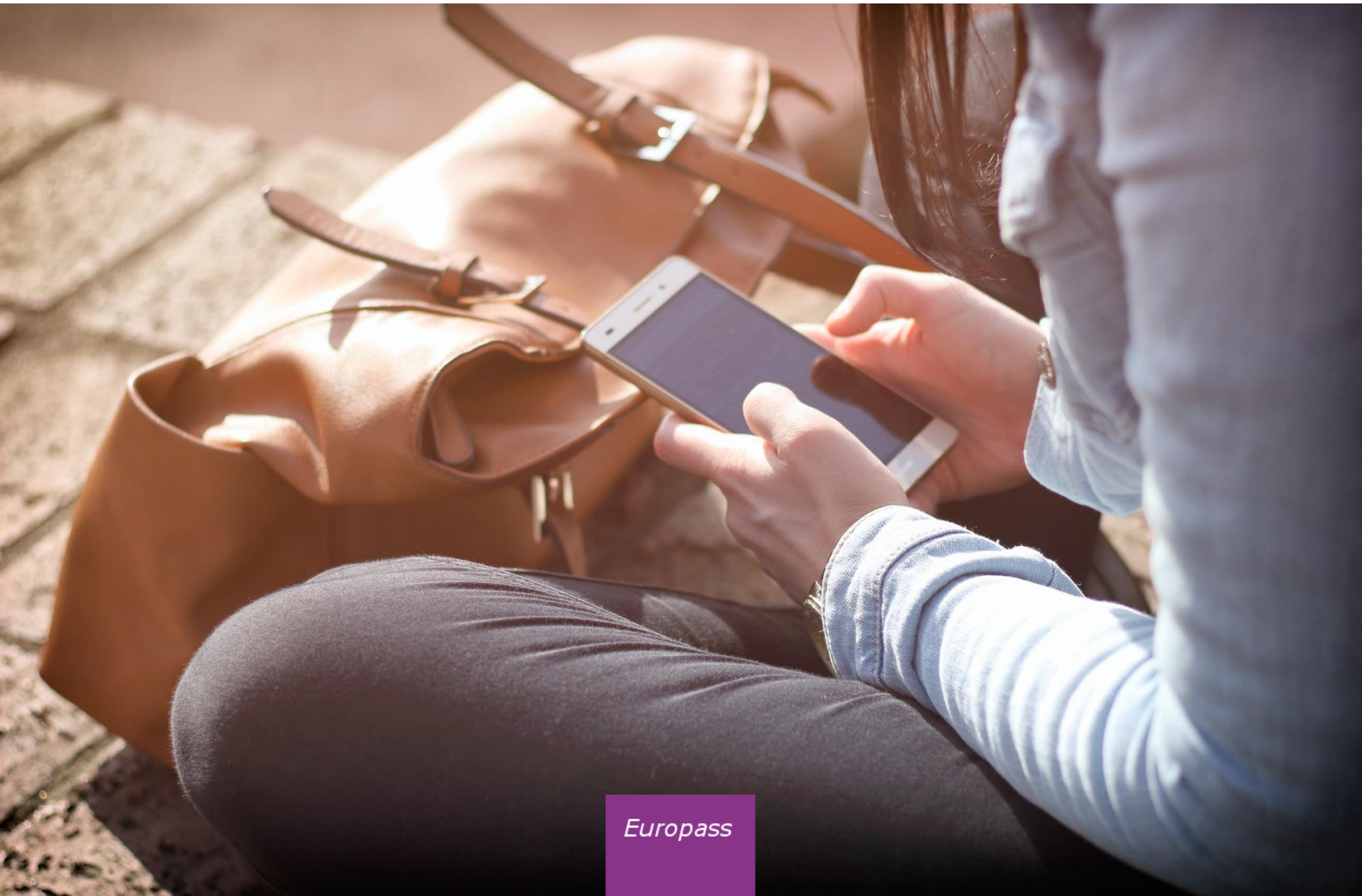
European Commission

JAG1-2

Digitally Signed Credentials

Concept Note

Document for the
Joint Meeting of the Europass Advisory Group and EQF Advisory Group
12 December 2018



1 Purpose of the document

This document describes the working concept for the Europass Technical Framework for Digitally Signed Credentials (hereafter 'the DSC Framework'). The note describes the ***objective, functions, users, types of credentials, rules of use*** and ***development*** of the Framework.

Members of the Europass Advisory Group and EQF Advisory Group are invited to give feedback on the concept.

