



an **NTT DATA** Company



## **Workshop | European framework for digitally-signed credentials**

Minutes



Workshop organised within the framework of the project  
'Support for business analysis of Europass2'

## List of abbreviations

<b>API</b>	Application Programming Interface
<b>DLV</b>	Deliverable
<b>DSC</b>	Digitally-signed credential
<b>EC</b>	European Commission
<b>EDCI</b>	Europass Digital Credentials Infrastructure
<b>eID</b>	Electronic Identification
<b>ENIC-NARIC</b>	European Network of Information Centres - National Academic Recognition Information Centres
<b>EQF</b>	European Qualifications Framework for Lifelong Learning
<b>ESCO</b>	European Classification of Skills, Competences, Qualifications and Occupations
<b>EU</b>	European Union
<b>HRM</b>	Human Resource Management
<b>LOQ</b>	Learning Opportunities and Qualifications in Europe portal
<b>MS</b>	Member State

## Table of contents

1.	Introduction .....	1
2.	Presentation of the Europass Framework .....	1
3.	Presentation of the objectives of the workshop .....	1
4.	Framework for digitally-signed credentials: objectives, scope & conceptual model .....	2
5.	Europass Digital Credentials Infrastructure (EDCI).....	5
6.	Discussions about the EDCI .....	10
6.1	EDCI Accreditation Database .....	10
6.2	EDCI Credential Standard.....	11
6.3	Trust & Adoption .....	12
7.	Concluding remarks and next steps .....	13

### **ANNEXES**

Annex 1. List of participants

Annex 2. Scenarios for the implementation of the EDCI

Annex 3. Questions for discussion

### *Disclaimer*

The information and views set out in this document do not necessarily reflect the official opinion of the European Commission. Kindly treat this document confidentially.

## 1. Introduction

The expert workshop on a European framework for digitally-signed credentials took place on 6 November 2018. Thirty one participants joined this workshop (on-site and remotely). The list of participants can be found in Annex 1.

## 2. Presentation of the Europass Framework

Catarina Arnaut welcomed the participants and started a round of presentations.

In order to contextualise the scope of the workshop, Martin Le-Vrang briefly presented the Europass framework. Europass dates from 2004. Its portfolio of documents has become a success throughout the years, particularly the Europass CV. Europass has become one of the most visited websites from European institutions. Despite its success, new needs have emerged within this new digital age. For that reason, a new Decision<sup>1</sup> was adopted in April 2018 with the ultimate goal of modernising the Europass framework, the existing services and tools to successfully meet the evolving needs of citizens.

Martin continued by explaining that the Digital Education Action Plan<sup>2</sup> foresees the development of a framework for digitally-signed credentials which, inevitably, plays an important role in the modernisation of Europass. Even though some EU Member States have started initiatives in this field, the action plan highlights the need to take action at a European level. This workshop was thus organised to gather expert input to further develop the European framework of digitally-signed credentials.

## 3. Presentation of the objectives of the workshop

Catarina shared the agenda for the workshop and presented an overview of the Europass business analysis. everis is supporting the European Commission since June 2018 (and for a duration of 13 months) in five main tasks in order to: 1) identify business needs, 2) define solutions and 3) identify requirements for the technical implementation of these solutions. Particularly, the present workshop was organised within Task 1 of the Europass project, which aims at proposing a European framework for digitally-signed credentials.

The objectives of the workshop were also presented and included:

- Presenting the framework for digitally-signed credentials;
- Receiving feedback and gather further expert input on the proposed framework; and
- Validating the proposed framework.

Ultimately, the present workshop sought to further discuss, validate and get feedback on the proposed European framework for the digitally-signed credentials.

---

<sup>1</sup> DECISION (EU) 2018/646 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC. Last accessed on 07/06/2018 at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D0646&qid=1528377899596&from=EN>

<sup>2</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Digital Education Action Plan {SWD(2018) 12 final} (COM(2018) 22 final). Last accessed on 07/06/2018 at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN>

## 4. Framework for digitally-signed credentials: objectives, scope & conceptual model

The proposed European framework for digitally-signed credentials builds on inputs gathered during an expert workshop held on 4 June 2018 which brought together some stakeholders that have set up their own initiatives in this field.

In order to set the context of the framework, Catarina shared the following definition of digitally-signed credentials:

---

*Digitally-signed credentials are electronic documents which are awarded by qualified bodies to individuals to confirm and provide proof of their learning outcomes achieved in formal, informal and non-formal settings. We may often refer to them as 'digital certificates' as well.*

---

She went on to present the **objectives** and **scope** of the framework.

The framework aims at:

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

The framework has been designed to:

- Recognise learning outcomes achieved in formal, informal and non-formal settings from a lifelong perspective;
- Use a credit-based framework to allow for flexibility in documenting and acknowledging learning achievements from different contexts;
- Embed well-established classifications and credit systems at European level;
- Be based on open standards;
- Secure personal data; and
- Be made available for free to foster its easy and flexible adoption.

Afterwards, Catarina briefed the participants about the **conceptual model** that has been developed for the framework for digitally-signed credentials.

