SSI EduWallets

Verifiable Credentials, QMS & ELM

SSI EduWallets

Verifiable Credentials, QMS & ELM | Call 17 | Project ID 6344

Contents

Verifiable Credentials

What is a verifiable credential?

Verifiable Credentials (VCs) are a concept and technology within the field of decentralized identity and self-sovereign identity (SSI) paradigm over the web 3. The verifiable credentials provide a way to securely and digitally represent claims related to anything: they could be qualifications, achievements, identity or other pieces of information about an individual or entity. The verifiable credentials are presented in a JSON-LD or JWT format in order to be machine-readable. They are designed to be tamper-evident and cryptographically secure, ensuring the integrity and authenticity of the information they contain.

Why to use verifiable credentials?

Verifiable Credentials (VCs) offer several important benefits that make them a valuable tool in the field of digital identity and data sharing. Here are some reasons why you might choose to use Verifiable Credentials:

1. **Privacy and Control:** VCs allow individuals to have greater control over their personal information. With VCs, users can choose what information to disclose and to whom, without revealing unnecessary details. This enhances privacy and reduces the risk of personal data breaches.
2. **Reduced Data Sharing:** Traditional data sharing often involves giving access to entire databases or documents. VCs enable selective disclosure of specific claims, ensuring that only the necessary information is shared, reducing the exposure of sensitive data.

3. **Interoperability:** VCs follow standardized formats and protocols (such as W3C Verifiable Credentials[1] and DID standards[2]), making them interoperable across different platforms, services, and organizations. This enhances seamless data exchange and collaboration.
4. **Trust and Security:** VCs are cryptographically secured through digital signatures. This ensures that the information contained in the credential is tamper-evident and that the issuer's identity can be verified. It builds trust between issuers, holders, and verifiers.
5. **Fraud Prevention:** The secure nature of VCs makes them difficult to forge or alter. This helps prevent fraudulent claims or qualifications and reduces the risk of identity theft.
6. **Efficiency:** VCs streamline verification processes. Verifiers can quickly validate the authenticity of claims without needing to contact the issuer directly, reducing administrative burden and time delays.
7. **Decentralization:** VCs align with the principles of decentralized identity and self-sovereign identity (SSI). They empower individuals to manage their own digital identity, reducing the reliance on centralized identity providers.
8. **Use Cases:** VCs can be applied in various sectors, such as education (certificates and diplomas), employment (work experience and skills), healthcare (medical records), government (licenses and permits), and more. They offer a standardized solution for representing diverse types of verifiable information.
9. **Compliance and Regulation:** VCs can help organizations comply with data protection regulations like GDPR by allowing users to manage their data and consent more effectively.

[1] Sporny , M., Longley , D. and Chadwick , D. *Verifiable credentials data model V1.1*, *W3C*. Available at: https://www.w3.org/TR/vc-data-model/#abstract (last accessed: 08 July 2023).
[2] Sporny, M. *et al. Decentralized identifiers (DIDs) v1.0*, *W3C*. Available at: https://www.w3.org/TR/did-core/ (last accessed: 08 July 2023).

What does the data model of the verifiable credentials look like?

Following the W3C Verifiable credentials Data model and the definition of the EBSI verifiable attestation[3], which defines the body for all verifiable credentials, it is composed by following attributes:

Field	Description	Type	Required
context	Defines semantic context of the Verifiable Attestation	array<string (URI)>	True
id	Defines unique identifier of the Verifiable Attestation	string (URI)	True
type	Defines the Verifiable Credential type.	array<string>	True
issuer	Defines the issuer of the Verifiable Attestation.	string (URI)	True
issuanceDate	Defines the date and time, when the Verifiable Attestation becomes valid.	dateTime	True
issued	Defines when the	dateTime	True

[3] European Commission *Verifiable attestation*, *Verifiable Attestation - EBSI Specifications* -. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Attestation (last accessed: 09 July 2023).