The note reflects the outcomes of discussions at an expert workshop on digitally signed-credentials held on 6 November 2018 in Brussels.

2 Introduction

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*

Digitally-signed credentials[2] are electronic statements issued by an awarding body to an individual to confirm and provide proof of their learning outcomes. The **objective** of the Europass DSC framework is to enable the easier understanding and verification of qualifications, and other evidence of learning.

The DSC Framework will benefit users in the following ways:

- By offering a secure, trustworthy and fraud-resistant system that ensures data privacy and data protection.
- By offering a common technical approach for issuing digitally-signed credentials so that certificates from one Member State can be understood and verified in any other.

[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).

- By supporting learners to provide evidence of their learning in electronic format to employers or education and training 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.

Guiding principles for this DSC Framework are listed in *Annex 1*.

The DSC 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.

3 Users

The primary users of the DSC Framework will be:

1. Credential owners (including learners, jobseekers, workers, volunteers) who are awarded digitally-signed credentials and who in turn need to store them with the option to decide when and with whom to share them;
2. Awarding bodies (including education and training institutions, businesses, or civil society organisations) that may issue digital-signed credentials to credential owners; and
3. Verifiers (including employers, education and training organisations, recruiters) who may be interested in verifying the authenticity and accreditation of digitally-signed credentials from the respective owners.

The needs and requirements of these users will be carefully analysed, through user scenarios, when designing and developing the DSC Framework.

4 Functions of the framework

The DSC framework will have five functions:

 IDENTITY	1) An awarding body will identify the individual to be awarded a credential documenting their skills or qualifications
 ISSUE	2) The awarding body will issue a digitally-signed credential to the individual (the individual is thereafter the 'credential owner) or revoke a credential that has been previously issued
 STORE	3) The credential owner may store their digital credential (e.g. in their Europass e-Portfolio or place of their choosing)

 SHARE	4) The credential owner may share their digital certificate (e.g. with an employer or education institution)
 VERIFY	5) The verifier will verify the authenticity and accreditation of the digital credential shared by the credential owner

5 Credential Types

The previous sections outlined the users and functions of the DSC framework which are constant throughout the framework, however, the framework will support authentication of a diverse range of credentials over time. User scenarios, identification of stakeholders, developing, testing, piloting and implementation will be tailored to the particular nature of each credential.

The DSC framework will support authentication of 5 types of credential:

1) Qualifications: these are 'a formal outcome of an assessment and validation process which is obtained when a competent authority or body determines that an individual has achieved learning outcomes to given standards' (Article 2 (f)). Specifically for the purposes of the DSC Framework, qualifications refers to qualifications included in national qualifications frameworks (NQFs) and/or referenced to the European Qualifications Framework (EQF), as well as qualifications supplements such as the Diploma Supplement which supports understanding of the qualification.
2) Course credentials: these include courses offered by private organisations, training organisations or employers where a digitally signed credential is issued in the name of the awarding body (e.g. Microsoft Learning).
3) Records of experience: these include employment experience, volunteering experience, or reference letters where the awarding body issues a digitally-signed record of experience. This credential includes the Europass Mobility which is signed by awarding bodies to describe the outcomes of learning experiences.
4) Certification of skills: includes a formal process of assuring that an individual is qualified in terms of particular knowledge or skills for a certain profession, sector or tasks (e.g. PM² Project Management Certification)
5) Recognition statements: these include statements on comparability, recognition or other decisions regarding qualification from credential evaluation services such as the ENIC-NARIC.