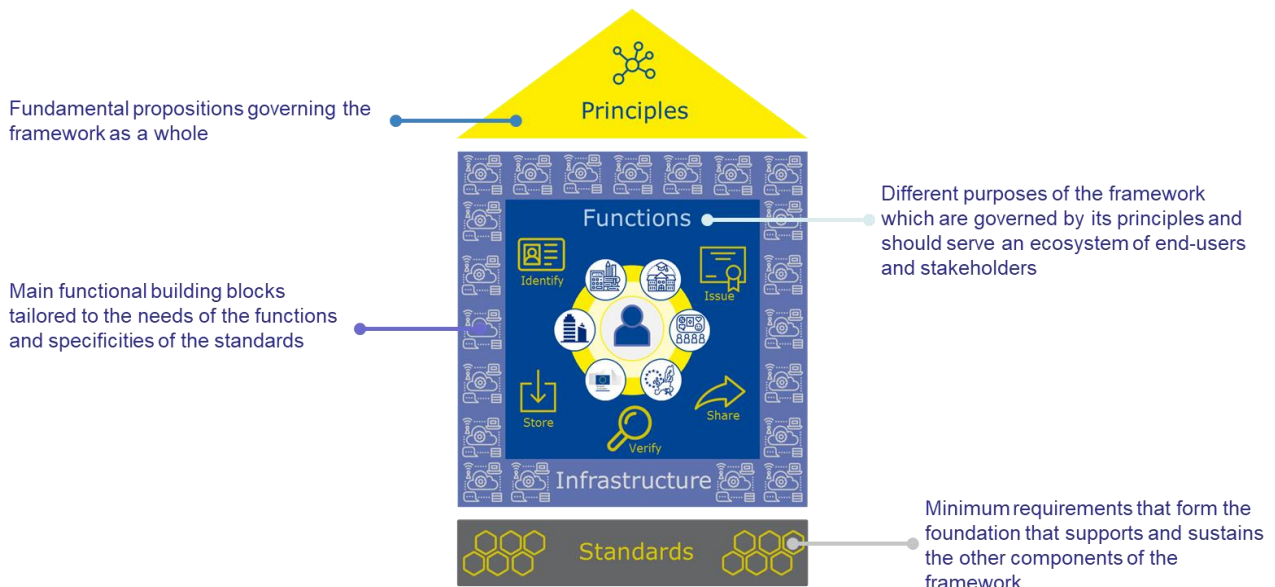


Figure 1. Conceptual model for a framework for digitally-signed credentials

Her presentation particularly focused on two components of the framework, namely the principles and functions.

Ten **principles** have been defined for the framework and are summarised in the figure below.



Figure 2. Principles governing the European framework for digitally-signed credentials

The conceptual model defines five main **functions** of the framework which are:

- **Identify** the individual who is going to be awarded a credential documenting her/his skills, competences or qualifications;
- **Issue** a digitally-signed credential or a revocation certificate to an individual;
- **Store** a digitally-signed credential after having been issued by an awarding body;
- **Share** a digitally-signed credential with an employer or other organisations; and



- **Verify** the authenticity of the digitally-signed credential that has been willingly shared by an individual with an employer or other organisations. The accreditation of the awarding body could also be verified.

In order to exemplify these functions, they have been depicted in the figure below.

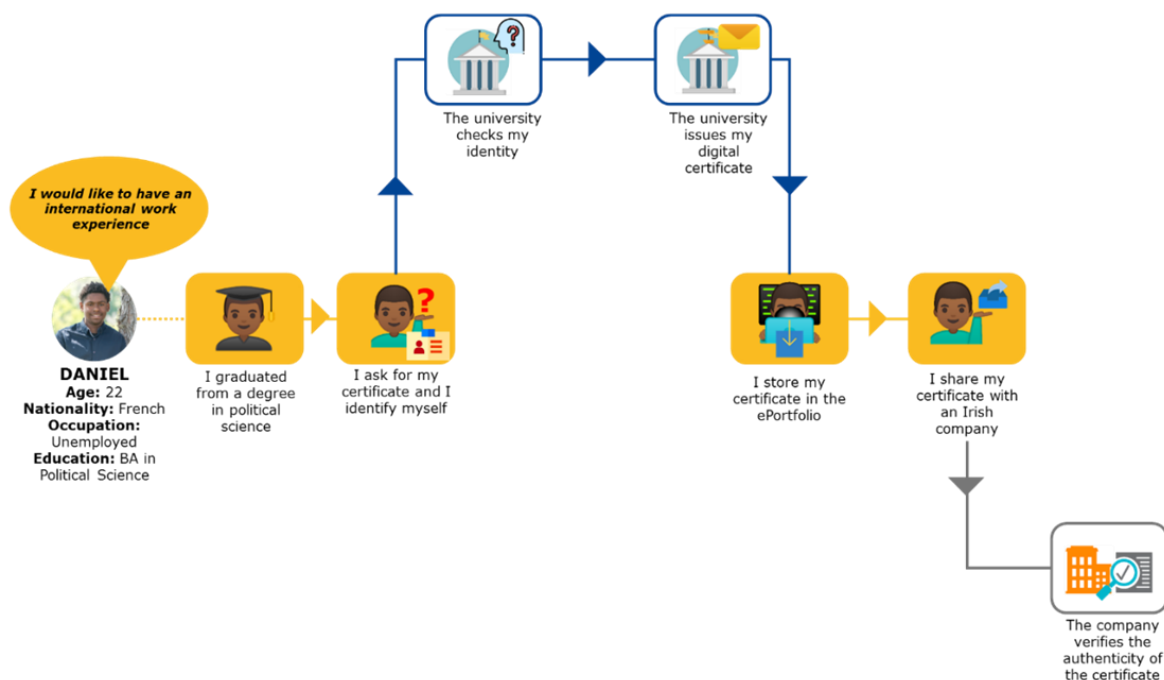


Figure 3. User story depicting the functions of the European framework for digitally-signed credentials

After the presentations, participants were invited to provide feedback and ask questions about the presented framework. Some of the issues raised are listed hereafter:

- **Reassess if digitally-signed credentials should be understood as documents.** The current definition refers to credentials as *electronic documents* but this term might not be the most appropriate. Looking at other companies such as Google, they are not talking about documents, but about *data*. The two concepts are very different and it was suggested that digitally-signed credentials should be understood as data because we are sharing proof of data; and
- **Reassess the current use of the term digital certificates.** The term *digital certificates* is very well-established by now. However, the way it is being used in the context of this framework conflicts with the same term in other contexts, in particular, the eIDAS regulation. In this sense, it is necessary to rethink the use of this term and how it may conflict with other existing definitions.

everis will carefully analyse these comments and consider them in future developments and discussions.

## 5. Europass Digital Credentials Infrastructure (EDCI)

To provide a more in-depth understanding of two other components of the conceptual model (i.e. the infrastructure and the standards), Anthony Camilleri presented the European Digital Credentials Infrastructure (EDCI). He started by defining three **types of credentials** that can be issued using the EDCI: 1) accredited qualifications, 2) non-accredited qualifications and 3) records of experience.

