Digital Student Data & Recognition

A White Paper for the ENIC-NARIC Networks

April 2020

Nuffic
meet the world

Erasmus+ Key Action 3,
DigiRec Consortium

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

Table of content

Executive Summary

Student data are offered increasingly in a digital format, which will work transformative to the current credential evaluation practices that were modelled on receiving and processing paper documents. This white paper systematically explores the relationship between digital student data and the recognition of foreign qualifications.

The leading question being:
"How can digital student data solutions and digitization of the credential evaluation process support fair and smooth recognition in line with the Lisbon Recognition Convention?"

The purpose of the white paper is to assist the 57 nationally appointed European academic information centres in the 55 countries of the ENIC-NARIC Networks, to develop policy and processes and be better prepared for the ongoing digitization. This paper should be read in the understanding that new digital student data initiatives are developed at an accelerated speed.

The white paper frames digitization both as digitization of student data and as the digitization of parts of the credential evaluation process. It also notes that in the (near) future 'digital learner data' instead of 'student data' may be more commonly used.

The benefits that digitization can offer ENIC-NARICs are improvements in security, speed, consistency, reliability, cost-efficiency, convenience, environmental policies, data control and statistics. However, each ENIC-NARIC centre differs in terms of mandate and size, and any strategy adapted needs to take into consideration the particular national recognition infrastructure.

The identified (potential) challenges include pluriformity of standards, acceptance and privacy laws. Moreover, a third of surveyed ENIC-NARICs had a legal framework that required paper handling of the applications.

When discussing digital student data, it is important to distinguish between the student data, technology 'delivering' the data, and standards. Digital student data come in four different levels of data maturity: 1) An image of the document (i.e. a PDF), 2) Structured data, 3) Standard compliant structured data and 4) Comparable data. The maturity level of the data will influence what aspects to look for when dealing with the data and also the level of digitization of your own processes.

Technology to deliver data should be seen as part of a larger business, information and technology architecture. Any well-designed information architecture should be able to consume information from different technologies, and as such be inclusive.

Standards can be distinguished on three levels: 1) the standard for the student information itself (e.g. credits in terms of the ECTS standard), 2) standard for the digital data format in which the student information is captured (e.g. the ELMO) standard designed by EMREX (see 4.2.1), and the standard for the architecture in which the digital student data is delivered.

The white paper looks into the lifecycle of the credential evaluation process, focusing on the input (data received), throughput (processing of the data, including evaluation) and output (recognition statement). For the input side, authorized sources and the ability to verify information are key.

For the throughput side, it is recommended to digitize all student data, and create a digital workspace that allows for interoperability and flexibility. Explore systematically the steps you are able to automate and ensure the process is in line with the Lisbon Recognition Convention (as practically translated into the EAR manual). Set up digital identification of the issuer of a specific set of data. Consider creation of a database of qualifications or connecting with an API to a trusted source (e.g. the Database of External Quality Assurance Results, DEQAR) to import information.

When switching to digital recognition statements, ensuring that stakeholders accept the digital format is key. Offering transparency about the (new) statements and how to verify these, a communication campaign to stakeholders, as well as data formats that are widely accepted are a few aspects to enlarge acceptance.

Recommendations are made on national and European level:

ENIC-NARIC centres

- Prepare yourself for ongoing digitization to serve your countries' students and higher education institutions;
- Reserve funds to switch to a more digital system and for staff training;
- Be prepared for a changing role of the credential evaluator in the future due to the ongoing automation, and consequently to a changing role of the ENIC-NARIC centre in the national context;
- When designing/choosing a database/system, comply with (inter)national regulations and choose a design for your database or system that allows you to act in line with the Lisbon Recognition Convention. Take the European Area of Recognition -EAR- manual as a starting point to verify;
- In case of increased automated steps, describe the process and principles of your evaluation database or system for quality assurance purposes;
- Ask other ENIC-NARIC centres for help and learn from their implementation process;
- Review whether your legal framework allows for handling the digitization of the credential evaluation process. If not, discuss this with the appropriate legal authority in your country.

The ENIC NARIC Networks

- Advocate for basic principles to stakeholders and support the development of common standards;
- Engage in a dialogue together with stakeholders to reap the 'low hanging fruit' for making student data digital;
- (Smart) databases and systems should operate in line with the Lisbon Recognition Convention (i.e., as formulated in the EAR manual);
- Centres monitor implementation and share developments, and good practices;
- Start a dialogue with trusted sources (to be identified by the Networks) to make information available for credential evaluation;
- Include by default identified trusted sources and verification services as official information in the country pages for all ENIC-NARIC centres;
- The ENIC-NARIC Network may explore how digitization could serve policy objectives for fair and smooth recognition, such as portability of recognition decisions and automatic recognition.

Part 1

1. Introduction

1.1 Rationale

The use of digital student data is gaining ground around the world. In Europe alone numerous initiatives advanced over the last few years to digitally share information about study results between students and higher education institutions. Digital exchange of student data has enormous potential for the recognition of foreign qualifications in terms of automated and therefore faster and more consistent recognition decisions.

A movement towards digital student data will transform the current credential evaluation practices that were modelled on receiving and processing paper documents. This situation raises a series of fundamental questions on how to use these digital data and how to develop digital processes, that are compliant with international agreed practice and treaties, notably the Lisbon Recognition Convention and in the future, the Global Convention on the Recognition of Qualifications concerning Higher Education.

This also include many practical questions, such as what sort of digital student data are around and what do you look for in terms of authenticity? How can the digitization benefit the credential process? What are obstacles and what are advantages?

All these questions are part of a larger question that has not been explored by the ENIC-NARIC Networks yet: how do digital student data on one hand and the recognition of foreign qualifications on the other relate?

1.2 Goal

The goal of this white paper is to fill this void and systematically explore the relationship between digital student data and the recognition of foreign qualifications, with the leading question being:
"How can digital student data solutions and digitization of the credential evaluation process support fair and smooth recognition in line with the Lisbon Recognition Convention?"

The purpose of this white paper is to create an understanding of the effects of digitization on the day to day credential evaluation work, and to offer new policy perspectives as well as practical recommendations/guidelines.

Here the authors of this paper wish to highlight that analyzing digital student data is like analyzing a moving target: new initiatives are developed constantly. Therefore, this white paper should be read as a general introduction and exploration into the topic.

1.3 Support ENIC-NARIC Networks

The white paper is primarily developed to assist the 57 appointed national information centres in the 55 countries of the ENIC-NARIC Networks, to develop policy and processes and be better prepared for the ongoing digitization.

The centres of the ENIC-NARIC Networks are the main audience of this paper because of the unique position they have serving as the backbone for the recognition of foreign qualifications in the Lisbon Recognition Convention treaty countries. While mandates of centres vary, they are all tasked to support the implementation of the Lisbon Recognition Convention on national and European level and are uniquely positioned to steer (and possibly streamline) the digital developments to the benefit of recognition.

1.4 Structure

This white paper is divided into three parts. The first part contains the introduction, of which this paragraph is part of. It lays out the reasons for undertaking this white paper and further outlines general considerations and conditions for implementation of measures. The second part provides an overview of the difference between data, technology and standards and next focusses on the three stages of the credential evaluation process: the input, throughput and output. In the last part of the white paper, recommendations are formulated for the use of digital student data and design of digital processes.

1.5. Methodology

This white paper has been developed in several stages by a project team consisting of ENIC-NARICs and other stakeholders (see 1.6). The first stage consisted of desk research to collect examples, which served as a basis to develop a blueprint for the white paper. Next, the ENIC-NARIC Networks were surveyed to collect their needs. Based on this input a first version of the white paper was drafted.

This first draft was discussed with a group of 33 participants from 18 countries at a mini - conference in Tallinn, Estonia May 2019. The participants represented ENIC-NARICs, higher education institutions, public ICT organizations for education and student and accreditation organizations. The collected input was used to produce this final version of the white paper.

1.6 About the DigiRec project

This white paper is produced as part of the European Commission Erasmus+ Key Action 3 Connecting digital exchange of student data to recognition (DigiRec) project.
The DigiRec consortium is composed of the following representatives from the ENIC-NARIC Networks: The Netherlands (Nuffic, coordinator), Estonia, France, Italy, Norway, Sweden, Poland and Canada, as well as EMREX (represented by the Norwegian Directorate for ICT and Joint Services in Higher Education & Research) and the Groningen Declaration Network.
DigiRec started in March 2018 with a duration of two years. The project is co-funded by the Erasmus+ Programme, Key Action 3, NARIC call, of the European Union.

2. General considerations for implementation

This section covers the general considerations and conditions for implementation.

2.1 How do we frame digitization?

The working definition for digitization used in this paper is “the conversion of information into a digital form and the digital handling of that information ”. In other words, digitization has two aspects:

2.1.1 The transformation of the information into digital data.

In the framework of this white paper, the focus is on any piece of information that is needed as part of the credential evaluation process which is offered in a digital format. This includes:

- Identification of the student (e.g., first and last name, date of birth);
- Qualification/Diploma obtained;
- Transcript (courses followed);
- Accreditation status;
- Credits and grades from the student;
- Level (e.g., place in NQF);
- Profile of studies;
- Learning outcomes.
- Note this list is indicative and not exhaustive. Moreover, as on paper, it is important the digitized data come from a trusted and authoritative source, and be delivered in a secure way to avoid falsification.

2.1.2 The digitization of (parts of) the credential evaluation process.

The transformation of paper information into digital data also drives digitization of the credential evaluation process. Digitized student data may require a digital environment to be received and being handled. Moreover, having information digitized opens up a range of possibilities for faster and more consistent evaluation of students' qualifications. These specific needs of credential evaluation, may also drive the way student data are digitized and made available.

2.2 How do we frame digital student data?

In this publication we speak of digital student data as the digital version of the 'paper' student data, traditionally used for evaluations. However, a term that may become more widely known in the (near) future is 'digital learner data'.

'Learner' captures the wide range of education experiences of a person such as the increasing options to 'stack' and collect learning (for example through standalone learning units as MOOCs and/or micro-credentials) to gain specific knowledge or skills. On the other hand, 'student' is commonly used to refer to the person following a traditional delivery of education (in class degree programmes). Consequently, it would be more fitting to use the term 'digital learner data'.