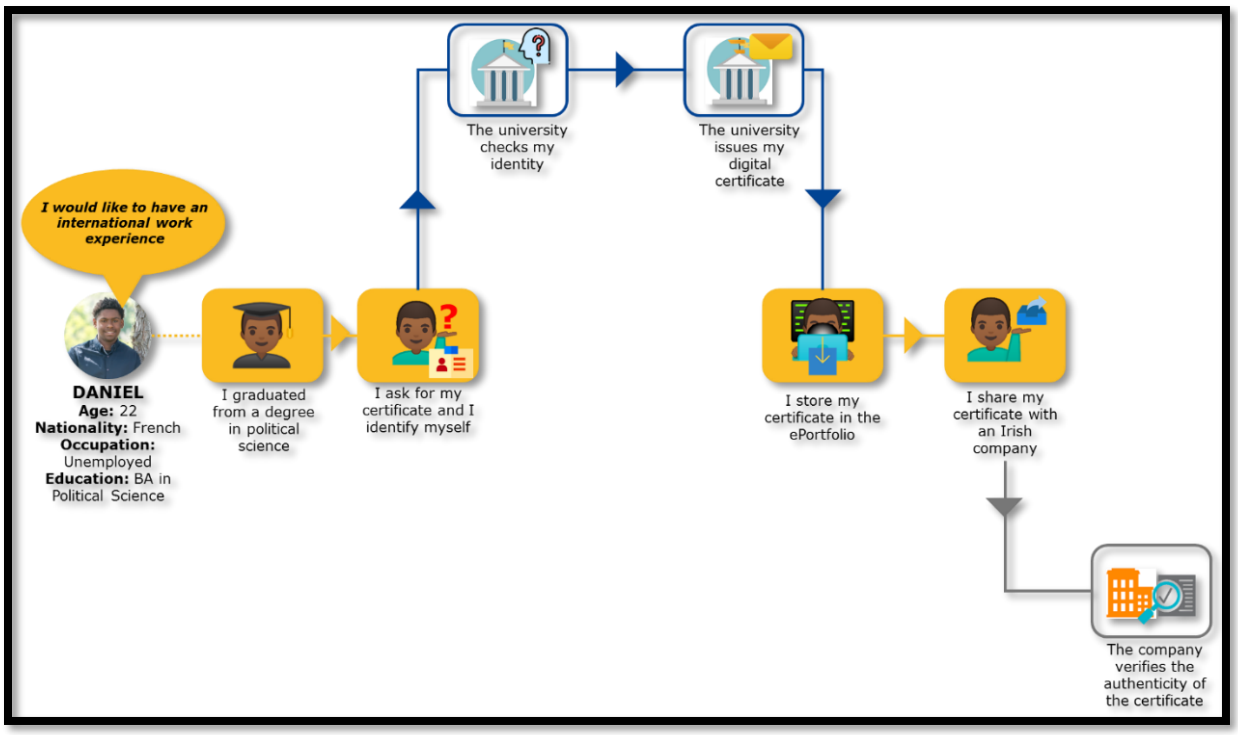
Phase 1 development of the DSC framework will focus on (1) qualifications and (2) course credentials.

6 DSC Framework in Practice

The DSC Framework will be implemented through development of user scenarios, identification of stakeholders, development, testing and piloting for each credential type.

The use case set out below illustrates the 5 functions of the DSC framework in a scenario where:

- ✓ 'Daniel', a university student, graduates with a degree in Political Science in France;
- ✓ following graduation, Daniel requests his digitally signed credential (DSC) and submits necessary identification;
- ✓ the awarding university completes necessary checks and issues the DSC for the degree in Political Science;
- ✓ Daniel stores his DSC in the Library in his Europass e-Portfolio;
- ✓ Daniel shares his DSC with a company in Ireland as part of an application for a volunteering experience;
- ✓ The Irish company views the DSC and completes checks to confirm that Daniel is the credential holder and that the awarding university, and programme, are both accredited.



7 DSC Framework Business Rules

The DSC Framework will operate in line with **business rules**; all parties and users of the DSC Framework must comply with these rules.

The rules determine the operation of the DSC Framework and are necessary to ensure the guiding principles of the DSC Framework are respected at all times (See *Annex 1*).

The Commission, in consultation with Member States, stakeholders and experts will work to identify the best technical solutions to enshrine these rules in implementation of the DSC Framework.

An overview of these rules is set out below for each of the functions of the DSC Framework (*IDENTIFY; ISSUE; STORE; SHARE; VERIFY*) with comments on technical solutions or implementation.

 IDENTITY	Rules for Identification
Credential owners and awarding bodies must be identified in order to issue a digitally-signed credentials.	

The current working technical solution to identify persons (i.e.credential owners) and organisations (i.e. awarding bodies) is linked to eIDAS (Electronic Identification, Authentication and Trust Services (Regulation (EU) N°910/2014)). The eIDAS Regulation sets out rules for electronic identification and trust services for electronic transactions (such as issuing a digitally signed credential). These services help verify the identity of individuals and businesses online or the authenticity of electronic documents.

A secondary identification option will be developed for credential owners who cannot provide evidence of identification (e.g. third country nationals).

 ISSUE	Rules for Issuance
Any legal entity can use the DSC Framework to issue a credential (in compliance with the business rules). ***Only organisations with appropriate national accreditation may issue accredited qualifications (Credential Type 1 above).*** ***Rules for revocation of credentials will be defined which awarding organisations must also comply with.***	

The European Commission will provide an issuer tool free of charge for awarding bodies that wish to make use of it, as well as provide code and technical support for awarding bodies to integrate the issuer in their systems meaning any technology for issuing credentials can be used in conjunction with the DSC Framework.