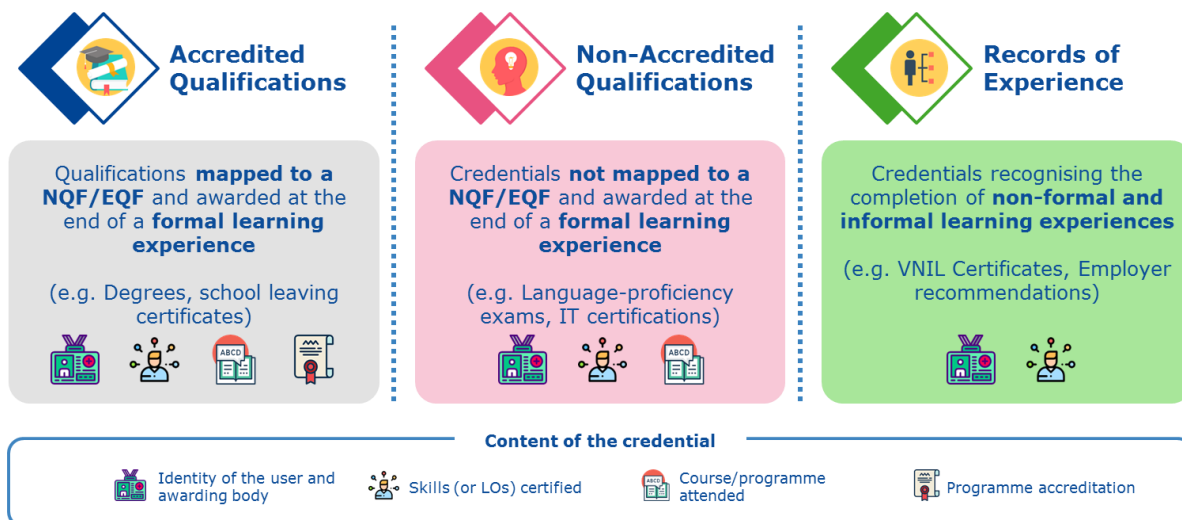


Figure 4. Types of credentials

Then, Anthony steered his presentation into explaining the core building blocks that will help operationalise the framework, namely:

- eIDAS;
- Standards;
- Services; and
- Software.

For each building block, Anthony introduced the components that will be a part of the EDCI and outlined the main interactions between them as summarised in the figure below.



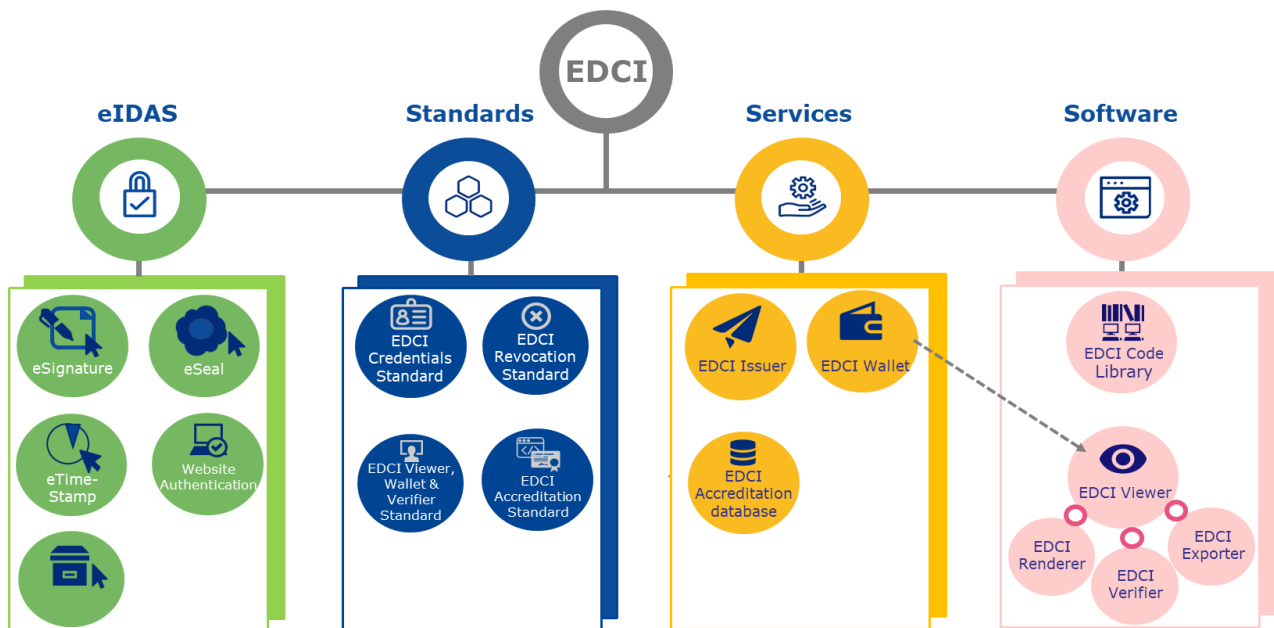



Figure 5. Overview of the main components of the EDCI



Afterwards, focusing on the five functions (identify, issue, store, verify and share), Anthony went on to present three **scenarios for the implementation of the EDCI** (see annex 2), in particular:

- Today: Paper-based;
- Full EC Dependence; and
- Minimal EC Dependence.


Participants were invited to ask questions and provide feedback on the presented infrastructure. The main topics, comments and questions of the discussion are listed hereafter.



Topic	Comments and Questions
<p><b>Openness Interoperability Reusability</b></p> 	<ul style="list-style-type: none"> <li>• Participants noted that openness and interoperability are key, but there is a need to further analyse the relationship between Open Badges, ESCO, EQF, among others. It is important to re-use existing standards and systems as much as possible. <b>How will they be connected?</b> <ul style="list-style-type: none"> <li>○ Current procedures need to be fully compatible with the EQF. In fact, EQF and ESCO are mentioned in the new Decision<sup>3</sup> that sets out the legal basis for Europass and therefore should be considered. Others are being discussed.</li> <li>○ ESCO, LOQ, eIDAS building blocks etc. are already being analysed. We have yet to identify a universal unit of learning and explore other existing options. Furthermore, all of them have their limitations that should also be accounted for. We are nevertheless aiming for maximum compatibility with existing standards and services, and will re-use these wherever possible.</li> <li>○ DIDs have been rejected due to incompatibility with eIDAS infrastructure.</li> </ul> </li> </ul>


<sup>3</sup> DECISION (EU) 2018/646 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC.