However, this white paper uses the term digital student data, for very practical reasons. The term 'digital student data' is currently widely used and introducing the lesser known term 'digital learner data' may be confusing and distracting from the aim of this paper. This said, when using 'student data' the paper does intend to capture all digital data as testimony of learning submitted by the applicant.

2.3 Examples and trends

What is the current state of digital student data portability and the digitization of credentials? The landscape is diverse with many developments taking place. Chapter 3 and 4 outline part of these developments. This section aims to provide a general overview of policy initiatives to support digitization of student data in the European area and beyond, as well as related initiatives that may benefit from digitization of student data.

2.3.1 European Union

The European Union, although only comprising part of the European Higher Education Area (EHEA) and the treaty countries of the Lisbon Recognition Convention region, is a major driver in this area for digitizing student records. In January 2018 it launched its Digital Education Plan (COM(2018)22 final). This Communication covers a wide range of aspects, from the use of data to inform policy, to support of online learning platforms. The EU also developed initiatives to support the digitization of student data. A few examples are mentioned below.

2.3.1.1 Digitally signed qualifications

Under Europass, the European Commission is working towards the launch of digitally-signed credentials and qualifications. These are electronic documents issued by education and training institutions that confirm the award of a qualification (diploma) or credential (stand-alone learning) to a person. The technical format will be based on open standards and integrated into the new Europass platform, where digitally-signed qualifications can be stored and shared with employers and credential evaluators. The aim is to offer 100% verification, easy transfer and a common format for the learning experienced. In addition, Europass also works towards a digital Diploma Supplement to replace the paper version. More information is provided in chapter 4.

Example 1: Diploma Supplement

The Diploma Supplement is issued by institutions in the EHEA and provides additional information about the degrees / diplomas and/or transcript issued. This information is very useful for recognition on programme level (workload, profile and learning outcomes). Therefore, digitizing this information would likely speed up decision making (see also chapter 5).

2.3.1.2 Erasmus Without Paper

The Erasmus+ programme is a funding programme from the European Union to support education, training, youth and sport in Europe. While EU initiated, its funding for education and transparency instruments for mobility have a wide impact on the EHEA and its efforts on digitization serve as major drivers in the European region. The next funding phase of the programme begins in 2021 and by that time, the programme should be run without paper. The Erasmus Without Paper (EWP) Network plays a pivotal role in achieving this. There are other initiatives such as EMREX (discussed in chapter 4) and the European Student card (below) and there are discussions on cooperation, to ensure compliance.

Example 2: EU Student eCard

The European Student eCard initiative aims to digitize the administration around student mobility for both higher education institutions and students, and should make it easier for students to access services during their mobility.
It would not be unimaginable if in the future a credential evaluation (i.e., on system level) or other information useful for credential evaluation is included as part of this card.

Example 3: Automatic recognition
Automatic recognition of European Higher Education Areas (EHEA) qualifications focusses on recognition on system level, meaning the quality and level of a foreign qualification are automatically accepted (and do not follow an extra procedure) if criteria for automatic recognition are met. How does digitization help? Quality and level are data that are relatively easy to digitize because the information is standardized and available. When accreditation status and level are provided by digital means, it is even easier for the credential evaluator to accept these. An example is the DEQAR database (see chapter 5). Automatic recognition combined with digitization also opens up the possibility for portability of these decisions on system level. Yet, it should be noted that portability of recognition decisions is currently being explored and can be complex because they are dependent on the national context (notably access rights) where recognition is sought.

2.3.2 Groningen Declaration Network

The Groningen Declaration Network (GDN) is a voluntary network and under its umbrella further digitization of student data is discussed, bringing together best practices, pilots, task forces and visions for the future.

GDN sprang from the realization that digital student data as stored by (national) digital student data depositories, may function as mobility boosters for students, higher education institutions, employers, recognition authorities and funding authorities. From 2007 onwards, the European Association for International Education (EAIE) conferences were used as the first sounding board to discuss. GDN itself as created in 2012 at a historic meeting in Groningen, the Netherlands, and established legally as a foundation in 2016.

The GDN is a diverse, global and interconnected ecosystem which includes large digital learner data depositories, educational institutions, government bodies, third party academic data processors and innovative companies, all seeking to facilitate educational and professional mobility.

The goal of the GDN is a global, equitable, accessible Digital Learner Data Portability environment. The opportunity is to convene practitioners and supporters to continuously share digitization development and use cases, strategies and tactics that are working, expand the number of new projects moving forward globally where capacity is lacking, and continue to bring new ideas as technologies and methods evolve to the fore to help achieve the goal.

Its annual meetings have been a key catalyst to the establishment of digital learner data depositories and exchange networks in and between China, the United States, Australia and New Zealand, Africa, Canada, and numerous countries in Europe. Since 2019 GDN has begun to mobilize digital learner data efforts in Latin America similar efforts will spread to India and southern Asia.

The inclusion of credential evaluation services and ENIC-NARICs has been a sustained aim of the GDN right from the start, because the process of recognition of foreign qualifications is where student data, enrollment issues, and licensure converge. It is they that stand at the juncture where digital credentials get 'converted', just like foreign bank notes get converted by money exchangers. The evaluation reports and recognition decisions that these agencies produce facilitate and further the academic and professional career of global skilled migrants, and the agencies involved are very much a part of the Digital Learner Data Ecosystem that the GDN advocates. Therefore, GDN has collaborated with various ENIC-NARICs and credential evaluation services in projects, research projects and other initiatives.

2.3.3 National actors

Apart from these supranational initiatives, national actors and initiatives play an important role. There are various initiatives to digitize data and some will also be mentioned in chapter 4, 5 and 6. National diploma depositories often play a central role in making their data digitally accessible for recognition and verification purposes.

2.4 General considerations

Should ENIC-NARIC centres go digital and if so why? This section generally lists advantages, as well as challenges for ENIC-NARIC centres, that may serve as push and pull factors towards implementation.

2.4.1 Benefits

- Security.
  Digital credential evaluations are (currently) more difficult to tamper with than paper evaluations;
- Speed.
  Digital solutions save time for applicants and credential evaluation services over paper data and procedures;
- Consistency.
  Digital solutions can automate steps in the credential evaluation process. Granted these follow the principles of the Lisbon Recognition Convention, this can be expected to contribute to more consistent and fairer recognition decisions;
- Reliability.
  Email addresses from applicants (often students) may be more reliable over time than their physical addresses;
- Cost-efficiency.
  Maintenance costs for printers, purchase of paper, envelops, seals, stamps, ink, costs for physical storage: these are over time higher than the initial cost for new software and retraining of staff. Staff do not have to resend duplicates of lost evaluations. Instead, the applicant uploads as many duplicates he/she wants;
- Convenience.
  It is becoming more and more common for individuals to apply for jobs digitally or displaying their credentials on social media (i.e., LinkedIn). If your service only offers paper evaluations, you are in effect forcing your clients to print their paper evaluation instead of offering a digital service from the start. Employers and institutions may, furthermore, easily verify the authenticity of the digital evaluation regardless of office hours. Additionally, digital evaluations are never lost: they can easily be retrieved and uploaded;
- Environmental policies.
  One tree is needed for every 9000 paper evaluations you issue. Thinking of Paper is a result of a chemical manufacturing process at printing mills. Delivery of paper both at your office and to your applicants entails transport on roads by vehicles that run on fossil fuel. In order

to send anything through the mail, you need paper envelopes and paper stamps. Digital credentials and statements, on the other hand, save trees and hardly leave any carbon footprint. Note that technical infrastructure (such as computers, servers) and technologies (using power) leave a carbon footprint, so if 'green' is a consideration, green digital data should also be considered in your choice;

- Control of Data.
  There are technological solutions available that allow you to revoke a digital credential evaluation after it has been issues. This you cannot do with paper;
- Statistics.
  There exists software that can help you generate statistics and keep track of how your evaluation statements are being used and by whom. This you cannot do with paper;
- Time and place independent operations of the national information centre.
  A digitized process allows for flexibility as to when and where the operations are conducted. In times where access to paper or a physical office is not possible (e.g., the COVID19 pandemic), a digitized process can ensure operations are continued. Choosing this flexibility can also be for reasons to balance staff work-life and (connected) supporting an inclusive workforce by enabling staff to partially work from home.

2.4.2 Challenges

There are challenges to consider:

- Standards.
  A lot of the digital student exchange going on apparently use PDF files. The good thing about PDF files is that they constitute a universal standard that is accessible by everyone. Yet, from a data maturity level, the PDF format forms the lowest category (see chapter 3). Future digital data solutions may use digital data and there is currently no agreement on what standard is being used. Moreover, the information needed to make an evaluation may not always be available (in digital format);
- Acceptance.
  Apart from whether the legal framework allows the ENIC-NARIC centre to digitize their process, there is also the aspect of practical acceptance by stakeholders. Strategies may differ, depending on the national context;
- Privacy laws.
  Privacy laws apply both to paper and digitized data. However, due to easier sharing and storage of digitized data, and more stringent laws, these laws should be carefully monitored in relation to digital student data exchange;
- In the United States, FERPA applies, while in the European Union, all data handling should be GDPR (General Data Protection Regulation) compliant. The GDPR regulation came into force May 2018 and states the principles for privacy and protection of data in the European Union. All ENIC-NARICs that are EU Member States have to follow this regulation, which has an impact on how data are being processed and stored. When considering implementing digital student data solutions, the following points should be considered:
  - For the EU Member States, all processes should be GDPR compliant, yet how this is interpreted differs how the regulation is implemented in your country;
  - The applicant has the right to be forgotten and also a right to rectification;
  - Data minimization: ask and use only the information needed to carry out the assessment. Any unnecessary additional data should be flagged as soon as possible by the evaluation service to then be deleted;
  - Information security: all the information should be stored in a safe way, to avoid loss or theft of data. Should a breach of personal data occur despite the security barriers set up, the owners of the data must be made aware of the situation;
  - Disclosure limitation: the holder of the qualification should be the owner of the data.