Field	Description	Type	Required
	Verifiable Attestation was issued.		
validFrom	Defines the date and time, when the Verifiable Attestation becomes valid.	dateTime	True
validUntil	Defines the date and time, when the Verifiable Attestation expires	dateTime	False
expirationDate	Defines the date and time, when the Verifiable Attestation expires	dateTime	False
credentialSubject	Defines additional information about the subject that is described by the Verifiable Attestation	object	True
credentialStatus	Defines discovery information about the current status of a Verifiable Attestation.	object	False

Field	Description	Type	Required
credentialSchema	Contains information about the credential schema (template	object	True
evidence	Contains information about the process which resulted in the issuance of the Verifiable Attestation.	array<object>	False
proof	Contains information about the proof.	object	False
termsOfUse	Defines the terms under which the Verifiable Attestation was issued.	array<object>	False

Example source code of a VC:

```
Unset
{
    "type": ["VerifiableCredential", "VerifiableAttestation", "VerifiableUserLearningOutcomes"],
            "@context"[ "https://www.w3.org/2018/credentials/v1" ],
             "id": "urn:uuid:35ab06f9-3461-4b99-a5f9-aac84792a4d5",
             "issuer": "did:key:z6MkrY1TmB9mWpTrHDTfaMyMt1qvPmQbHYqAKc8S6SHbmyc4",
             "issuanceDate": "2023-07-18T16:23:35Z",
             "issued": "2023-07-18T16:23:35Z",
             "validFrom": "2023-07-18T16:23:35Z",
            "credentialSchema": {
              "id": "https://proto.example.com/edu/api/v1/wallet/credentialSchemas/3",
              "type": "JsonSchemaValidator2018"
             }
```

```
            "credentialSubject": {
        "id": "",
        "title": "User learning outcomes",
        "performed": [
         {
          "title": "Product test",
          "specifiedBy": {
           "teaches": [
            {
             "learningOutcome": {
              "name": "IT-Projektmanager/IT-Projektmanagerin"
             }
            }
           ]
          }
         },
         {
          "title": "Product test"
         },
         {
          "title": "Product test",
          "specifiedBy": {
           "teaches": [
            {
             "learningOutcome": {
              "name": "IT-Projektmanager/IT-Projektmanagerin",
              "relatedESCOSkill": "http://data.europa.eu/esco/occupation/8b6388a4-4904-471b-9331-d3b1211f5525"
             }
            }
           ]
          }
         }
        ]
       }
      },
      "type": "UserLearningOutcomes"
    }
```


4

[4] European Commission *Verifiable diploma schema*, *Verifiable Diploma Schema - EBSI Specifications* -. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Diploma+Schema (last accessed: 09 July 2023).

In which contexts verifiable credentials can be used?

Verifiable credentials have a large number of contexts that can be used, since they are built on the same physical documents (digitized and secured). They can be used both for identification (for the identity of a natural person), or for official documents such as diplomas, licenses or even non-official diplomas.

Verifiable credentials schemas

Verifiable credential schemas are data models or definitions of the content or body of any type of verifiable credential. The VC schemas[5] have the purpose of defining a common shape and rules for the creation and use of any VC in order to achieve interoperability between systems, because the data models of each verifiable credential schema can be read by everyone. These verifiable credentials schemas are defined in a JSON-LD format and in each verifiable credential it can be found a mandatory field called “credentialSchema” where the schema of the verifiable credential is represented in order to check if it accomplishes the definition of the schema. Below it is displayed the definition of a schema for the verifiable credential of userLearningOutcomes:

```
Unset
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "User learning outcomes verifiable accreditation",
 "description": "Schema of a user learning outcomes verifiable accreditation",
 "type": "object",
 "allOf": [
  {
   "$ref":
"https://api-pilot.ebsi.eu/trusted-schemas-registry/v2/schemas/0xeb6d8131264327f3cbc5ddba9c69cb9afd34732b3b787e4b3e3507a25d3079e
9"
  },
  {
   "properties": {
```