Topic	Comments and Questions
<p data-bbox="209 454 357 479"><b>Blockchain</b></p> 	<ul style="list-style-type: none"> <li data-bbox="448 241 1257 266">• <b>Why is Blockchain the ideal technology for this system?</b> <ul style="list-style-type: none"> <li data-bbox="480 293 1445 349">○ Blockchain meets the needs of the infrastructure. Blockchains are 1) immutable and 2) decentralised.</li> <li data-bbox="480 376 1445 499">○ Accreditation records should be available in perpetuity and therefore this is an appropriate technology. They are also awarded in a decentralised fashion, but need to be trusted throughout the European Education Area, therefore in such a case the technology reflects the reality.</li> <li data-bbox="480 526 1445 582">○ Blockchain can help to solve trust issues in particular in respect to the proportionality and subsidiarity principles that regulate the EDCI.</li> </ul> </li> <li data-bbox="448 609 954 633">• <b>How open will the Blockchain be?</b> <ul style="list-style-type: none"> <li data-bbox="480 660 1238 685">○ The Blockchain will allow for private write and public read.</li> </ul> </li> <li data-bbox="448 712 1294 736">• <b>Will the blockchain be used to issue and store credentials?</b> <ul style="list-style-type: none"> <li data-bbox="480 763 1445 846">○ There is no intention to build this solution. However, as long as the implementation is eIDAS-compliant, there is nothing to exclude this being used to issue and store credentials by private providers.</li> </ul> </li> </ul>
<p data-bbox="193 987 376 1077"><b>Third country nationals and refugees</b></p> 	<ul style="list-style-type: none"> <li data-bbox="448 887 1445 943">• <b>How will the EDCI services work for non-European citizens? How will non-European credentials be recognised?</b> <ul style="list-style-type: none"> <li data-bbox="480 969 1445 1052">○ According to the Decision<sup>4</sup>, Europass services should support the integration of third country nationals (including refugees). In these cases, accreditation still needs to go through national processes.</li> <li data-bbox="480 1079 1445 1135">○ Refugees could have their qualifications recognised by ENIC-NARIC networks, and then effectively re-issued by the networks.</li> <li data-bbox="480 1162 1445 1285">○ Foreign networks and already established systems can potentially operate as awarding bodies and integrate their services with Europass. These need to be considered as a special case of issuers. Foreign qualifications are recognised by ENIC-NARIC Centres.</li> </ul> </li> </ul> <p data-bbox="432 1301 1066 1326"><i>Both issues will be further discussed and developed.</i></p>

<sup>4</sup> DECISION (EU) 2018/646 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 April 2018 on a common framework for the provision of better services for skills and qualifications (Europass) and repealing Decision No 2241/2004/EC.

Topic	Comments and Questions
<p data-bbox="244 535 323 562"><b>Issue</b></p> 	<ul style="list-style-type: none"> <li data-bbox="448 237 1329 300">• <b>Who will have the power to issue digitally-signed credentials (particularly qualifications)?</b> <ul style="list-style-type: none"> <li data-bbox="480 322 1445 416">○ Since every country has different legislation systems formally matched through EQF, the permission to issue qualifications should be given at Member State level.</li> <li data-bbox="480 439 1445 501">○ One body in each country would be given master permission to issue and would then sub-delegate permission to others.</li> <li data-bbox="480 524 1445 586">○ Institutions will have full liberty (as they have now) to decide how they issue and store qualifications.</li> </ul> </li> <li data-bbox="448 609 1358 669">• <b>What happens with respect to permissions for eSeals within an organisation?</b> <ul style="list-style-type: none"> <li data-bbox="480 692 1445 754">○ This is the responsibility of the awarding body, as per standard practice for eSeals.</li> </ul> </li> <li data-bbox="448 777 1430 804">• <b>Can the EDCI deal with certificates issued across all Member States?</b> <ul style="list-style-type: none"> <li data-bbox="480 826 1445 889">○ There is no such thing as transnational qualifications at this stage. An accredited qualification needs to be accredited in each Member State.</li> </ul> </li> <li data-bbox="448 911 1059 938">• <b>Why does the EDCI need an ECDI-issuer?</b> <ul style="list-style-type: none"> <li data-bbox="480 960 1445 1023">○ The service is required for smaller providers who do not have or will not commission their own software.</li> </ul> </li> </ul>
<p data-bbox="181 1451 384 1478"><b>Authentication</b></p> 	<ul style="list-style-type: none"> <li data-bbox="448 1055 1445 1117">• <b>How will the EDCI deal with cases when authentication cannot be performed through users' national ID?</b> <ul style="list-style-type: none"> <li data-bbox="480 1140 1445 1368">○ It was noted by the participants that there are limitations to using the national ID as a way to authenticate users because there are many cases when it is not possible to authenticate users through their national ID. Some examples given: a diploma is not linked to any national identity; a course does not have a national identity; a user has more than one national identity; people that study abroad have a "temporary identity"; and refugees and other citizens that lost their national identity.</li> <li data-bbox="480 1391 1445 1485">○ Furthermore, participants stated that it is important to look not only to eIDAS but also to what is being developed in the field of multiple identities. User authentication should go beyond just national identity.</li> <li data-bbox="480 1507 1445 1664">○ In reality, the national ID of a user is, by default, the first level of authentication, but the EDCI will allow for other options. Authentication through ID is not mandatory and the system will just say that the check was not performed. Other sources of authentication will be possible such as first name, last name, date of birth etc.</li> </ul> <p data-bbox="432 1686 1214 1713"><i>Meetings with relevant DGs will be set up to further discuss this.</i></p> </li> <li data-bbox="448 1736 1230 1762">• <b>Do you need users' eID in order to issue a credential?</b> <ul style="list-style-type: none"> <li data-bbox="480 1785 1445 1901">○ To issue credentials, the national ID is also not mandatory. All that is needed is some personal data. Where individuals authenticate with their national eID, the system can automatically compare whether they are the true owner of the credentials in their wallet.</li> <li data-bbox="480 1924 1445 2036">○ Personal eID is only used for an optional automatic verification that a student is the intended recipient of a credential they already hold. The matching will be the <i>information contained in the credential</i> with the <i>information contained in their eID</i>.</li> </ul> </li> </ul>