Note: although there is a trend towards digital, there are still a significant number of qualifications that remain paper based, at least for a while. Examples are qualifications obtained in the past, or qualifications from regions that are not digitizing yet. At the same time, there is already an entire industry around digitization of documents, running the whole gamut from PDF, Optical Character Recognition, to structured data. This development could make for a future where also pre-digital documents may be offered in a digitized format.

2.4.3 The context of the ENIC-NARICs

Another consideration is how implementation can support the public role of the centre and responsibility to its quality of services (i.e., implementation of the Lisbon Recognition Convention). This public role depends on the role of the centre in the (inter)national context.

National legal framework

A first survey completed by over 30 ENIC-NARIC centres showed that at least a third had national legislation in place that required original (paper) documentation to be submitted. This situation should be taken into consideration in the discussion when designing policies towards digitization.

Mandate and services

The ENIC-NARIC Networks are the national information centres in the European region, having a task under the Lisbon Recognition Convention Treaty to implement the Lisbon Recognition Convention. However, the mandates of the individual ENIC-NARIC centres can differ widely due to that recognition of foreign qualifications is organized differently in every country. In some countries, ENIC-NARICs make legally binding decisions; in other countries, they advise higher education institutions, who are the final ones responsible for the recognition decision. There are also countries where the national information centre does not make any evaluations at all, but rather focuses on the information provision aspect. Some ENIC-NARICs are providing services to employers, others do not. Some ENIC-NARICs have a staff reaching 80 full-time employees, other centres are staffed with two persons.

It is important to keep these national differences in mind, because the national legal framework and the way recognition is nationally organized, as well as the services offered by the ENIC-NARIC centres, will together determine what type of digital solutions for the workflow can be created.

Part 2 - Digitization in the credential evaluation process

Part two discusses digital solutions in three different stages of the credential evaluation process: input, throughput and output. Understanding the difference between (digital) information on one hand and technology to transfer this digital information on the other is key for discussing these three stages. Therefore, part two starts with an introduction to elucidate both concepts while also clarifying the concept of 'standards'.

3. Data, technology and standards

This chapter focusses on explaining the difference between data, technology and standards, in order to support a transparent discussion on the topic.

3.1 Maturity of digital information

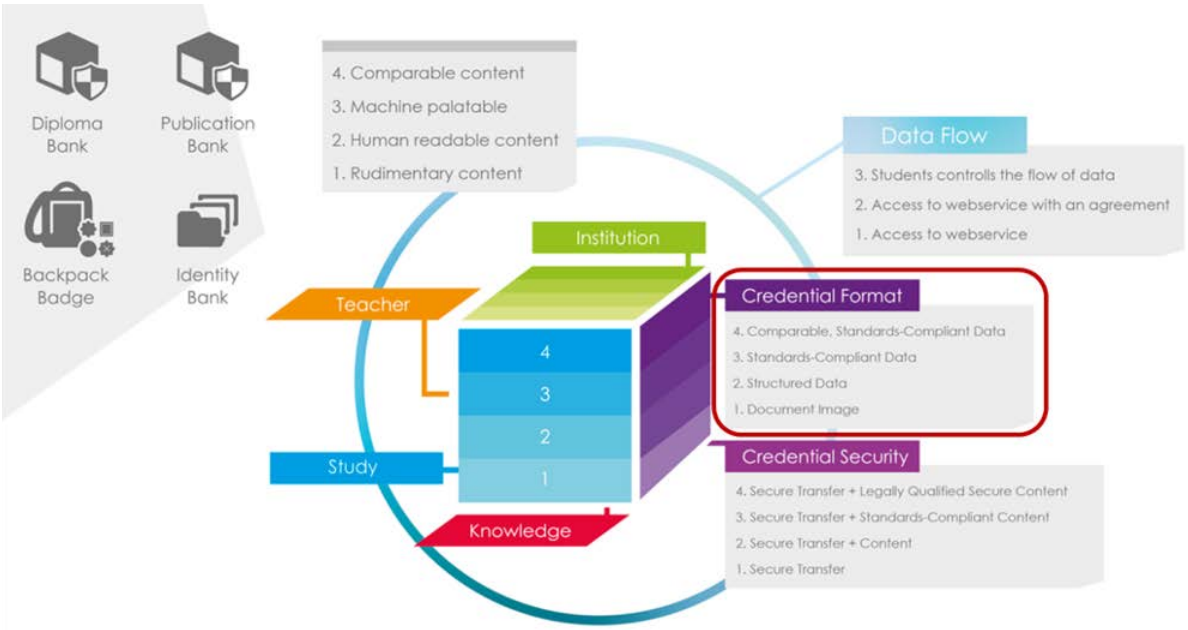
Digital student data comprehends all student information presented in a digital form, such as: name, birthdate, qualifications, (information on) transcripts including grades, learning outcomes.

At the same time, while paper is paper, there are different levels of 'digital'. Therefore, these levels are discussed in this paragraph, by using a classification made by the RS3G group. "RS3G" is the name of a cooperation between suppliers of software implementers and stakeholders in the EHEA that was founded in 2007. With partners from all over Europe and the United States of America, RS3G became an incubator for later projects and initiatives such as ELMO, EMREX, Erasmus Without Paper and the Groningen Declaration Network. One of the results of the "RS3G" cooperation was a maturity cube for digitization. The format of data was one of the aspects, including the following four levels of maturity:

- An image of the document, for instance a PDF;
- Structured data;
- Standard compliant structured data;
- Comparable data.

In this list, an image of the document makes the lowest level while comparable data makes the highest. The different levels are further explained below.

Figure 1: Four levels of data maturity compared to data format and credential format and security



1. **An image of the document.**
   When moving from the first to the last level of digitization, introducing an image of a document enables a digital flow of data. This also makes it possible to include security mechanisms such as digital signatures, encryptions etc. Exchanging data is faster than in a paper world, and it is possible to add trust to the document to prevent fraud. At this level of digitization, the information is a document that still needs to be processed manually in the same way as a paper document. An example is a PDF or JPEG from an original diploma or transcript.
2. **Structured data.**
   To enable better support with less manual registration, structured data need to be introduced to the process. With this we move away from the document itself and focus on the content of the document, exchanging the information as separate data elements. In many cases the original information used to produce a document is stored as data at issuer. For instance, a diploma or a transcript of records that is stored as structural data at education institutions. In this scenario the issuer can skip the production of a document and exchange the data itself. Now the receiver of the information can start using the data - in an automated process performing work earlier done manually.
3. **Standard compliant structured data.**
   To achieve a higher level of digitization, you introduce open standards for describing the structural data. At this level, the parties delivering data and consuming data agree on how this data structure should be implemented. All parties following the standard will be able to exchange data between them, and the data from many delivering institutions can be handled the same way in the receiving systems. One has to agree on the structure of the data, what kind of data should be included in the exchange, how it should be formatted, what should be mandatory, what kind of data document format (e.g., xml, Json). This is often a highly formal process that may take years to accomplish.
4. **Comparable data.**
   On the highest level of maturity, comparable data is added. In addition to agreeing on the format of the data, one introduces standards for the data itself. Examples of standard data in the education sector are European Qualification Framework (EQF) levels, International Standard Classification of Education (ISCED)-F-codes, and European Credit Transfer and

Accumulation System (ECTS) credits. An increasing amount of standard data offers the opportunity to automate more of the manual processes. The more standardized data you introduce to the process, the more rules can be made to automate the handling of these data. This will also prepare the organization for the use of AI in the process.

Table 1: Applicant's birth date in data

	Level data maturity	Example
1	An image of the document	The applicant's birthdate appears on an image (photocopy of the diploma or scan) and cannot be imported but has to be manually typed into a database.
2	Structured data	The birthdate is presented no longer as an image but as data, allowing it to be imported into a database and handled digitally. However, at this stage it is just 'loose' data without information about its meaning. It is not clear this piece of data is in fact the applicant's birthdate. Therefore, still 'manual' work is needed to identify the meaning of this piece of data, before it can be used.
3	Standard compliant structured data	At this level it is clear that the applicant's birthdate is a birthdate. The data format is standard, identifying the birthdate as birthdate, which eases the way of importing to handle the information. However, there is no standard how the data need to be delivered. This means that the birthdate may be presented as a date/month/year from one applicant, while month/date/year from another. Or the date may be written as numerical and text, 2 May 1998, Two May Nineteen ninety eight.
4	Comparable data	There is an agreed standard. The birthdate is recognized as birthdate and is delivered in a numerical and particular order (date/month/year). At this level it is possible to automate some of the data processing and take decisions automatically.

The different data levels are important to consider when digitizing the three stages of the recognition lifecycle: receiving data, 'processing' the data and generating data as part of the evaluation outcome. Table 2 below provides an overview of the four different data maturity levels and the implications for these three stages, while also indicating the opportunities and challenges for each.

Table 2: Digitization maturity levels comparison chart for ENIC-NARICS

Maturity level	INPUT 1 (Application form)	INPUT 2 (Documentation)	THROUGHPUT (Case processing)	OUTPUT (Decision)	Opportunities	Challenges/ risks
0. Analogue with basic computer support	Paper forms	Paper copies or originals	Manually (assessing paper);	Paper letter, sent as regular mail	None – analogue is no longer an option for most institutions	Time consuming
			Basic computer support (word processing etc)			Environmental costs
1. Analogue/ digital hybrid	Downloadable form on website (fill in on screen or by hand, submitted by regular mail)	Paper copies or originals submitted by regular mail	Manually (assessing paper)	Paper letter	Fewer errors	Distrust of electronic documents – the 'Gutenberg effect'
	Downloadable form on website (fill in on screen or by hand, submitted as e-mail attachment)	PDFs, JPGs submitted as e-mail attachments	Manually (assessing documents on screen)	(Encrypted) evaluation statement sent as e-mail attachment	Environmental gains (less paper)	Data protection/GDPR issues
		Encrypted PDFs sent by email directly from the institution through a digital platform.	Computer support (electronic archives, databases)	Integration with secure digital e-mail possible	Postal delivery times no longer part of case processing time	Open PDF files can easily be manipulated.

