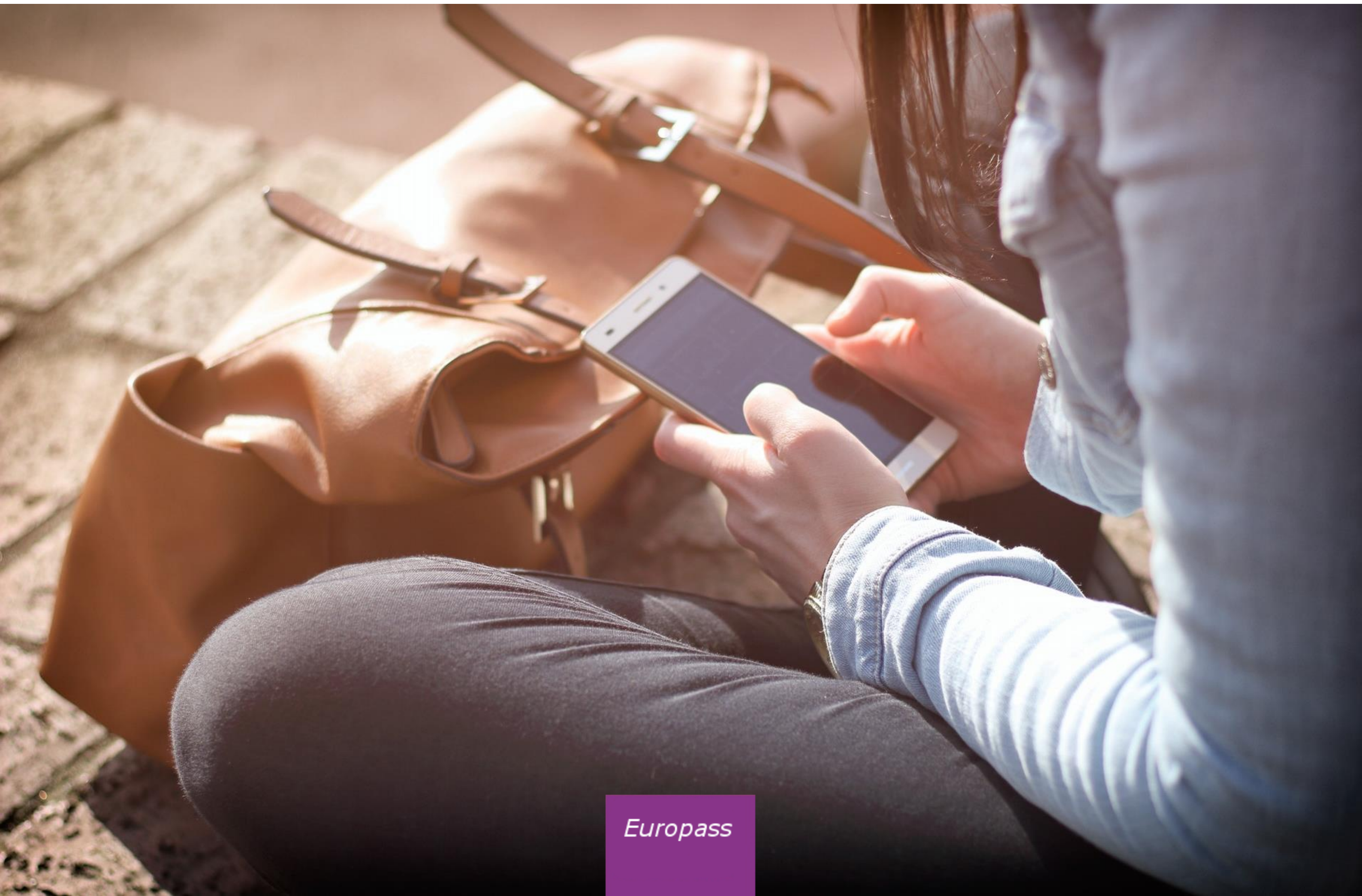
EPASS AG 1-6

No more papercuts

Digitally Signed Credentials in the new Europass

Document for the
1st meeting of the Europass Advisory Group
28 September 2018



1 Purpose of the document

The Commission is developing a technical framework for digitally-signed credentials while developing Europass. In this document the Commission describes the overall approach and next steps in order to start a discussion on the matter with the Europass Advisory Group.

Members of the Europass Advisory Group who are interested to be involved more closely in shaping and testing the approach are invited to express their interest.