Topic	Comments and Questions
<p><b>Verification</b></p> 	<ul style="list-style-type: none"> <li>• <b>Can anyone verify credentials?</b> <ul style="list-style-type: none"> <li>○ The only way to verify is using the EDCI Verifier.</li> <li>○ However, anyone can download the verifier software and do it themselves (although it is not the recommended way).</li> </ul> </li> <li>• <b>Which parts of the workflow in the EDCI should include verification of the authenticity of the digital credential?</b> <ul style="list-style-type: none"> <li>○ Verification checks should happen both when credentials are stored on the wallet and when they are shared. Following the assumption that the user does not know if their credential is “real”, verification upon storage can help avoid diploma mills. Diploma mills and sub-standard qualifications are a serious problem.</li> <li>○ It is important to take into account situations where ministries or companies may want to verify large batches of credentials.</li> </ul> </li> </ul>
<p><b>Privacy &amp; Consent</b></p> 	<ul style="list-style-type: none"> <li>• <b>How do you manage consent with respect to the EDCI?</b> <ul style="list-style-type: none"> <li>○ The Accreditation database contains public information. Everything else in the system only happens with data owners’ explicit consent.</li> <li>○ The wallet will give users the chance to decide what information to share, with whom and for how long (e.g. share public profiles through different URLs).</li> <li>○ A limitation that was pointed out was that if the employer leaks the URL everyone will be able to see it. There is no intention to use zero knowledge proofs.</li> <li>○ Furthermore, by giving users the chance to send documents by e-mail (the EDCI allows delivery by e-mail or by secure delivery direct to the person's EDCI Wallet) that information becomes public and others can access it. These issues should be accounted for.</li> </ul> </li> </ul> <p><i>A decision has yet to be made in regards to how granular the permissions to share personal data will be.</i></p>
<p><b>Scalability</b></p> 	<ul style="list-style-type: none"> <li>• <b>Is the solution scalable?</b> <ul style="list-style-type: none"> <li>○ Participants noted that the current conceptual model may have some scalability issues as it aims to create a database of records of every possible credential (even from outside Europe). This issue needs to be considered and discussed.</li> <li>○ On the other hand, to say that credentials will be indefinitely stored in the wallet also raises some scalability issues.</li> </ul> </li> </ul> <p><i>These issues will be further discussed and developed.</i></p>
<p><b>Accreditation of qualifications</b></p> 	<ul style="list-style-type: none"> <li>• <b>Who runs the EDCI Accreditation database?</b> <ul style="list-style-type: none"> <li>○ It is still undetermined. Ideally, each Member State (or other authorities at regional level) should run a node.</li> <li>○ Non-accredited qualifications should be given a more positive name.</li> </ul> </li> </ul>

Topic	Comments and Questions
<p data-bbox="181 331 387 360"><b>Time-stamping</b></p> 	<ul style="list-style-type: none"> <li data-bbox="448 241 1437 271">• <b>Should EDCI use eIDAS time-stamping or blockchain time-stamping?</b> <ul style="list-style-type: none"> <li data-bbox="480 293 895 322">○ This has not been defined yet.</li> </ul> </li> <li data-bbox="448 338 1102 367">• <b>Will eSeals be valid after certificates expire?</b> <ul style="list-style-type: none"> <li data-bbox="480 389 1445 445">○ As long as the eSeal was valid when the document was sealed, the seal on the document remains valid indefinitely.</li> <li data-bbox="480 461 1382 517">○ Participants noted that it is important to look further into eIDAS time-stamping services.</li> <li data-bbox="480 539 1445 595">○ Furthermore, some organisations issue certificates that only last a couple of years and the EDCI system should take this into consideration.</li> </ul> </li> </ul>

everis will carefully analyse these comments and consider them in future developments and discussions.

## 6. Discussions about the EDCI

In order to discuss the proposed framework for digitally-signed credentials and its EDCI, participants were divided into four working groups. Discussions in groups were steered by a set of questions (see Annex 3). At the end of the activity, each group shared their answers, ideas, challenges and/or suggestions in plenary.

### 6.1 EDCI Accreditation Database

The first discussion focused on the EDCI Accreditation Database. In particular, it aimed to gather input on 1) reasons to develop a joint tool, 2) the most efficient way to collect data based on current systems and 3) the advantages and disadvantages of using blockchain.

During this exercise, participants identified **needs** that must be properly addressed in order to foster the success of the EDCI Accreditation Database. In particular, the database should:

- Have a clear governance model;
- Be able to capture changes over time;
- Transform existing information through automated processes;
- Register information once;
- Incorporate quality assurance requirements: machine readable format for public data;
- Embrace a broader definition of education, in particular, include lifelong learning and non-formal learning;
- Decouple the writing of data and verification process from EC acceptance; and
- Avoid centralisation.

Regarding the **collection of data** for the EDCI Accreditation Database, participants were invited to comment on current systems and suggested the following:

- The approach and solution will differ in accordance with Member States' systems. For example, some Member States currently do not have an accreditation database. In that case, funding should be provided;
- Each nation state should be delegated write access by the European Commission;

- There is openness to use APIs by Member States;
- An EC central system is not feasible but the database should in some way linked to national databases (there would be no real damage if national databases were destroyed); and
- Scraping is also technically not feasible as it relies on other websites and it is prone to arbitrary changes that may happen to the Member States' websites.