[5] Cohen, G. and Steele, O. (2023) *Verifiable credentials JSON schema specification*, *W3C*. Available at: https://www.w3.org/TR/vc-json-schema/ (last accessed: 09 July 2023).

```
    "credentialSubject": {
      "description": "Defines additional properties on credentialSubject to describe the body of the verifiable credential",
      "type": "object",
      "properties": {
        "id": {
          "description": "Defines the did of the credential subject",
          "type": "string"
        },
        "title": {
          "description": "Title of the credential subject",
          "type": "string"
        },
        "performed": {
          "description": "Defines the learning activity that a person participated in or attended",
          "type": "array",
          "items": {
            "$ref": "#/$defs/performed"
          }
        }
      },
      "required": [
        "id",
        "title",
        "performed"
      ]
    }
  }
 }
],
"$defs": {
  "performed": {
    "description": "Defines the learning activity that a person participated in or attended",
    "type": "object",
    "properties": {
      "title": {
        "description": "Defines a title of the learning achievement",
        "type": "string"
      },
      "startedAtTime": {
        "description": "The date the learner started the activity",
        "type": "string",
        "format": "date-time"
      },
      "endedAtTime": {
        "description": "The date the learner ended the activity",
        "type": "string",
        "format": "date-time"
```

```
    },
    "specifiedBy": {
     "description": "The specification of this learning activity",
     "type": "object",
     "properties": {
      "teaches": {
       "description": "The expected learning outcomes this learning activity specification can lead or contribute to",
       "type": "array",
       "items": {
        "$ref": "#/$defs/teaches"
       }
      }
     }
    }
   },
   "required": [
    "title"
   ]
  },
  "teaches": {
   "description": "The expected learning outcomes this learning activity specification can lead or contribute to",
   "type": "object",
   "properties": {
    "learningOutcome": {
     "description": "The learning outcome of the learning specification",
     "type": "object",
     "properties": {
      "name": {
       "description": "A legible, descriptive name for the learning outcome",
       "type": "string"
      },
      "relatedESCOSkill": {
       "description": "A URI to the related ESCO Skill",
       "type": "string"
      }
     },
     "required": [
      "name"
     ]
    }
   }
  }
 }
}
```

SSI Edu Wallets implementation

As part of the project (implementation of a demo application) we developed a customized type of verifiable credential by the use of Wallet Kit from walt.id[6]. We called it "**userLearningOutcomes**" and it was designed following the verifiable diploma schema from the European Blockchain Services Infrastructure (EBSI)[7]. This example of verifiable credentials matches the use case of our implemented "proof-of-concept" in compliance with the European Learning Model[8]. We used a standard classification schema defined by the European commission which supports a common, multi- and semantically rich language and defines the learning properties that a user achieves through the completion of educational courses or assessments. Making them interoperable between member states of the EU, the userLearningOutcomes verifiable was specifically developed in order to act as a much simpler VC than the default example provided for the EBSI definition. For our "proof-of-concept" only a few attributes were mandatorily needed.

Below you can see the structure of the VC schema of the userLearningOutcomes type:

```
Unset
{
 "credentials": [
  {
   "credentialData": {
    "credentialSubject": {
     "id": "",
     "title": "User learning outcomes",
```

[6] Walt.id *Walt.id Wallet Kit*, *walt.id*. Available at: https://github.com/walt-id/waltid-walletkit (last accessed: 08 July 2023).
[7] European Commission *European Blockchain Services Infrastructure*, *Home - EBSI -*. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home (last accessed: 09 July 2023).

[8] European Commission *Introduction to the european learning model* , *European Learning Model for Stakeholders | Europass*. Available at: https://europa.eu/europass/en/node/2128 (last accessed: 09 July 2023).

```
      "performed": [
       {
        "title": "Product test",
        "specifiedBy": {
         "teaches": [
          {
           "learningOutcome": {
            "name": "IT-Projektmanager/IT-Projektmanagerin"
           }
          }
         ]
        }
       },
       {
        "title": "Product test"
       },
       {
        "title": "Product test",
        "specifiedBy": {
         "teaches": [
          {
           "learningOutcome": {
            "name": "IT-Projektmanager/IT-Projektmanagerin",
            "relatedESCOSkill": "http://data.europa.eu/esco/occupation/8b6388a4-4904-471b-9331-d3b1211f5525"
           }
          }
         ]
        }
       }
      ]
     }
    },
    "type": "UserLearningOutcomes"
   }
  ]
 }
```

European Learning Model

What is the ELM?

ELM is a data model and a semantic standard used to describe metadata about learning."It is openly licensed, and intended to be used by any stakeholder, in any education, training and employment context, that needs to describe learning data. Available in 29 languages of the European Education Area".[9]

What is the target of the ELM?