Maturity level	INPUT 1 (Application form)	INPUT 2 (Documentation)	THROUGHPUT (Case processing)	OUTPUT (Decision)	Opportunities	Challenges/ risks
		Encrypted PDFs sent directly to a receive account.			Use of mature technology (e.g. PDF files)	
2. Digital with mostly manual processes	Online form (data submitted by 'click of button')	PDFs, JPGs uploaded via online form	Manually on screen still the norm	(Encrypted) evaluation statement sent as e-mail attachment or downloadable online	Easier and more accessible application procedure	Legislative issues
		Structured data from external sources becoming possible – e.g. from national ID registers	Digital case handling systems	Evaluation statements based on blockchain technology. Both structured and unstructured data depending on the recipient.	Shorter case processing times	PDFs and JPGs require more digital storage space than structured data
			Some structured data allow for limited automatization	Possibilities for export of structured data to external registries and recipients	In line with expectations and national policies/ICT-developments	Vulnerable to obsolescence and changes in technology
					Increased portability of decisions	
					Applicants are offered additional digital services, e.g. e-wallets and e- portfolios to store electronic evaluation statements, digital credentials, micro credentials etc.	
3. Digital with limited use of structured data, standardization and automatization	Online form	Structured data from external sources increasingly becoming the norm	Increasingly automatized	Export of structured data to external registries or recipients increasingly becoming the norm	Structured data	Data quality issues - lack of standards, common formats
	User interaction ('self service') increasingly an option		Some 'self service' options for users possible		Automation of processes	Initial costs tend to be high
					Increased security and quality	
					Structured data require less digital storage space	
					Lower costs over time	

Maturity level	INPUT 1 (Application form)	INPUT 2 (Documentation)	THROUGHPUT (Case processing)	OUTPUT (Decision)	Opportunities	Challenges/ risks
4. Digital with extensive use of structured data, standardization and automatization	User interaction	Structured data from external sources is the norm	Automatization/ AI becoming the norm	Export of structured data to external registries or recipients is the norm	User in control	Fear of redundancy due to automatization
			'Self-service' options for users becoming the norm		Artificial intelligence (AI)	Increased environmental costs due to energy required for data processing
					Predictive analytics	Various 'unknown unknowns'
					Various 'unknown unknowns'	

Source: "Digitalisation in recognition. A policy paper initiated by the Nordic Council of Ministers." The ad hoc group on digitalization in recognition, 2020, page 12-13.

3.2 Technology

When building new support for work processes, you can use the concept of 'architecture' for the information systems being built. Architecture for information systems can be divided into three layers: business architecture, information architecture and technology architecture. This often helps in making order to a complex reality, and it is useful to be aware of these layers when discussing software systems.

1. Business architecture describes the purpose of the business, what the goals are, what processes are involved, the policies and stakeholders.
   The business architecture for recognition describes the purpose of doing recognition, who are involved and what are the work processes. A convention like the Lisbon Recognition Convention has elements of a standard built-in, describing some rules for doing recognition at a high level. To increase cooperation among countries, simplify the process for both citizens and ENIC-NARIC centres, one could imagine setting up standard guidelines for the recognition process as formal or informal standard at a more practical level.
2. Information architecture describes the information for your business, data models and structures, data sources.
   The information architecture for the recognition process is what data you need for doing recognition, what are the sources of these data, what information is produced during the process, how you organize the data.
   In this area there exist some standards. Examples are ELMO (used in Erasmus Without Paper and EMREX), the upcoming Europass format for digital credentials, standards from IMS Global on digital credentials like Open Badges, standards from PESC like EdExchange. In addition, there are a number of standards from generic standardization bodies ISO, W3C, CEN dealing with models for credentials and diplomas. Not many actors exchange structural data as of today so for some time now we will see a great variety of models and formats in use. Over some time, we will certainly see a change in this, with fewer more mature standards in use. But there is no need to wait for this to happen. The really hard work here is to get hold of and secure recognition data for the future. You should build good data models internally based on existing standards to handle this information, consuming result data from different sources, let the owner get control of the data, and prepare for data exchange with shifting standards over time.

3. The technology architecture is a specification of the technology used to support your business processes.
   The technology architecture describes the technologies for supporting the recognition process, handle input and output information, technology to automate processes, storing data, securing information. At this level there exist a lot of standards covering any business areas. Here we are talking about standards for storing data, exchanging data, cloud services, artificial intelligence, blockchain, platforms, digital signatures, cryptology, etc.

For all layers of architecture there exist a number of methods to describe the architecture. Note that with a well-designed information architecture, you should be able to consume information from different technologies like EMREX, Europass, blockchain and technology not invented yet. And open up the data for the data owner using the same technologies.
If the design of a system is correct, the information architecture will be independent of the technical implementation. To accomplish this, you need a good architecture and design.

3.3 Standards

A standard is the documentation of a product, a rule, a guideline or a definition. Standardization is the process of coming to an agreement on a standard. It is time consuming building a formal standard, where all parties come together to discuss the specifications. In this paper, 'standard' is used in three different meanings:

- standard for the student information itself (e.g., level in terms of EQF, or students credits in terms of ECTS);
- standard for the digital data format in which the student information is captured (e.g., ELMO, EDCI, IMS OneRoster, PESC academic college transcript);
- standard for the architecture in which the digital data format is delivered (e.g. EMREX, EWP, Europass digital credentials, Blockcert, Open Badge).

Some specifications have emerged from outside the standardization bodies and have been adopted in the development communities. An example is ELMO, which is a data format for learning opportunities, building upon a formal European standard data model, and adopted by EMREX and Erasmus Without Paper. This kind of specifications is often referred to as ad-hoc standards, not because they have been approved by an official standardization body through a standard process, but because they are commonly used.

A number of standardization bodies exists, international and national ones. Some of these are general standardization bodies like ISO and CEN, taking care of a great variety of standards. Others are more specific to certain fields, such IMS global and PESC for education.

4 - Input

The input chapter focusses on the digital student data a credential evaluator can receive. The three paragraphs provide examples of the type of educational data submitted by applicants. The (dis)advantages of each example are discussed and recommendations for their use provided. Note that developments in digital student data go fast and new examples emerge constantly. The project team made an effort to group the most common ones. The final paragraph presents minimal standards for the input side.

4.1 An image of the paper credential

Many centres receive digital copies of a paper credential, or themselves make paper they receive digital by transferring the paper into JPEG of PDF format. Below different types of digital copies are discussed, from a PDF based on a simple scan to a PDF generated on basis of digital data. The examples correspond with maturity level 1 discussed above.

4.1.1 A PDF sent or uploaded by applicant

In this case, the applicant:

- sends a file as an attachment to an email;
- uploads a file to an electronic application system.

The diploma owner authorizes a third party to release and share information to the credential evaluation, for example via an email with a:

- link to a service that enables downloading of the applicant's digital credential (e.g. e-transcript.);
- notification a digital credential is available for downloading from a previously installed portal.

Format

JPG/JPEG, PDF.

Advantages

The most common file format is the PDF. It is more or less a universal standard. This is a convenient form of document. It is portable. It can easily be uploaded to an electronic application system and made accessible for processing. Saves money and storage space. It does not deteriorate over time. Eliminates paper handling, frees up resources and speeds up turnover time. More environmentally friendly than paper (e.g., manufacturing, transportation).

Disadvantages

The document is not formatted data and the consequence is that it does not allow to handle the data digitally. Other disadvantages may include: insecure delivery, possible unfamiliarity with a different lay-out of a document and trust issues. An ordinary PDF or JPG/JPEG file has the same inherent flaws as a paper document, i.e. it can easily be manipulated by the applicant before uploading to an electronic application system. The scanned copies can be poor and illegible (e.g., the applicant can be unable to deliver good quality copies) and security features like colors, dry stamps or other security features may not be visible. The attachment may contain malicious software that can infect your computer. Anonymization of the digital file to make it GDPR proof (in case it needs to be stored in a database for future reference) is a time-consuming task.

In the case of digital copies of paper credentials insecurity in delivery can best be countered by rigorous verification.

Recommendations

- Accept only high-resolution digital copies in color – it helps to verify the necessary elements of the document (e.g. China – different colors of diploma at each level of education, Syria – colors of diplomas assigned to the universities; visible dry stamps and microprints or security features). This requires sufficient storage capacity;
- Invest in the relevant software to read the digital copies and enough memory space to store them;

- Use online verification portals (if applicable) to verify the authenticity of the document. Examples: UK HEDD https://hedd.ac.uk/enquirer-login and Ukrainian EDBO https://info.edbo.gov.ua/edu-documents/;
- When in doubt – verify the digital source or ask a fellow ENIC-NARIC;
- Contact the awarding institution or other competent authority for verification. Trust, but verify!

4.1.2: Digital credential shared by applicant via a third party

Input

This is a variation of example 4.1.1, the difference being that the PDF file is transferred encrypted from a third party and certified by a third party. In addition, the PDF may be generated on basis of digital data.

Format

Encrypted PDF.

Advantages

The advantages are similar to the one mentioned in 4.1.1. In addition, an encrypted PDF with a digital signature (certification) is difficult to hack (for example with the purpose to alter the information), therefore more secure than ordinary PDF or JPG/JPEG.

Disadvantages

As seen in example 4.1.1, there may be possible unfamiliarity with the new format and consequently trust issues. Furthermore, because of the self-destruction or expiry date it may be difficult to archive the digital documents without the proper software. There may problems with the verification of the source of the digital document, e.g. authorization from the university, ownership of the data and compliance with data protection laws (e.g. GDPR). There may be also a problem in case of spoofing, phishing etc.

The internal administrative staff that collects and/or checks the information provided by the applicant may not know what to do with the digital credentials. The access to the verification portals sometimes requires fees/receive account. Mistake in username/password leads to login failure.

Recommendations

- Determine that the third party is authorized to issue electronic credentials on behalf of the attribute (document owner);
- Download files from third party portals/receive account services when applicable. Examples: MyEquals https://www.myequals.edu.au/, eSCRIP-SAFE https://escrip-safe.com/login, Parchment https://www.parchment.com/log-in/ etc.
- Make sure that your admin knows how to process encrypted PDF files. For example, avoid printing encrypted digital documents on paper and then scanning them – the scanned documents may lose important features and the environmental benefits of digitization are lost in the process.