**Blockchain** has been proposed as the ideal technology for the EDCI Accreditation Database system due to decentralisation and immutability. Participants were invited to comment and provide feedback on this choice. In particular, it was suggested that if blockchain is used it should:

- Be used to verify eSeals;
- Include a layer for verification; and
- Include accreditation, authority and identity checks.

Furthermore, it was agreed that blockchain brings a layer of openness and subsidiarity but that despite its advantages, other evolving standards should also be discussed and not completely discarded.

## 6.2 EDCI Credential Standard

Participants were invited to provide suggestions of existing standards that should have formal mapping and be compatible with the EDCI Credential Standard in order to foster its adoption. During this exercise, they collectively recognised that existing standards should be reused as much as possible. The suggested standards are summarised below.

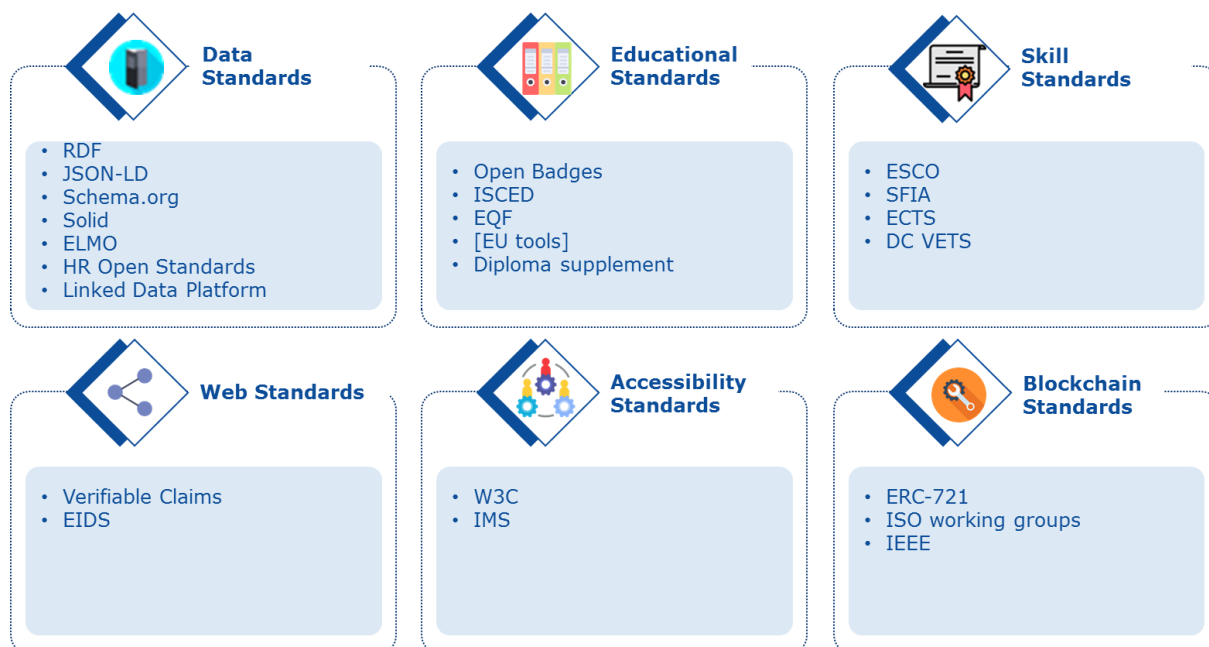


Figure 6. Existing standards that should be considered

Afterwards, participants shared ideas and suggestions on how to **ensure a widespread adoption** of the EDCI Credential Standard, including:

- Release the standard with mapping (different scenarios should be mapped out);
- Pilot with a few universities;
- Add legacy systems;
- Align with a several parties to minimise effort;
- Have EQF as a minimal core;
- Provide the necessary funding; and
- Promote adequate marketing campaigns, for example, organise workshops with stakeholders, talk directly to major players, utilise the Europass network at national level for direct contact with country-level major players etc.

### 6.3 Trust & Adoption

The last discussion focused on the topics of trust and adoption of the presented infrastructure. Participants were invited to share their opinions on the best way to ensure **trust** in the verification results. In particular, they were invited to comment the following options: 1) only allow the EC and/or Member States to run wallet and verification software and 2) create a certification infrastructure for verification software. The main outcomes were presented in plenary, including:

- The promotion of openness and decentralisation;
- Every Member State should get its own private key and should have its own certification infrastructure; and
- Blockchain should be used itself as a trust mechanism to cancel fraud. More specifically, each Member State (or each certification software) should have write-access to the blockchain.

Furthermore, one participant identified avenues for fraud and misuse in the presented infrastructure, in particular:

- Potential misuse of private keys, specifically those allowing private companies to use Member States' private key. The existence of different national views on trust over private keys and companies increases this risk; and
- The emerging marketplace over the data in blockchain and accreditation ranking systems.

Afterwards, participants were invited to foresee **adoption** issues and the main suggestions were to 1) focus on issuers first to have an initial basis of credentials issued and available in the EDCI format and 2) make a business case for industry players (e.g. Why should they care?; What's in it for them?) and pursue direct contact at a high level.

The proposed approach to self-sovereignty encompasses: 1) credentials that are user-held, -controlled and -owned, which are storable on any device, 2) dependencies on EU/Member States infrastructure for verification and 3) no dependencies on proprietary software, private companies or other closed infrastructures whatsoever. Participants were invited to comment on whether this approach reaches the appropriate **balance between trust and convenience**. The main ideas discussed include:

- Overall agreement with 1) and 3);



- The approach should consider PDF as a format that combines visual (user-friendly) presentation of the data, holds structured data (e.g. as XML/JSON attachment, in the simplest case) and digital signatures. The PDF standard is quite open, and several tools and libraries exist to manipulate it;
- All the action is in 2) and it depends on the authority that has signed (and then can be checked); and
- Convenience should be prioritised over trust (the optimal choice is not a 50/50 balance) if a quicker user adoption is desired especially in the start.