"The ELM is a data model that aims to establish a single semantic vocabulary for learning in Europe. By unifying technical vocabularies, it allows for seamless data interchange across borders for multiple scenarios" [10]. It is defining information about:

- Qualifications and learning opportunities
- Qualifications standards such as core vocational profiles
- Credentials awarded to individuals describing their learning activities, achievements, entitlements and/or associated assessments
- Accreditation and licensing of courses, programmes and institutions
- Recognition of qualifications and credentials
- Person identity information and student membership/enrolment in educational institutions.

[9] F. Camilleri, A. (2023) *European learning model*, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/European_learning_model (last accessed: 13 July 2023).

[10] Europass Learning Model *Upcoming launch of the European Learning Model V3: Europass*, *Upcoming launch of the European Learning Model v3 | Europass*. Edited by the European Commission. Available at: https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3 (last accessed: 08 July 2023).

Why to use ELM v3?

"The European Learning Model v3 is an extension of the W3C Verifiable Credentials Data Model expressed as JSON-LD, for the purposes of providing a standardized technical format of any learning described within the European Union and European Economic Area"[11].

"While previous versions of the ELM were mainly aimed for the use of the European Commission and Member states, the new model is targeted for all education and employment stakeholders in Europe"[12]. The new Ontology provides a standardized vocabulary for the whole united model. Ontology is made up of relations between concepts, meaning that we now know for instance that a learning outcome in a learning opportunity is the same thing as a learning outcome in a qualification. This **allows the creation of knowledge graphs** to explain relationships between data, which will be extremely useful in enhancing and strengthening AI models.

ELM v3[13] is aligned with and interoperable with other models, including being completely compatible with ELMO and the EBSI Diploma Use Case. It is also linked to existing frameworks and classifications (e.g. EQF, ESCO[14], ISCED-f).

---

[11] European Learning Model v3 *european-commission-empl/European-Learning-Model* Edited by European Commission. Available at: https://github.com/european-commission-empl/European-Learning-Model

[12] Europass Learning Model *Upcoming launch of the European Learning Model V3: Europass*, *Upcoming launch of the European Learning Model v3 | Europass*. Edited by European Commission. Available at: https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3 (last accessed: 08 July 2023).

[13] Europass Learning Model *Upcoming launch of the European Learning Model V3: Europass*, *Upcoming launch of the European Learning Model v3 | Europass*. Edited by European Commission. Available at: https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3 (last accessed: 08 July 2023).

[14] ESCO *About Esco*, *ESCO*. Edited by European Commission. Available at: https://esco.ec.europa.eu/en/about-esco (last accessed: 08 July 2023).

What is the use of ELM?

"The ELM has a multitude of uses, all contributing to **easing the recognition process for learning throughout Europe**. By providing a single multilingual standard to describe learning, the ELM can support and accelerate the recognition processes of diplomas, study-periods abroad and other documents which may be presented to competent authorities across the EU"[15].

How is the ELM defined?

ELM defines a series of classes and data properties in order to classify the information of the skills and learning outcomes that a user achieves by accessing a learning resource. More information about the classes and properties can be found here[16].

Qualification Metadata Schemata

QMS[17] is a specific application of the ELM model that allows it to indicate structure information on learning outcomes in XML or RDF format. It refers to a **standard structure** used to describe and represent **detailed information about a specific qualification**. This schema is commonly used in the context of Verifiable Credentials and other qualification management systems to provide additional details about a given qualification or competency.

The Qualification Metadata Schemata includes relevant information about the qualification within the verifiable credentials, such as the name of the qualification, the

---

[15] European Commission *Introduction to the european learning model (ELM)*, *ELM Browser*. Available at: https://europa.eu/europass/elm-browser/index.html#rdf-application-profiles (last accessed: 09 July 2023).
[16] Peroni, S. and Garijo, D. (2023) *Europass Learning Model Ontology. Revision: 3.1.0.*, *Language selection*. Available at: https://europa.eu/europass/elm-browser/documentation/rdf/ontology/documentation/elm.html (last accessed: 09 July 2023).
[17] European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'.