2 Background

The new Europass Decision outlines the importance of authentication measures to support the verification of digital documents on skills and qualifications:

> *Europass shall support authentication services for any digital documents or representations of information on skills and qualifications.*
>
> *Article 4(6) Europass Decision*

In January 2018 the Commission adopted the Digital Education Action Plan[1] with the goal to support technology-use and digital competence development in education and announced the work on digitally-signed qualifications:

> *Provide a framework for issuing digitally-certified qualifications and validating digitally-acquired skills that are trusted, multilingual and can be stored in professional profiles (CVs) such as Europass. The framework will be fully aligned with the European Qualifications Framework for Lifelong Learning (EQF) and the European Classification of Skills, Competences, Qualifications and Occupations (ESCO).*
>
> *Action 3 of the Digital Education Action Plan*

Both policy initiatives highlight the importance of digital infrastructure and tools to document, share and verify learning achievements (including skills and qualifications).

In this context, digitally-signed credentials[2] are electronic documents which are awarded by organisations to individuals to confirm and provide proof of their learning outcomes. A European technical framework for issuing digitally-signed credentials ensures that digital qualifications issued in one Member State can be understood and verified in any other. The technical approach to be designed for the framework will allow for identifying, issuing, storing, sharing and verifying digitally-signed credentials.

The Europass online platform is expected to support the implementation of this framework by offering, among others, the possibility to store and share digitally-signed qualifications. In addition, two of the established Europass documents, which describe learning outcomes of an individual (qualifications supplements and Europass Mobility), are signed by issuing organisations and the

[1] 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. (COM(2018) 22 final).

[2] This document uses the term "digitally signed" instead of "digitally certified", but with the same meaning. It also uses the term "credential" to include qualifications, but potentially also other Europass documents that are documenting skills and qualifications and that are signed by an issuing party (such as Europass Mobility).

Europass CV is a representation of information by an individual. Therefore, as part of the modernisation of the established Europass documents as web-based tools, a framework for digitally signing credentials will enable secure, efficient and trustworthy authentication of digital documents on skills and qualifications. The technical framework will not replace quality assurance, accreditation or other national public or private systems but will offer technical solutions that issuers, holders and recipients of digital credentials can use. The technical framework will be built on open standards and be made available for use on a voluntary basis, free-of-charge to users. Initially, the technical framework will focus on qualifications that are part of the formal education and training systems (i.e. qualifications to which Member States assigned NQF levels), and then possibly to international, private or sectoral qualifications, as well as qualification supplements, Europass Mobility or similar documents.

3 Added value

Although a few initiatives have recently emerged in the field of digitally-signed credentials (see annex I for examples), there remains a need to adapt and align current paper-based certificates to the present digital era. Digitally-signed credentials pose challenges related to security, privacy and trust. On the one hand, the personal data of the learner or jobseeker need to be secured. On the other hand, a wide range of stakeholders, such as employers, education and training institutions, public employment services or civil society organisations need to be able to verify the authenticity and validity of certificates. Finally, from a perspective of lifelong learning, individuals should be able to progressively store and share digital certificates which document their skills, competences, qualifications, and practical, mobility and volunteering experiences.

A technical framework could be used by Member States and various stakeholders when issuing digitally-signed credentials to learners. It could for example be implemented in IT systems that awarding bodies use to create diplomas and certificates for students. The technical framework should address the challenges outlined above so that it benefits users in various ways:

- A technical framework for digitally-signed credentials provides a secure, trustworthy and fraud-resistant system that ensures data privacy and data protection.
- A common technical approach for issuing digitally-signed credentials ensures that certificates from one Member State can be understood and verified in any other.
- Learners are able to provide their certificates in electronic format to employers or education providers.
- Employers, education and training providers and other bodies will be able to check that certificates and other qualifications are valid and authentic. They can also have easy access to background information on a certificate or qualification.

4 Guiding principles

When creating the technical framework for digitally-signed credentials, the Commission applies a set of ten principles. They are aimed at underpinning the functions, infrastructure and standards of the framework:

- User-Centricity. A diverse ecosystem of stakeholders will be making use of and/or benefiting from the framework, as well as supporting its implementation. Their needs vary considerably and they should be taken into account when defining the use cases for the framework. In addition, the needs and requirements of distinct stakeholders should be carefully analysed and integrated when designing and developing the infrastructure that allows for identifying, awarding, storing, sharing and verifying a certificate. As such, the infrastructure of the framework should be easy to use for all stakeholders. Lastly, learners and jobseekers should be at the centre of the framework. Their learning achievements trigger the award of a digital certificate, and they control whom to share it with for verification.
- Subsidiarity and Proportionality. The European Union is governed by the principles of subsidiarity[3] and proportionality[4]. The technical framework will therefore focus on areas of clear European added value. This will include in particular a uniform and transparent way of technically issuing credentials that Member States and stakeholders can voluntarily apply so that the digital credentials can be understood throughout Europe. It will exclude the rules and the process of developing curricula, of defining qualifications, and of issuing credentials.
- Inclusion and accessibility. The framework should consider the diversity of learners and jobseekers who are going to be awarded, store and share digital certificates. In addition, it should also take into account the individuals who issue and verify them. Multilingualism is an important feature of the framework as it fosters inclusion by making it possible to understand the content of digital certificates (i.e. recognised skills, competences and qualifications) at EU level. The infrastructure of the framework should be accessible to all individuals (including people with disabilities, elderly and other disadvantaged groups) regardless of their level of digital skills.
- Openness. Considering that the framework is aimed at encouraging the gradual adoption of digital certificates, it should be built on open standards and foster the use of open source software technologies. Such open approaches tend to reduce costs, promote collaboration between different parties, ensure interoperability, and reduce the risk of lock-ins with dominant solution providers, allowing thus for flexibility and freedom.
- Data protection by design and by default. In accordance with the General Data Protection Regulation (GDPR), the framework will ensure the implementation of technical and organisational measures, such as pseudonymisation and data minimisation, in order to collect and process only the strictly necessary personal data for each specific purpose. In particular it aims at limiting the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
- Interoperability. The technical framework will ensure that digitally signed credentials can be processed by various IT systems, as requested by the holder of the credential (while ensuring full compliance with the GDPR). This allows that stakeholders can seamlessly interact with various qualifications platforms, by exchanging information within or outside of the Europass2 ecosystem.

[3] "*Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level*." (Article 5(3) TEU).

[4] "*Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties*." (Article 5(4) TEU).

- Transparency. The infrastructure of the framework should present each end-user and stakeholder the correct information at the right time to allow them to use a digital qualification for its intended purpose. Transparency applies to the standards used for identification, issue, storage, sharing and verification. It implies traceability of how each function is implemented each time it is used, availability of the underlying metadata within a digital qualification and of summative data on the whole system to stakeholders.
- Resilience. The system should continue functioning and reliably offering its services even in the face of adverse conditions. As such, the framework and its infrastructure should be resistant to fraud (i.e. from malicious use of the system for unintended purposes), and ensure data integrity (i.e. protection of data from unauthorised changes due to hacking) and data availability (i.e. ensuring that data are always accessible and are not destroyed by natural disasters, mistakes in technical implementations or hacks).
- Reusability. Existing solutions, specifications, standards and tools developed by others which have proven to be sound, useful and relevant elsewhere should be considered and reused to the extent possible. Furthermore, new solutions, specifications, standards and tools should be further reusable by others in the public interest.
- Qualifications as a Public Good. Awarding qualifications, and recognising and validating the competences and skills of individuals is in the public interest of the EU Member States. The technical infrastructure should therefore take into account that certain qualifications/credentials can only be issued by accredited awarding bodies according to the rules established by the respective Member State.

5 Functions of the framework

The framework for digitally-signed credentials serves a diverse ecosystem of stakeholders. This ecosystem puts learners and jobseekers at its core as the data owners. They will be awarded digital certificates which document their lifelong learning outcomes. This ecosystem is also comprised of organisations which issue digitally-signed credentials (typically education institutions and other awarding bodies), as well as employers and other organisations which need to verify them.

In order to serve the ecosystem of stakeholders, the framework should have five different functions:

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

6 Next steps

Following the adoption of the Digital Education Action Plan and the Europass Decision, the Commission has started to explore potential approaches for implementing the technical framework. In its work the Commission's project team is supported by experts for authentication in electronic systems and for the use of technology in the education and training system.

In June 2018 the Commission organised a first workshop with additional external experts to provide their input to this process. These included leading researchers in the field of distributed ledger technology in education, experts for open badges, and for the use of digital solutions for education in national administration.

In November 2018 the Commission intends to discuss the preferred implementation approach in a second workshop with experts in the field. To this end, the Commission is looking for experts in the following fields:

- National, regional or sectoral projects for issuing digitally signed credentials
- Distributed ledgers in education and training
- Open badges
- Solutions for managing identities in electronic systems, for digitally signing and for revoking documents
- Technical interoperability in education and training
- Data ownership and data protection

Members of the Europass Advisory Group that have expertise in one or more of these fields and that are interested to join the expert workshop are kindly asked to express their interest by e-mail to EMPL-EUROPASS@ec.europa.eu.