	Rules for Storage

STORE	
There are no limitations on storage. Credentials owners may store their credential on any device, in any format.	

Credential owners will have an option to store their credentials in the Library in their Europass e-Portfolio, with in-built functionalities for easy sharing and viewing of the credential.

The Europass e-Portfolio, Library and storage of credentials will be provided free-of-charge to users and code and technical support for third parties to build a Library in their own systems will also be provided.

 SHARE	Rules for Sharing
Credential owners may share their credential in three different ways through the DSC Framework: 1) Share a URL (weblink) of a 'certificate-page' so that a third party can view the credential 2) Share the data of their credential with a third party application (e.g share information on their credential directly with a jobs board) 3) Export/download a credential as PDF, badge or print	

Owners will control what they share (e.g. send a weblink or send information directly) and for how long (e.g. the weblink stays active for 24 hours). Credential owner will receive clear information and instruction on sharing their credential and maintaining direct control over the credential.

 VERIFY	Rules for Verifying
1) The DSC Framework will support verification of credentials including that: • the *awarding body has really issued the credential*; • the *credential is still valid*; • if *the credential has been revoked* All the above checks will be able to PASS or FAIL, while the revocation check may also be UNABLE TO VERIFY if the revocation information cannot be accessed. 2) The Framework will also support verification of identity to ensure that *the person presenting the credential is the owner*. The check can PASS or FAIL, depending on whether the information matches. If the check cannot be performed, the DSC Framework will mark it as UNABLE TO VERIFY. *3)* Where the credential being verified is an *accredited qualification*, additional checks will be performed to ensure *the awarding body is authorised to issue the qualification*. The check can PASS or FAIL, depending on whether the awarding body and qualification.	

8 Building the DSC Framework

The DSC Framework will comprise a number of building blocks to support the functions and rules outline above. The building blocks include:

1) Synergies with the eIDAS regulation and eIDAS services including:
   - eSignature: to identify credential owners;
   - eSeal: for authentication of awarding bodies, and for signing credentials;
   - eTime-Stamp: for timestamping transactions
   - Website authentication: to secure and authenticate web-delivered data
   - eDelivery: to transfer credentials

2) A full assessment of data protection issues to ensure minimal collection and processing of strictly necessary personal data (particularly, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility). The DSC Framework will fully support the principle is self-sovereignty whereby an individual has direct ownership and control over their own data in all times.

3) Use of open standards. Open standards are necessary to clearly establish the format, security features and comprehensiveness of information to be verified. The Commission will publish all Open Standards to allow for third parties to make use of the DSC Framework. As per the Europass Decision (*Article 6 (2) (b)*), the Commission shall consult Member States on development of any open standards. The Commission shall make a presentation on the development of any open standards as part of updates on the development of the DSC Framework in future Europass AG meetings.

4) Software and Services. Based on the concept as outlined above the DSC Framework will require a number of specific services or software to be developed to ensure effective implementation:
   - Issuer: a tool to allow an awarding body to issue digitally signed credentials and to store records of the credentials they have issued or revoked
   - Library: a virtual 'wallet' for credential owners to view, store and share their credential for verification. These functionalities are planned as part of the Europass e-Portfolio.
   - Accreditation Information: the DSC Framework will require a source of trustworthy information on accredited NQF/EQF qualifications, and revoked qualifications, to support verification of accreditation.
   - Viewer: a tool to allow credential owners to view their credentials (e.g. on the phone or other devices)

   The code and documentation for these software and services will be published so as to assist third parties develop their own systems or become interoperable with the DSC Framework.

9 Next Steps

- The Commission will have a standing item at all Europass AG meetings in 2019 on the development of the DSC Framework, including presentation on key issues for consultation such as the use of open standards. The Commission will also report on progress to the EQF AG where relevant.
- The Commission will continue to liaise with experts, including relevant project owners in Member States, and other Commission services on the development of technical solutions to build each of the elements of the framework.
- The Europass AG will be informed of opportunities to test elements and functionalities of the DSC Framework as they become available. In addition, the Commission will continue outreach to interested stakeholders for testing and piloting of the DSC Framework and report on this to the Europass AG.

Annex 1: Guiding principles

The following guiding principles underpin the functions, rules and operation of the DSC 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.
- 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

[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).

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.