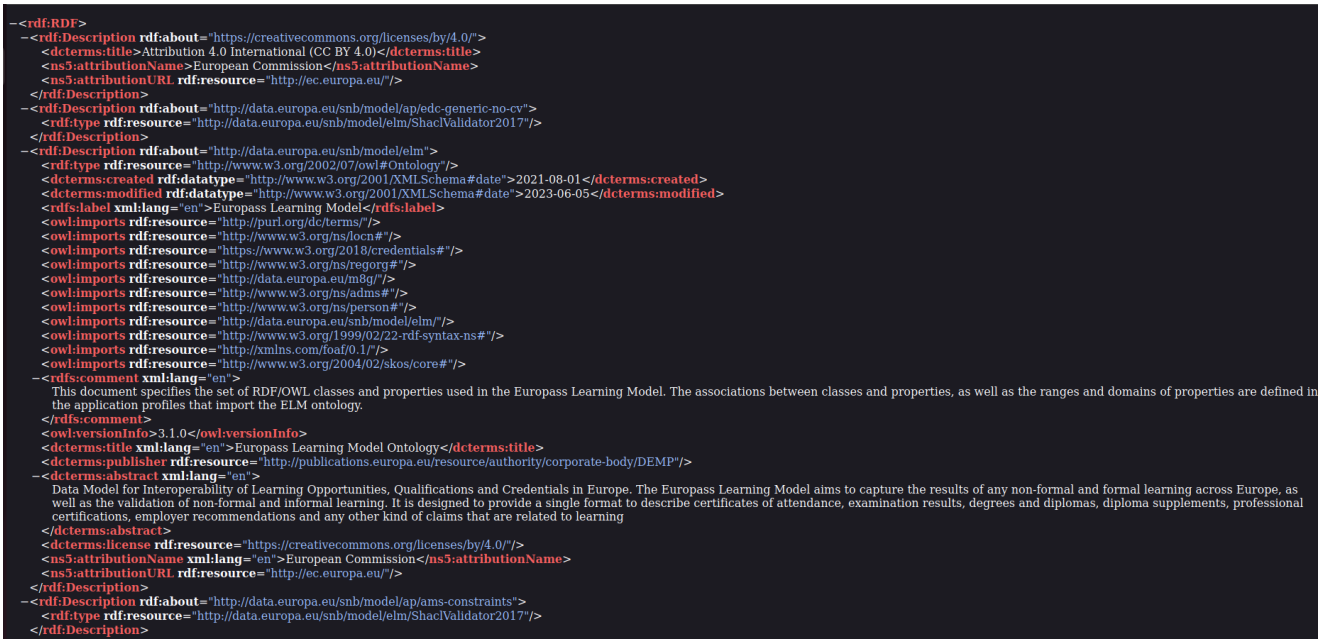
associated education or training level, the learning outcomes or skills acquired, the issuing institution, credits or study hours, among other attributes.

The qualification scheme used within verifiable credentials helps to expose the learning results that a user has acquired in a structured and detailed way, so that these verifiable credentials, once presented to third parties, can obtain the results in a structured and detailed way.

The use of QMS within ELM provides a standard and accepted way within the member states of the European Union to describe in detail the skills that a user has obtained in his/her own learning history ("track record"). Through the combination of the ELM and QMS, interoperability is obtained between ambiguous systems which make use of these data schemes. Verifiable credentials that conform to this framework will be easily interoperable with other systems by using a standard structure that defines the skills, qualifications and occupations a user can achieve.

"The QMS is a RDF3 vocabulary with an RDF schema. Additionally, there are XML4 schemata available to support the encoding of information in XML. The schemata also define controlled vocabularies as fixed value lists for some properties in the schema. QMS is applicable in many contexts"[18]. It can be applied to encode, publish and exchange qualification metadata over multiple environments/technologies. Below an example of the class "LearningAchievement" that the ELM defines is displayed :

[18] European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'



19

QMS 2.0 Data model

The QMS 2.0 data model has numerous classes and fields that create a complete definition of all the skills that a user can obtain when carrying out and finishing an educational process. The most relevant are described in the next table:

Class	Description
qualification	The details of a qualification that can or has been awarded such as the (expected) learning outcomes. This can be a copy or a specialization of an existing qualification standard.
accreditation	An accreditation record. An Accreditation is the

[19] Europass Learning Model Ontology RDF schema of LearningAchievement Edited by the European Commission. Available at: https://publications.europa.eu/resource/authority/snb/model/elm (last accessed: 09 July 2023).