The Commission will then present the conceptual model for the Europass digitally-signed credentials at a joint meeting between representatives of the Europass Advisory Group and the EQF Advisory Group in December 2018.

Annex I: Recent initiatives in the field of digitally-signed credentials

This list has been prepared to provide information on existing initiatives in the field of digitally-signed qualifications. The list of initiatives is not intended to be exhaustive and has been completed with information gathered during the months of May and July 2018 through a desk research and interviews with initiative owners.

- ### Open Badges on the Blockchain - Open University UK, Knowledge Media Institute

  Introduction of OpenBadges data related to the OpenLearn web access into a set of Ethereum Smart Contracts, allowing to store the certificates from different sources in the same place.

  http://kmi.open.ac.uk/review/pdf/kmi-review-issue-10-2017.pdf
  https://openbadges.org/about/

- ### UNIC's Blockchain Initiative for academic certificates - University of Nicosia

  Use of Bitcoin blockchain technology to issue electronic PDFs verifiable through UNIC's website verification tool or by replicating UNIC's open-source instructions (available at block.co).

  https://block.co/blockchain-certificates/

- ### Blockchain in education pilots - Government of Malta

  Implementation of a nation-wide pilot project for academic credentialing and professional certifications using Blockcerts open standards, defined by the Malta Qualifications Framework (MQF) and adapted to the European Qualifications Framework (EQF).

  http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/
  https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/September/15/PR172070.aspx

- ### Recipient-owned credentials - The University of Melbourne

  Issuance of a Teaching Certificate using the Learning Machine issuing system based on Blockcerts open standards.

  http://newsroom.melbourne.edu/news/university-melbourne-issue-recipient-owned-blockchain-records

- ### Infrastructure to issue digital certificates - Aristotle University of Thessaloniki PKI

  Issuance of Qualified Certificates for e-Signatures following European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

  https://pki.auth.gr/index.php.en

- **Digital Badge Academy - Sussex Downs**

  Use of Digitalme's Open Badge Academy to showcase skills in a "digital and verifiable way" through endorsements by experts, educators and peers.

  https://www.openbadgeacademy.com/sussexdowns

- **Teacher's badges - Oulu University, partners, and the Ministry of Education of Finland**

  Creation of a new system to be applied across educational sectors which will consist of a shared structure, model, and awarding criteria for badges to recognise the competences of teachers.

  http://www.digital-competences-for-teachers.eu/
  http://www.oppiminenonline.com/

- **Digital Certificates Project - MIT Media Lab Learning Initiative and Learning Machine**

  Development of a system to ensure the management, ownership, transferability, longevity and trust of certificates through tools, software and strategies related to the bitcoin blockchain technology.

  http://certificates.media.mit.edu/

- **Blockchain for education - Fraunhofer Institute for applied information technology**

  Creation of a platform to facilitate certificates management through smart contracts in the Ethereum blockchain.

  https://www.fit.fraunhofer.de/en/fb/cscw/blockchain.html

- **Edubadges - SURF**

  Issuance of micro-credentials that cover both formal and non-formal learning and exploration of the use of blockchain in combination with the Edubadges infrastructure.

  https://www.surf.nl/en/innovationprojects/customised-education/edubadges-and-micro-credentialing.html
  https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/whitepaper-on-open-badges-en-micro-credentials.pdf

- **Lifelong learning competencies on the blockchain - VDAB & GO!**

  Linkage of competencies to individuals through a "bring-your-own-standards" blockchain-based online platform, through which future employers will be able to consult candidates' diplomas but also their skills.

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

- **Badgr - Concentric Sky**

  Use of a free and open source achievement recognition and tracking system to issue, organise, and share Open Badges offered as a service or as an open source.

https://badgr.com/

- Digital Badges - Acclaim

  Issuance of badges compliant with the Open Badge Infrastructure (OBI) metadata, allowing users to store and share their badges in their profile or in other OBI-compliant badge wallets.

  https://www.youracclaim.com/

- Credentials Dashboard - Accredible

  Issuance of certificates and badges that are verified in the platform through third parties or by using blockchain technology.

  https://www.accredible.com/

- IndiaChain - Government of India, Niti Ayog

  Implementation of a blockchain-based solution linked to IndiaStack, a government identification database.

  http://indiastack.org/
  https://www.newsbtc.com/2018/02/06/indiachain-governments-blockchain-based-certification-for-education-degrees/