4.1.3: Digital extract from database shared by applicant via third party

A third party sends an email with a link to a service that enables downloading of the applicant's extract from a digital student data depository. While this is not an image of a paper, this still fits data maturity level 1 because the data are currently often (but not necessarily!) provided in a PDF.

Format
Encrypted PDF.

Advantages
These are similar to this mentioned under 4.1.2.

Disadvantages
The same as in 4.1.2. In addition, there may be an obstacle that some legal systems require a digital diploma and transcript or diploma supplement and the abstract / summary from the database may not be enough. However, although this should be taken into account, it should also be considered that digital student data are on the rise and it may be in the interest of the country to adapt the legal system accordingly.

Recommendations
- If the PDF is (qualified) signed using a digital seal (see eIDAS-legislation), one should be able to trust the issuer of the document. One need to check the signature if it represents the higher education institution;
- Determine that the third party is authorized to issue a digital extract from a digital student data depository on behalf of the diploma holder. Example: Norwegian Diploma Registry has a feature to look at shared data and download a signed PDF: https://www.vitnemalsportalen.no/
- Make sure that your admin knows how to process encrypted PDF files;
- Finally, it is paramount that the delivery and verification of the digital documents are only possible through proper authentication.

4.2 Standardized data
While the previous paragraph provided examples that fit the first data maturity level, this paragraph offers an illustration for the other levels: standard formatted and standardized data. Here the student data are delivered not as a picture, but as data, which are easier to transfer. These digital student data can be used in a semi-automatic recognition process (see chapter 5).

When student data are delivered in digital form, it is crucial that the 'authenticity' of the data, just as with a paper file, is guaranteed. In general, two elements are important:
- Data should come from a trusted source;
- The data were delivered in a secure way, meaning that they could not be altered by a third party.
- Note that the examples provided in this paragraph are not only examples of standardized data, but also examples of digital architectures as described in chapter 3.

4.2.1: EMREX
The example used is 'EMREX'. EMREX started as an Erasmus+ project and grew into a network that allows data transfer directly from the data source (diploma registry or SIS, student information system) to the receiving system (e.g. an ENIC-NARIC centres' database).

EMREX is user driven, meaning that only the student or former student can authorize delivery of data. The student/applicant logs into home portal and releases data to host via a format translator. All exchanges of data are encrypted and digitally signed to ensure reliability of the data. The network is open, and any organization can connect and deliver results.

EMREX uses "ELMO" (xml), which is a standard format including a number of standard data elements. XML stands for Extensible Markup Language and defines rules to encode documents in a format that is both human readable and machine readable. The XML syntax is a base for many formats. In addition, EMREX offers the opportunity to include attachments like PDF files to support exchange of the document itself (like a Diploma or Diploma Supplement) in addition to the data.
An active partner in the EMREX network can have one or both of the following roles:

- Provide the student with application(s) that allow them to fetch their results (e.g. achievement records) from another higher education institution, either in the same country or from abroad;
- Provide national client(s) with the functionality to fetch assessments (results from courses, qualification(s)) from the databases containing this information. This will later on be referred to as the National Contact Point (NCP).

EMREX is a decentralized system and the following elements are too: authenticating the student, fetching results for a student and storing results for a student.

Advantages
This example offers a standard format and (a number of) standard data elements. These can be imported into a structured database, and enable automation. EMREX is based on data standard ELMO. New sources should therefore not cause extra work with handling these data. It is possible to include a PDF which is helpful for systems that legally require a digital diploma and transcript or diploma supplement.

The student owns these data, which is GDPR compliant. Data are sent from a secure source to a secure host, no need to produce digital copies of a 'document'. No or little typing required at host. The data transfer is secure and virtually impossible to hack. Since the data comes from a trusted source there is no need for verification.

Disadvantages
A future inconvenience may occur if fees are introduced.

Recommendations:
Make sure that your admin knows how to deal with such data. Install relevant software to receive the data and reserve funds to invest in case of paid services.
Note EMREX is one example of more technologies around to present digital student data.

4.2.2: Badges/Digital/Open badges/Micro-credentials shared by applicant

A digital badge is a clickable graphic that contains an online record of student achievements. Digital badges can be issued to the learner by organizations and higher education institutions. The badges can be shared with a third party, or used on social media (e.g. LinkedIn). The data formats included in a badge, can differ from badge to badge. Note that this example is not a data architecture.

Badges are currently mostly used in relation to MOOCs and other learning units. They are included here because credential evaluators may increasingly come across these in the future due to the expected ongoing flexibilization (stacking of learning units or modules) of the higher education landscape, or if they are adapted to traditional learning.

In theory badges can be used for providing data about any type of learning, including full degrees. In practice, they are often used to show completion of smaller learning units (i.e. micro-credential courses) or other forms of learning within and outside the education system. Examples are Massive Open Online Courses (MOOCs) or courses offered on Lynda (affiliated with LinkedIn).

Format
Depends on the design.

Advantages
Badges work well with social media and E-portfolios. It is a way to document lifelong learning/retraining of workforce.

Disadvantages
Possible unfamiliarity with this form of credentials and related trust issues.

Recommendations
- Determine first of all whether your office evaluates the type of learning the badge represents;
- Determine answers to the following questions: What is the credential for? What does it represent? Does it represent coursework, professional development or attendance at a conference (i.e. trivial)? Are the badges verifiable? In whose name was it issued (earned by?) Who issued it? When does it expire?
- Tip: Given that digital badges in particular may include (non-accredited) learning that occurred outside of the education system, one may wish to look at the recommendations in 'Oops a MOOC', that deals with the recognition of this type of learning, following a traffic light model;
- Finally, it is paramount that there is security either in the delivery or in the verification of the digital documents.

4.2.3 - Digital credential Europass

As shortly mentioned in chapter 1, the European Commission will launch in 2020 the Europass digitally-signed credentials infrastructure (EDCI). Higher education institutions can use this infrastructure to issue their qualifications digitally.

The digital credential can be stored on Europass or the device of the credential/qualification holder. Europass already verified if the institution was authorized to issue the degree as well as the qualification holder. The qualification holder can share the credential/qualification with employers or credential evaluators.

The digital credentials issued by Europass are both available as an image and its data are machine readable, meaning the student data can be imported in a database for handling the application in an automated manner (see chapter 5).

Qualifications will include:
- Information about the awarding body;
- information about the person receiving the credential;
- information about the learning achievement represented by the credential;
- a visual representation of the achievement; and
- an eIDAS compliant digital signature (e-Seal).

Advantages
Qualifications issued are offered in different formats. They can be issued as PDF files, but the information provided is also machine readable, making it easy to import the information into a database for evaluating the credential.

Disadvantages
There may be initial unfamiliarity issues.

Recommendations
- Familiarize yourself with the key aspects of the Europass digital credential system to understand the elements to check;
- Make sure that your administration knows how to read and import the data.

4.2.4 - Digital credentials shared by Blockchain technology

Blockchain is an example of a technology architecture (see 3.2) to exchange student data, and not a data format in itself. In a blockchain, data are no longer centrally stored (e.g. in a database), but a footprint of the data (such as a diploma) is stored. This can be done in different formats. From PDF to structured data. The blocks can be accessible to third parties if given a 'key' by the owner of these data to access the record.

Blockchain as a technology is considered safe. The blocks are linked in a chain using cryptography (hashes). If the information in one block is altered, this automatically changes the hash of that block which would break the chain. A break will immediately be noticed by the other members of the network, which makes fraud difficult to impossible. It is for these reasons -security and access- that blockchain is often mentioned in policy initiatives. In chapter 6 the specific blockchain example of DiploMe is given when discussing 'output' of the credential evaluation.

Advantages
The data can be shared directly by the applicant and made accessible for processing. Compared to paper this saves money and storage space. Eliminates paper handling, frees up resources and speeds up turnover time. More environmentally friendly than paper (manufacturing, transportation etc.). It is impossible to hack, therefore technically highly secure. Applicants can also share data directly with your organization (peer-to-peer system) without the need of a third party 'middleman'.

Disadvantages
Blockchain is a new technology and the alleged advantages mentioned above fully depend on its implementation. Data transferal in a blockchain is considered highly secure and alterations impossible. Yet, this also depends on who is part of the blockchain network and how the network has been shaped.

The source of the documents stored in the blockchain should be trusted and verified to avoid fraudulent documents are included. Degree mills could operate a blockchain service that cranks out immutable records that are nonetheless fake. Fraud can also occur when documents are uploaded by applicants in the blockchain. For that reason it is important to consider which typology of blockchain is proposed (open, permissioned, private): the most common and used option for administrative services and, in general, the suggested blockchain for credential evaluation services is a permissioned blockchain, where only certified institutions can upload data regarding qualifications.

Some consider the necessity of wallets and keys (nb: which is also used in other technologies) a negative design choice, because it limits portability and depends on private software platforms and privately-owned companies.

Recommendations

- In case a credential is issued on a blockchain:
- Determine that the third party is authorized to issue credentials using Blockchain technology on behalf of the institution;
- Only accept digital credentials using blockchain technology that can be verified on the university website. Example: MIT https://credentials.mit.edu/ or from a permissioned blockchain, where only certified institutions can upload information on qualifications:
- In addition, in case of joining a blockchain:
- Create and use a blockchain where privacy is guaranteed by default and by design;
- Explore the potential use of blockchain technology as part of a shared network and/or an ecosystem, and not as a database of a single institution.

Example 4: Blockchain architecture, DiploMe

The DiploMe service, recently implemented by CIMEA and fully operational since April 2019, represents the first use case of blockchain technology applied to credential evaluation. It aims to provide a 'wallet' for people, where it is possible to store certified qualifications with blockchain technology, creating a decentralized, transparent, certified, and unchangeable qualification management system. The qualifications and the certificates are uploaded to blockchain by certified authorities (universities, ENIC-NARIC centres, national administrations, etc.), and the source of the information is always linked to the information itself. In this way the certified qualification becomes easily shareable and portable, reducing the risk of falsification. The evaluation statement is also issued on the blockchain, ensuring fast and secure delivery.