## **7. Concluding remarks and next steps**

Overall, the presented framework received positive reactions from the experts. Some important issues were raised and everis will take them into consideration to improve the proposed framework. On the one hand, there is a need to rethink the definition of digitally-signed credentials, look further into eIDAS, address concerns regarding scalability and further develop the argument of why blockchain is the best solution. On the other hand, it is important to not forget about the needs of people outside Europe, embrace lifelong learning and non-formal learning, audit how private keys are used and assess how Member States will show that they are using the standards to get a private key.

As for next steps, the European framework for digitally-signed credentials will be further developed. More high-level discussions will take place with the Advisory Groups of Europass and EQF. In addition, outreach actions will also be organised in order to engage Member States and other organisations that may be interested in implementing the EDCI.

# ANNEXES

## Annex 1. List of participants

<b>Name</b>	<b>Surname</b>	<b>Organisation</b>
Catarina	Arnaut	everis, Belgium
Armand	Beuvens	Arhs, Belgium
Oscar	Burgos	DG DIGIT
Anthony	Camilleri	Knowledge Innovation Centre, Slovenia
Pedro	Chaves	DG EMPL
Michael	De Boer	DG DIGIT
Daniel	De Seuil	Vlaamse overheid
Angeliki	Dedopoulou	DG EMPL (everis), Belgium
John	Domingue	Knowledge Media Institute of the UK Open University, UK
Fiona	Fanning	Pearson
Paula	Ferreira	Direção-Geral de Estatísticas da Educação e Ciência Ministry of Education, Portugal
Kieran	Gilmurray	Pearson
Alexander	Grech	Commonwealth Centre for Connected Learning, Malta
Bert	Jehoul	Open Knowledge, Belgium
Jonna	Korhonen	Europass AG
Martin	Le Vrang	DG EMPL, Belgium
Soulla	Louca	University of Nicosia, Cyprus
Panos (Panagiotis)	Louridas	Greek Research and Technology Network
William	O'Keefee	DG EMPL, Belgium
Rita	Pereira	everis, Belgium
Carles	Perez	everis, Belgium
Wolfgang	Prinz	Fraunhofer Institute for Applied Information Technology FIT, Germany
Graeme	Robertson- Liersch	DG Education, Youth, Sport and Culture
Athanassios	Siaperas	Cedefop, Greece
Nikos	Triantafyllou	University of the Aegean
Colin	Tuck	EQAR, Brussels

<b>Name</b>	<b>Surname</b>	<b>Organisation</b>
Julia	Turon	everis, Belgium
Erik	Van Den Broek	Europass AG
Pierre-Henri	Vandevelde	Arhs, Belgium
Geir Magne	Vangen	Oslo, Norway
Dimitris	Zacharopoulos	Aristotle University of Thessaloniki

## Annex 2. Scenarios for the implementation of the EDCI

### Identify

#### Today: Paper-based



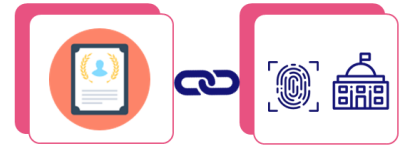
The credential states the identity of the awarding body and credential owner

#### Full EC Dependence



The digitally-signed credential is linked to the identity of the awarding body, such that only the awarding body may issue such a credential

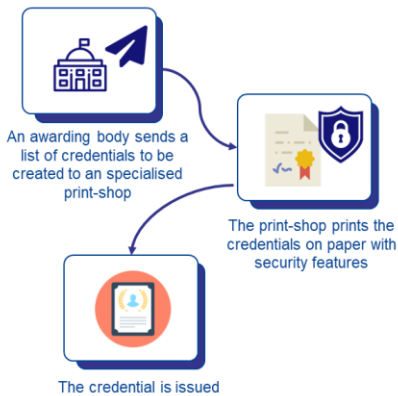
#### Minimal EC Dependence



The digitally-signed credential is linked to the identity of the awarding body, such that only the awarding body may issue such a credential

### Issue

#### Today: Paper-based

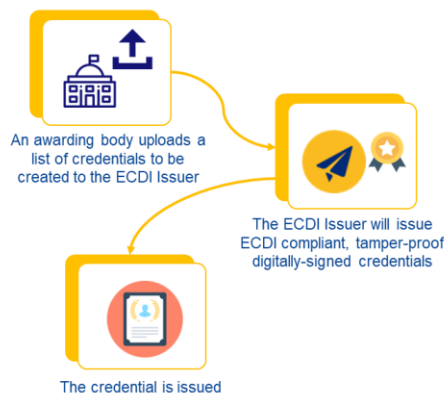


An awarding body sends a list of credentials to be created to a specialised print-shop

The print-shop prints the credentials on paper with security features

The credential is issued

#### Full EC Dependence

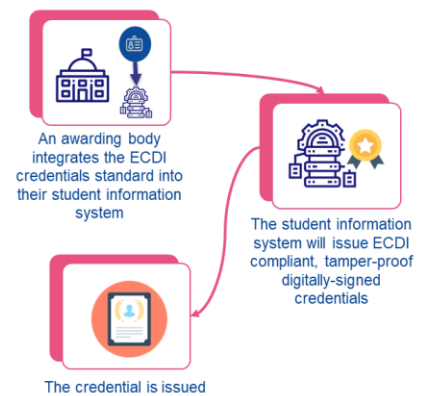


An awarding body uploads a list of credentials to be created to the ECDI Issuer

The ECDI Issuer will issue ECDI compliant, tamper-proof digitally-signed credentials

The credential is issued

#### Minimal EC Dependence



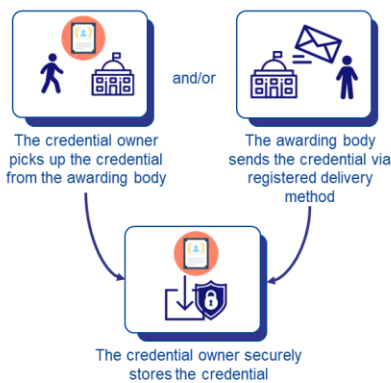
An awarding body integrates the ECDI credentials standard into their student information system

The student information system will issue ECDI compliant, tamper-proof digitally-signed credentials

