directory Verifiable Credentials services implement the following standards: W3C Decentralized Identifiers, W3C Verifiable Credentials, DIF Sidetree, DIF Well Known DID Configuration, DIF DID-SIOP, DIF Presentation Exchange.

SHARE PROJECT MANAGEMENT OFFICE
ASEAN Secretariat
Heritage Building
70 Jl. Sisingamangaraja
Jakarta 12110
Indonesia

Phone: +62 (21) 726 2991
E-mail: info@share-asean.eu
Website: www.share-asean.eu

SHARE IS A PROJECT OF

SHARE IS IMPLEMENTED BY