Diplome is built as an open ecosystem, which institutions, awarding authorities and certifying authorities can join it without any change in their existing technologies, according to the concept of interoperability. This is possible since DiploMe represents an example of private permissioned blockchain (see chapter 3). Diplome utilises a standard Ethereum blockchain and can run on any Ethereum-based variants.
Diplome's user wallet is composed of a standard user blockchain address/account and one or more smart contracts each handling one or more qualifications. The holder of the qualification is the owner of the information and of the cryptographic key that allows access to the saved data, through a mechanism fully compliant with the principles expressed by the General Data Protection Regulation (GDPR).
The implementation of this new system represents a cultural shift from analogic to fully digital credentials where only the most necessary information is shared. Paper can still be used according to national legislation and academic culture but at the same time the relevant information is kept secure on blockchain and can be shared in a simple, secure and certified way.

4.3 Recommendations

One of the basic principles of the Lisbon Recognition Convention says that all applicants have the right to fair assessment of their qualifications. Therefore it is advisable that the electronic recognition system was not only limited to the documents issued electronically but

also allow to upload scanned documents. There is still a large number of applicants who have only traditional documents and the majority of higher education institutions still do not award digital documents.

The digital credential may have different forms. It may look the same as a traditional paper document or it can be an abstract / summary from the digital student data depository. Irrespective of the form of the credential it should provide all the information that is necessary for recognition decision (degree, credits, grades, learning outcomes etc.). However, it should be taken into account that in some legal systems a paper or digital diploma and transcript or diploma supplement are required and the abstract / summary from the data depository may not be enough. At the same time, it could be expected that with the ongoing digitization, legal systems that are 'paper oriented' have to be revised. Standardization of digital diplomas is about to happen now, and this will be a data package with standardized formats and standard data, a lot of information about the qualification and courses involved. The formal documents as we know them will be secondary in such data packages. All this is done to provide better services for the data owners and for the receivers of the information to enable digitalized processes.

The digital credentials should be issued by an authorized source. As mentioned in the previous section the digital documents are not necessarily issued by a higher education institution awarding a degree. They are often issued and sent or published by a third party. In such a case it should be possible to verify (e.g. through the website of the awarding higher education institution) whether the third party in question is authorized to issue credentials on behalf of the awarding higher education institution.

It should be possible to verify whether the credentials are authentic and whether they have been modified. This applies mostly to the scanned copies of paper documents. But also in the case of a credential that has been downloaded from the portals and sent as a PDF file. The ideal situation is when the credential can be verified automatically (i.e. through blockchain or other digital signature solutions e.g. eIDAS for) or in cases of PDF files on-line and free of charge.

It should be possible for a recognition body to receive and save the digital documents in digital archives without printing out the digital version.
The system of issuing or sharing of digital credentials should comply with the legislation concerning protection of personal data (e.g. GDPR).

5. Throughput

Whereas the previous chapter focused on the type of data received, this chapter discusses what happens in the ENIC-NARIC office and the possibilities of digital solutions to process these data. Therefore it will first provide an overview of the type of databases available. Next, the chapter reflects on the implementation of digital solutions in the main steps of the credential evaluation process, while analyzing the (dis)advantages and the minimal standards desirable using the Lisbon Recognition Convention as a benchmark. Finally, the chapter provides recommendations for implementation.

5.1 What happens in the office? Databases

This chapter provides an overview of type of databases currently in use. Note that the examples of databases are stereotypes and that actual databases differ because their functionalities will always depend on its purpose and its users, including the considerations mentioned in chapter 2. For each type, it is discussed how they support, or can support, the five elements of a qualification that should always be taken into consideration when evaluating a foreign qualification: quality, level, learning outcomes, profile and credits. Moreover, the advantages and disadvantages of each of them are highlighted.

5.1.1 The 'digital paper' workflow

In this example the paper is transformed to an image (JPEG, PDF), which allows for easier electronic processing than a stack of paper files would do. However, no application or database is used to process the information or manage the workflow (as in the next example). While decisions may be stored electronically, or even detailed in an Excel sheet, this is in essence a paper workflow.

The type of solution focuses on receiving paper documentation and may therefore be considered to not be the best option for today's reality and a future where more digital student data will be offered. Moreover, also the way the information is handled, involves significant manual work, when compared to the technical alternatives available.

5.1.2 The digital database

In this example, paper or digitized paper student records (i.e. PDF or JPEG files) are included in a database for processing. There are many variations possible on how this is done, but roughly two options can be distinguished:

1. The ENIC-NARIC employees enter the information provided by the applicant (on paper) in a web-based application. The evaluation is made as if it was a paper file and stored in the application and as soon as it is ready for the applicant, printed out, signed and sent by post.
2. Applicants (individuals or entities such as higher education institutions) manually enter data about the(ir) educational career and upload relevant data such as passport copy, diplomas, diploma supplement and a lists of marks. This can for example be done via registration on a website and log in to apply for a diploma evaluation.

When this information is entered and uploaded, the database consists of a mix two types of data: (standard) formatted data (the manually included information by the applicant) and images (PDF files of passport, diploma, transcripts, etc.). In case the standard data were included by the applicant (i.e. name, etc.) this information will need to be verified by the administrative staff or credential evaluator.

Information that the credential evaluator needs in order to make the evaluation, appears in the application, which allows for easy processing. Moreover, there are steps in the process that can be automated if the data are available in standard format. For example, it can be searchable for previous decisions. This can be done by the credential evaluator dealing with the case, or the database can be made accessible to stakeholders searching for this information to help them in their recognition decision. Furthermore, in more advanced database systems, rules can be included, for example to automatically recognize qualifications on system level that fulfill certain requirements.

5.1.3 The fully digitized workflow

In this model, all the student data are available in a standard data format. This requires a trusted data source delivering standard data on the diploma, transcript and (if available) diploma supplement.

To describe this option is not easy, because while elements are in place, this option is not in full existence yet. The reason is that not all necessary student data are available in a standard data format and/or can be delivered from a trusted source. This will become clear when looking at the table in the second paragraph, 4.2.

5.2 Automating the credential evaluation process

There are many advantages to automate the credential evaluation process, the main ones being to speed up the time needed for the evaluation (in line with the Lisbon Recognition Convention) and decisions being more consistent, contributing to fairness. However, as seen in previous paragraphs, it will all depend on how the solutions are implemented whether these benefits can be reaped.

5.2.1 Overview credential evaluation process

To create transparency in how digital student data and automation of steps can support the credential evaluation process, the table below is designed. It outlines the different stages of the credential evaluation process for the three different scenarios as discussed above: 1) a (digital) paper situation, 2) a database with manually included digital student data, and 3) a system where student data are delivered digitally and processed by the system. These stages follow the Lisbon Recognition Convention as translated in the agreed upon good practice of the European Area of Recognition manual. Note that each step is a simplified version and does not detail all the aspects to consider.

Two nuances:

- In reality, the second type of database could also receive direct student data. Therefore this could turn into a more hybrid model than presented here;
- This last option (the right column) is not (yet) in place and therefore the column also offers more an exploration and a starting point of what would be required for implementation following the Lisbon Recognition Convention. For the sake of the argument, it not only implies that only digital data are accepted, but also that the information is largely processed by the system.

Table 3: Digital student data, automation of steps and the credential evaluation process

	1. Digital paper workflow	2. Database with (manually included) digital student data	3. System including standard digital data delivered digitally
File complete?	▪ Credential evaluator checks if information uploaded by applicant corresponds with required documents	▪ Credential evaluator checks if information uploaded by applicant corresponds with required documents	▪ System checks if file is complete ▪ Identification person through a trusted verification mechanism
1. Quality Check the accreditation status	▪ Credential evaluator looks up the accreditation status	▪ Credential evaluator looks up the accreditation status and/or ▪ The database can pull up the information based on previous decisions that can be accepted	▪ Information is provided by a trusted source (i.e. accreditation agency or national diploma register) and can be automatically accepted or ready for assessment by the credential evaluator.
2. Authenticity Verify the authenticity	▪ Credential evaluator evaluates the authenticity, and conducts internal and external verification if necessary	▪ Credential evaluator evaluates the authenticity and conducts internal and external verification if necessary	▪ Verification is done automatically through delivery by a trusted source (i.e. a diploma registry or the higher education institution).
3. Purpose of Recognition Establish the purpose and establish the access options	▪ Credential evaluators considers the purpose of recognition	▪ Credential evaluators considers the purpose of recognition	▪ The system needs trusted information to determine the purpose
4. Level Establish the level of the qualification in the national system and whether it gives access to further study in the country of origin?	▪ Credential evaluator checks the level of the qualification in the national system and acces rights	▪ Credential evaluator checks the level of the qualification in the national system and access rights ▪ The database can pull up the information based on previous decisions.	▪ Information on the level of the qualification is provided by a trusted source (i.e. accreditation agency or diploma registry or (in the EHEA) from a digitized Diploma Supplement).
5. Profile What is the profile of the programme?	▪ Credential evaluator establishes the profile, based on the information in the transcript and Diploma Supplement	▪ Credential evaluator establishes the profile, based on the information in the transcript and Diploma Supplement	▪ Information on the profile is provided by a trusted source (i.e. the higher education institution).
6. Workload What is the workload of the programme?	▪ Credential evaluator establishes the workload, based on the information in the transcript and Diploma Supplement	▪ Credential evaluator establishes the workload, based on the information in the transcript and Diploma Supplement	▪ Information on the workload is provided by a trusted source (i.e. the higher education institution). The system establishes the workload in terms of credits.
7. Learning Outcomes What are the LO's of the programme?	▪ Credential evaluator establishes the learning outcomes ▪ NB: In many cases, learning outcomes are not readily available. They can however be constructed from the level, profile and workload (5, 6 and 7 below)	▪ Credential evaluator establishes the learning outcomes, transcript and Diploma Supplement ▪ See NB left column L.O.'s may not be available	▪ Information on the learning outcomes is provided by a trusted source (i.e. the higher education institution, Diploma Supplement). ▪ See NB left column L.O.'s may not be available
Final evaluation	▪ Credential evaluator grants recognition unless there is a Substantial Difference in terms of quality, level, profile, workload or learning outcomes in the purpose for which recognition is sought	▪ Credential evaluator grants recognition unless there is a Substantial Difference in terms of quality, level, profile, workload or learning outcomes in the purpose for which recognition is sought	▪ System grants recognition unless there is a Substantial Difference in terms of quality, level, profile, workload or learning outcomes in the purpose for which recognition is sought ▪ NB: systems like these are currently not available
Denial or partial recognition	▪ Credential evaluator communicates decision to the applicant	▪ Credential evaluator communicates via database decision to the applicant	▪ System communicates decision to the applicant

5.2.2 Automating the process

When looking at table 3 above and thinking about the credential evaluation and how this could be fully automated, the following considerations come to mind:

1. The extent required information is available (in digital format);
2. Availability of trusted sources to deliver the information;
3. Secure delivery of information;
4. Technical abilities of the database/system used to automate steps in the credential evaluation process;
5. The role of the credential evaluator in the recognition process.