The credential is issued

### Store

#### Today: Paper-based

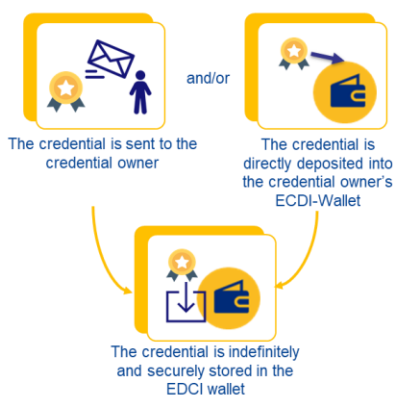


The credential owner picks up the credential from the awarding body

The awarding body sends the credential via registered delivery method

The credential owner securely stores the credential

#### Full EC Dependence

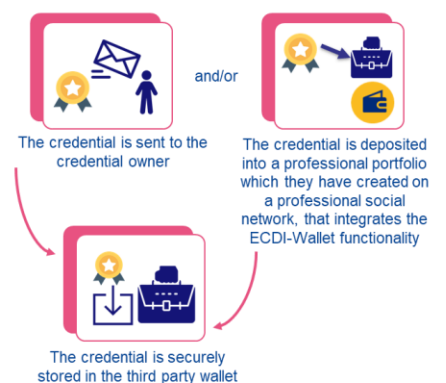


The credential is sent to the credential owner

The credential is directly deposited into the credential owner's ECDI-Wallet

The credential is indefinitely and securely stored in the ECDI wallet

#### Minimal EC Dependence



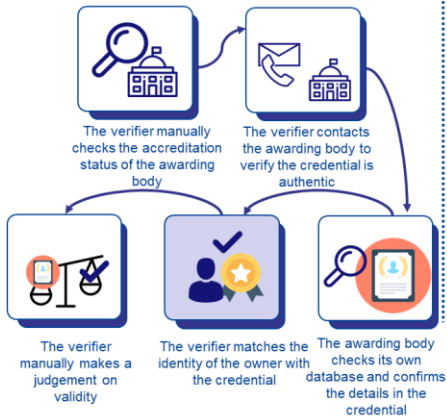
The credential is sent to the credential owner

The credential is deposited into a professional portfolio which they have created on a professional social network, that integrates the ECDI-Wallet functionality

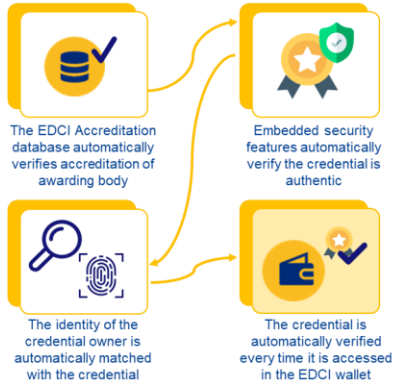
The credential is securely stored in the third party wallet

## Verify

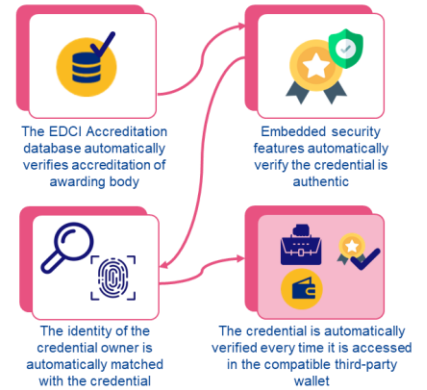
### Today: Paper-based (manual verification)



### Full EC Dependence (automatic verification by EC hosted wallet)

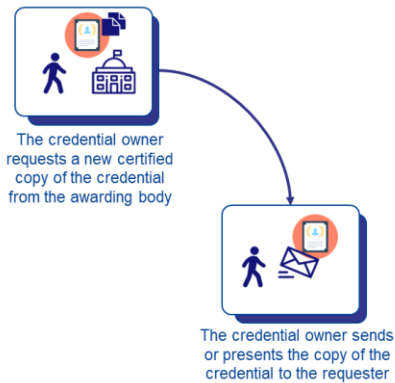


### Minimal EC Dependence (automatic verification by compatible third party wallet)



## Share

### Today: Paper-based



### Full EC Dependence



### Minimal EC Dependence



## Annex 3. Questions for discussion

### 1. EDCI Accreditation Database

The EDCI Accreditation Database proposes that Member States gather information on qualifications at European level so as to combat the threat of diploma mills and sub-standard providers. Is this a sufficient reason for a joint tool?

What is the most efficient way to collect these data based on current systems:

- Scraping existing databases (if so, what is the most efficient way to scrape?)
- Requesting information from Member States (submission of lists of qualifications periodically in a structured format)?
- Creating an API for Member States to submit and for the accreditation database to receive data?
- Replacing national databases with an EC-operated system?
- A combination of the above?

Blockchain has been proposed as the ideal technology for this system due to (a) decentralisation and (b) immutability. Do you see advantages or disadvantages of this choice?

### 2. EDCI Credential Standard

The EDCI proposes creating a new standard comprised of a metadata standard for a unit of learning as other standards are either too general (Open Badges, LOM) or limited to certain types of learning experiences (ESCO, EQF). Which existing standards should we ensure formal mapping and compatibility with to improve adoption?

What is the best way to ensure widespread adoption of such standard?

### 3. Trust & adoption

To ensure trust in the verification results, two options can be considered:

- Only allow the EC and/or Member States to run wallet and verification software, or
- Create a certification infrastructure for verification software.

*Which do you think is most feasible and why?*

Can you identify any avenues for fraud or misuse in the infrastructure as presented?

What adoption issues do you foresee for:

- Issuers integrating EDCI-Issue functionality into their student information systems?
- Operators of professional social networks in integrating EDCI-Wallet functionality?
- Makers of HRM systems in integration of EDCI-Verifier functionality?

Our proposed approach to self-sovereignty encompasses:

- Credentials that are user-held, -controlled and -owned, which are storable on any device.
- Dependencies on EU/Member States infrastructure for verification.
- No dependencies on proprietary software, private companies or other closed infrastructures whatsoever.

*Do you believe this approach reaches the appropriate balance between trust and convenience?*