5.2.2.1 Availability of information (in digital format)

When considering digitizing data, it should be taken into account that not all information for credential evaluation is available, and if it is available it may not be available in a singular format, complicating the standardization of the data. Below this is further explained.

A credential evaluator following the principles of the Lisbon Recognition Convention, focusses in its evaluation on the five elements of a qualification: quality, level, workload, profile and learning outcomes. The first two, quality (accreditation decision) and level (in terms of National Qualification Framework and European Qualification Framework level), are available for a majority of the EHEA countries. Exceptions may include pre-Bologna qualifications, or qualifications issued in the past at a time when Bologna Process was on its way but the accreditation status and levels in an EHEA country were not yet captured in standardized data. Outside of the EHEA, it differs from country to country whether this information is standardized. It will be more difficult to connect and compare information to for example an European Qualification Framework level, simply because the European Qualification Framework is not used. The same goes for the accreditation decision.

For the other three aspects, the information is not standardized in the European Higher Education Area (let alone outside), even on paper:

- Profile: the words used to describe the profile of a qualification differ from programme to programme;
- Workload: while credits can be uploaded, systems may differ between countries and even within one country. Judgements on differences in this respect should be based on thorough examination of the context of the credit system used;
- Learning outcomes: descriptions, if available, differ widely, one of the reasons being there are no international agreed standards for writing learning outcomes.

While the differences occur when using the same language, many qualifications and transcripts of records are provided in the language of the country. This all may result in difficulties to turn these data into standardized data.

5.2.2.2 Availability of trusted sources and secure delivery of information

Trusted sources and secure delivery are two different topics that are discussed together because of the benefits they have when combined.

ENIC-NARIC centres are for digitization dependent on the extent digital student data can be delivered or imported from a trusted source or not. A trusted source should be an authoritative party in the (inter)national context to deliver the data. Trusted sources are important to avoid fraud (i.e. information from diploma mills should be avoided).

Secure delivery of digital student data is crucial to keep the trust that information is not altered. Together, trusted sources and secure delivery can have immense benefits for credential evaluation.

For example: confirmation from a trusted source that the qualification and transcripts were issued to the applicant in a secure way, can make 100% verification of the authenticity of the degree possible in a split second, making manual verification redundant. Nota bene: this would be the most valuable for qualifications from countries where there are known problems with fraud. However, these may also be countries where verification at the source is problematic.

But also in relation to the five elements of a qualification, secure delivery from trusted source can assist credential evaluators. There may be less need to 'manually' check information (i.e. accreditation status and level, if confirmed from the source) and this contributes to automatize steps in the credential evaluation process.

5.2.2.3 Technical abilities of the database

The technical capabilities of the database or system used to import the student data and process them, is of crucial importance when speaking about automating the credential evaluation process.

The higher the data maturity level, the more it will be possible to automate steps (if delivered from a trusted source in secure way). This is also a variation of the 'chicken and egg' question "what drives what?": the digital student data the database or the possibilities for a digitized database/system the digitization of student data? Examples of automations are:

- Direct and 100% verification of information from trusted sources;
- (Automatic) search of records to pull up previous decisions that can be used for a new evaluation;
- Making use of artificial intelligence to include rules how to deal with the delivered information. For example: if the accreditation and level from institution x from country y is confirmed, the qualification can be automatically recognized on system level.

To be inclusive, databases may also be able to adapt to different data maturity levels, given that not everyone will be able to provide digitized student records.

Example 5: the DEQAR - API

The European Quality Assurance Register for Higher Education (EQAR) developed a database called 'DEQAR' that includes all external quality assurance results by registered agencies, based on agreed EHEA quality assurance standards, the ESG.
DEQAR provides an application programming interface (API) that allows you to feed this data directly into your local application or system.
As a recognition office or information centre (ENIC-NARIC) you may use the API to embed a search into your workflow to verify accreditation/evaluation status of an institution or study programme. In doing so, you can automate part of your search related to the quality. This is currently piloted by four ENIC-NARICs as part of the DEQAR CONNECT project.

DEQAR data is public and freely accessible for anybody free of charge, but EQAR reserves the right publish a list of registered users for transparency reasons. More information is available via the https://www.eqar.eu/qa-results/get-data/connect-to-api/ website.

5.2.2.4 The role of the credential evaluator

When using a basic database that is processing manually imported data and where the core information (diploma, transcripts) consists of images, the credential evaluator is clearly positioned as the authority to make decisions about the five elements of the qualification. However, this role shifts, when trusted data can be securely imported and steps automated. Wat is the role of the credential evaluator if student data are made digital, the credential evaluation process is digitized and steps are automated?

To fully automate the process and make the role of the credential evaluator superfluous, the system has to act in line with the Lisbon Recognition Convention and grant recognition unless there is a substantial difference.

In other words, the system has to have the ability to consider differences that are so significant (in terms of quality, level, profile, workload or learning outcomes) that they are likely to prevent the student from succeeding in the purpose recognition is sought for.

This would not only require the availability of a lot of information offered in standardized data (format), but would also require a system that is so advanced it can make a detailed consideration. In this respect it is important to note that the above table is only a simplification of steps and in reality many elements need to be considered, that also are country-specific. Perhaps the most difficult part is that credential evaluation, especially for difficult cases, is not an exact science. There may be contextual considerations that seem difficult to be captured in a system.

Yet, the role of the credential evaluator may shift when steps are automated into including rules for the database / systems used and overseeing processes.

5.3 (Dis)Advantages for the 'throughput' side

Advantages

- The major benefit of processing student data digitally is the opportunity for faster and more consistent recognition decisions. Digital processing student data, especially when combined with artificial intelligence, has the ability to automate various steps in the credential evaluation process, thereby always following the same rule;
- Creation of a digital archive makes it easy to consult according to different criteria (country, institution, qualification);
- Use of artificial intelligence to do part of the credential evaluation is relevant if the centre has a huge amount of date to compare the qualification with;
- In the long-run, digitization of the process of data will enable evaluation services to process applications at a faster pace.

Disadvantages

- Transition to a digital process requires -even if beneficial in the long run- an investment in terms of human and financial resources. Furthermore, there are costs associated to implement, maintain and secure a digital process, including the training of staff;
- The multitude of modes in which student data are offered from around the world may make it challenging to implement a process that is adaptive to accept all these different modes;

- Depending on the system used, it is time consuming to anonymize personal information on the documents once the service is done (i.e. the statement has been awarded).

5.4 Minimum standards based on the Lisbon Recognition Convention

- Keep the assessment still 'open' (or the information changeable) in order to change it in case of an appeal, and of a positive answer to the appeal procedure, this will satisfy Article III.2 of the Lisbon Recognition Convention: "Each Party shall ensure that the procedures and criteria used in the assessment and recognition of qualifications are transparent, coherent and reliable";
- this will satisfy Article III.5 of the Lisbon Recognition Convention: "Decisions on recognition shall be made within a reasonable time limit specified beforehand by the competent recognition authority and calculated from the time all necessary information in the case has been provided. If recognition is withheld, the reasons for the refusal to grant recognition shall be stated, and information shall be given concerning possible measures the applicant may take in order to obtain recognition at a later stage. If recognition is withheld, or if no decision is taken, the applicant shall be able to make an appeal within a reasonable time limit.";
- All this satisfies Article VI.1 of the Lisbon Recognition Convention "To the extent that a recognition decision is based on the knowledge and skills certified by the higher education qualification, each Party shall recognize the higher education qualifications conferred in another Party, unless a substantial difference can be shown between the qualification for which recognition is sought and the corresponding qualification in the Party in which recognition is sought".

5.5 Recommendations

- All qualifications received should be digitized, if they did not come already in the input phase as digital;
- Creation of a digital workspace and a digital workflow to manage all the application lifecycle;
- Such digital workspace should allow for interoperability, in order to be able to process various data standards, including current major ones (XML, JSON, EDI and PDF) while functioning as a unique and centralized database for all applications to avoid any form of data duplication and the multiplication of data storages;
- Such digital workspace should be also designed to remain flexible, evolutionary and open to possible future data standards, with or without the intervention of a third-party;
- Additional data should be added if not present or not requested to applicant in the input phase (name of the institution, name of qualification, awarding country, awarding year, etc);
- If the qualification is coming already with metadata (i.e. the data entry has been done by the applicant) the metadata could be used to automate the division of tasks among credential evaluators (e.g. qualifications with issuing country X go to the credential evaluator in charge of country X);
- In case the document has been verified, add this information in the metadata (e.g. confirmed falsified/authentic – no confirmation);
- Digital identification of the issuer of a specific set of data should be archived and used as future reference to facilitate the authentication of similar applications in the future and detect potential fraud;
- If a fraud is proved, evaluation services may be permitted (where applicable) to retain the falsified data to prevent future potential frauds;
- Consider the creation of a database of qualifications, searchable by categories (name of the institution, name of qualification, awarding country, awarding year, confirmed falsified, source

of the qualification, if student or university, etc.): useful to compare qualifications with other sample form the same institution, same year, etc, and be able to issue the same decision;
- In the same database the assessment report should be stored to enable comparisons of assessment decisions on similar qualifications;
- With the use of artificial intelligence, the archive will serve to automate at least part of the assessment work and as a basis to reduce 'manual' assessment.
- When automating steps, be sure that these are in line with the Lisbon Recognition Convention and the good practice as described in the EAR (HEI) manual;
- Ensure your office's quality assurance process includes any steps in the credential evaluation that are automated.

6. Output

The output of the process are the recognition statements following the decision. What statements are provided and in what format? How to get stakeholders accept evaluations based on digital student data and/or digital evaluations. In addition this chapter analyzes and reflects on possible (dis)advantages of digitization on output side, any minimum standards (using the Lisbon Recognition Convention as standard) for the output side, and provides recommendations for the output side.

6.1 What statements are provided and in what format?

6.1.1. Types of statements

In general there are different type of statements ENIC-NARIC centres can produce. These depend on the objective (i.e. employment, study, visa, etc.) and documents available. Examples are:

- Study periods for applicants who did not achieve their studies;
- Statement of comparability;
- Indication of the level of studies;
- Formal recognition decisions

The following are examples of the different sorts of digital evaluation statements and the ways they are currently being issued:

- Automatic format generated via a portal/database that is accessible by the applicant and whom can download the statement from there. In France this statement comes in a PDF format, in Austria and Sweden an encrypted PDF file with an electronic seal is used;
- Data provided via the EMREX network, formatted as ELMO (distributed the same way as assessments from higher education institutions);
- Formal recognition statements are made available to applicant through secure digital mailbox. Preferred format would be secure .pdf (Norway);
- Statements that are accessible via a secure (national) portal where applicant can access it and make it available to third party;
- E-recognition: statement verifiable online (eg. eSAQA provides an electronic seal with a secure link to the SAQA database);
- Blockchain initiative to certify the statements of comparability issued by the centre.
- These statements may present different security features fitting the data maturity level and mode of delivery. Currently most statements are issued as digital documents, and security features include: a digital stamp, digital signature and QR-code.

Example 6: Future development? Europass
Europass is exploring the possibility for ENIC-NARICs to include evaluation statements from digitally signed or paper based credentials in Europass. This idea is still in a conception phase and requires further development. But in this scenario, the statement is issued digital and can be included in the Europass ePortfolio and shared for the purpose of employment or further studies.

6.2 How to get stakeholders accept digital evaluations?

Acceptance of digital evaluations by stakeholders is very important. To convince all stakeholders (applicants, higher education institutions, employers, public bodies) to accept digital evaluations, it is essential to:

- Facilitate exchanges and collaboration between higher education institutions and ENIC-NARIC centres;
- Develop a communication strategy adapted to each stakeholder and based on:
  - the reliability of the information provided. Indeed, digital evaluation documents present different security features (digital stamp, digital signature, QR-code, blockchain);
  - the accessibility of the information provided. Easily available at any time, any moment and through any device;
  - at no cost basis and avoid extra costs for authenticity verifications.
- Consider a short guide providing information how the digitization process was implemented. This could enhance trust on the service and process.
- Official statement from MOE (or other govt. authority) that digital signature is the only kind available from country x;
- On more general level, close collaboration between ENIC-NARIC centres and the Groningen Declaration Network which has been advocating this right from its beginning in 2012.

Example 7: Creating paper look to facilitate acceptance
One way to facilitate the acceptance of digital evaluations is to create digital documents that have the look of the paper evaluations complete with colors, images/stamps and backgrounds/watermarks that mirror the paper document. This is what US institutions do with e-transcripts since 2002 and this may work for digital evaluations too.

6.3 Pro's and con's for the 'output' side

Advantages

- Faster procedures: statements can be made available instantly for the applicant after the decision is made, and information can be made accessible to a third party (after approval by the applicant);
- Security of information:
  - digitized statements are more secure than paper documents. They are more difficult to be modified by the applicant;
  - possibility to verify these statements via a secured platform. In some cases, the employer/higher education institutions/public body could check the authenticity online;
- Environmentally-friendly and cost efficient: no paper used, and no carbon footprint made to deliver the paper;

- Benefits for the ENIC-NARIC centres:
  - automation allows to generate reliable statistics (number of statements issued, per country, etc.);
  - decrease of administrative burden, and human resources can be used for other tasks;
  - it is easy to duplicate the evaluation document/final decision, or to cancel it if necessary;
  - seize the opportunity to implement a new process, to reflect on internal practices and internal quality assured procedure.

Disadvantages

The disadvantages are here identified as risks:

- Computer bug, potential hacking and new types of fraud may impact the output side;
- Requires a certain degree of tech savviness on the part of the applicant;
- Archiving and storage:
  - need to have enough room to store all the statements (and files);
  - validity period to check the digital evaluation
- National legislation:
  - related to personal data: the digital evaluation document must comply with national and European regulations;
- In some cases, national legislation requires the analysis of paper documents and original documents;
- Reluctance of some stakeholders who prefer to deal with paper documents.

6.4 Minimum standards based on the Lisbon Recognition Convention

Following the good practice of the Lisbon Recognition Convention, the evaluation statement should include all relevant information, and in case of a recognition decision or advice whether full, partial or no recognition is granted. It also should be issued within a reasonable time limit (art III.5).

In line with the Lisbon Recognition Convention and the public task ENIC-NARICs fulfill, any falsifications of the statement should be avoided. Therefore, the evaluation statement (in digitized document or data format) form needs to contain minimum security features. Their verification must be easily accessible to allow verification at any time.
In addition, the evaluation document must comply with the legislation in force (particularly regarding personal data).

6.5 Recommendations

For the issuing of digital statements, the following should be kept in mind:

- It is essential to develop a 'digital culture' among all stakeholders (applicants, higher education institutions, employers, public bodies) and to think about ideas (platform, new ways of communication, training) to promote the added value of digital evaluations;
- The digital delivery of the statement should always be free of charge for all stakeholders. This includes verification of the digital evaluation documents via a portal or a platform;
- The digital statements should be trusted. Therefore, they should contain appropriate security features (both statement and delivery), in order to gain the confidence of all stakeholders;
- Authoritative sources should be included to promote and provide information about the format in which the digital evaluations are issued, in order to achieve acceptance;
- Output of data should be available in a diversity of digital formats, as more and more postsecondary institutions are gearing up for digital student data. It has appeared on several occasions that employers or regulators are struggling to receive, process and base their decisions on digital data. Not only may they lack the infrastructural and digital workspace to process digital data, but they may also not have policies to process such data;
- Include by default identified trusted sources and verification services as official information in the country pages for all ENIC-NARIC centres.

Part 3 - Recommendations

7. Recommendations

This chapter formulates recommendations for ENIC NARIC centres and the ENIC NARIC Networks.

A core mandate of all ENIC centres is to support the implementation of the Lisbon Recognition Convention in the national context. Therefore, centres should be prepared to be able to advise what and how digital solutions can support the implementation of the Lisbon Recognition Convention in their national context.

ENIC-NARIC centres

- The Lisbon Recognition Convention states that all applicants have the right to a fair assessment and therefore ENIC-NARICs should facilitate the acceptance of digital data in their countries;
- Reserve funds to transfer a more digital system, and train staff accordingly;
- Be prepared to possibly change the role of the credential evaluator over time if more steps in the credential evaluation process are automated. This may shift the 'manual labor' normally executed during credential evaluations to supervising the execution of a technological and methodologic knowledge during an intensive process;
- Be prepared that the role of the ENIC-NARIC centre in the national context may also change, even for those centres that do not make any evaluations. Knowledge on the implementation of technical solutions in line with the Lisbon Recognition Convention may become increasingly necessary;
- When designing/choosing a database/system, make sure you:
  - Comply with international and national regulations;
  - Design the database or system so that you act in line with the Lisbon Recognition Convention. Take the EAR manual as a starting point to verify;
    You can also ask other centres for help, to make sure you can learn from their implementation process;
- Prepare yourself for ongoing digitization, and the fact that not keeping up to speed may disadvantage your students and higher education institutions;
- Legal framework. Given the developments towards digital student data, ENIC-NARIC centres are advised to review their national legislation and discuss with the appropriate legal authority how the legal framework can be adapted so that digital student data can be accepted. In case difficulties are encountered, it is recommended to report this to the Lisbon Recognition Convention Committee and ENIC-NARIC Networks (EB/NAB) to see whether support to a solution and/or a supranational solution can be found;
- Quality assurance processes. Whereas quality assurance processes of the credential evaluation process are currently focused on the workflow, it may be that when steps in the process are digitized, these steps need to become part of the quality assurance to ensure that the workflow is in line with the principles as laid down in the Lisbon Recognition Convention. Instead of describing what principles the credential evaluator adheres to, it should describe what principles the database or system follows.

The ENIC NARIC Network

- Advocate for basic principles to stakeholders, such as open and common standards and services that are public;
- ENIC-NARICs may together wish to support the development of industrial standards, since individual ENIC-NARIC offices may be too small to gear their digital systems to receive digital student data in a multitude of standards (this may be technically difficult to impossible and financially not feasible);
- Start a dialogue with stakeholders to identify the 'low hanging fruit' for making student data digital (actions that can be relatively easy be achieved);
- Ensure that databases and systems operate following the good practice of the Lisbon Recognition Convention (i.e. as formulated in the EAR manual), especially when they become smarter;
- ENIC-NARIC centres monitor and share developments related to the digitization of student data and credential evaluation in the national context and share good practices with the Networks;
- Trusted sources. It may be useful for the ENIC-NARIC Networks to identify what the specific trusted sources are for the required information to make a credential evaluation, and to start a dialogue to make this information available for credential evaluation. This should be done both on national and international level;
- The ENIC-NARIC Network may explore how digitization could serve policy objectives for fair and smooth recognition, such as portability of recognition decisions and automatic recognition.

Colofon

Acknowledgements:

- Nuffic (Coordinator) - The Dutch organisation for internationalisation in education
- Archimedes Foundation
- Centro Informazioni Mobilita Equivalenze Accademiche (CIMEA)
- Canadian Information Centre for International Credentials (CICIC)
- France Education International
- Groningen Declaration Network (GDN)
- Norwegian Agency for Quality Assurance in Education (NOKUT)
- Polish Agency for Academic Exchange (NAWA)
- Swedish Council for Higher Education
- Directorate for ICT and joint services in higher education and research (UNIT)

Cover

Nuffic image bank

Nuffic Kortenaerkade 11 2518 AX The Hague
PO Box 29777 2502 LT The Hague, The Netherlands
Tel: +31 (0)70 4260 260 www.nuffic.nl/en