Class	Description
	quality assurance or licensing of an institution.
learningOutcome	A learning outcome (i.e. knowledge, skill, autonomy-responsibility). The details, such as the description, of a learning outcome.
learningActivitySpecification	A LearningActivitySpecification is a specification of a process which leads to the acquisition of knowledge, skills or responsibility and autonomy.
assessmentSpecification	An AssessmentSpecification is a specification of a process establishing the extent to which a learner has attained particular knowledge, skills and competences against criteria such as learning outcomes or standards of competence.
entitlementSpecification	The specification of a right a person has access to, typically as a result of a learning achievement. A specification may take the form of the right to be a member of an organization, to follow a certain learning opportunity specification, or to follow a certain career. An entitlement may be prospective, i.e. awarding the right to apply for the entitlement, or actual, i.e. granting the entitlement.
organization	A legal organization (e.g. an awarding body, an academic or training institution,...).

Class	Description
scoringScheme	A scoring scheme. A numeric or text type of scoring methodology or convention. A grading system.
framework	The details about a semantic framework or system. Used to describe other semantic frameworks to which resources in EDCI can be associated, tagged or aligned with

[20]

More information about the QMS 2.0 Data model can be found in the document called "Publishing of Qualification and LearningOpportunity Data Documentation".

The current classes and properties used in the implementation of the "userLearningOutcomes" verifiable credential that was implemented for a "proof-of-concept" within our demo application are listed below:

- **learningActivitySpecification**
    - **teaches**: The expected learning outcomes to which this learning activity specification contributes to. This is given by a LearningSpecification. A learning activity can lead to or contribute to the acquisition of a set of skills, knowledge, autonomy and or responsibility. It MUST refer to an existing record in the "learningSpecificationReferences"-section of this document.
- **learningOutcome**
    - **name (prefLabel):** A legible, descriptive name for the learning outcome. Maximum cardinality of one per language.
    - **relatedESCOSkill:** A link/alignment to an ESCO Skill.

[20] European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'

Below an example body content of a “userLearningOutcomes” verifiable credential, using some properties of the QMS 2.0, is displayed:

```
Unset
{
  "credentialSubject": {
        "id": "did:key:z6MkhhosB653LLTzR6k6gUbMi3K24czgyNUfvqa4rG5G6x1p",
        "title": "User learning outcomes",
        "performed": [{
              "title": "Test1",
              "startedAtTime": "2023-08-09T14:39:17+02:00",
              "specifiedBy": {
                    "teaches": [{
                          "learningOutcome": {
                                "name": "Web-Designer/Web-Designerin",
                                "relatedESCOSkill":
"http://data.europa.eu/esco/occupation/c40a2919-48a9-40ea-b506-1f34f693496d"
                          }
                    }]
              }
        }]
  }
}
```

Documental sources

Cohen, G. and Steele, O. (2023) *Verifiable credentials JSON schema specification*, *W3C*. Available at: https://www.w3.org/TR/vc-json-schema/ (last accessed: 09 July 2023)

ESCO *About Esco*, *ESCO*. Edited by the European Commission. Available at: https://esco.ec.europa.eu/en/about-esco (last accessed: 08 July 2023).

Europass Learning Model *Upcoming launch of the European Learning Model V3: Europass*, *Upcoming launch of the European Learning Model v3 | Europass*. Edited by the European Commission. Available at: https://europa.eu/europass/tr/news/upcoming-launch-european-learning-model-v3 (last accessed: 08 July 2023).

Europass Learning Model Ontology RDF schema of LearningAchievement Edited by the European Commission. Available at: https://publications.europa.eu/resource/authority/snb/model/elm (last accessed: 09 July 2023).

European Commission (2020) 'Publishing of Qualification and Learning Opportunity Data Documentation'.

European Commission *European Blockchain Services Infrastructure*, *Home - EBSI -*. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home (last accessed: 09 July 2023).

European Commission (no date b) *Introduction to the european learning model (ELM)*, *ELM Browser*. Available at: https://europa.eu/europass/elm-browser/index.html#rdf-application-profiles (last accessed: 09 July 2023).

European Commission *Introduction to the european learning model* , *European Learning Model for Stakeholders | Europass*. Available at: https://europa.eu/europass/en/node/2128 (last accessed: 09 July 2023).

European Commission *Verifiable diploma schema*, *Verifiable Diploma Schema - EBSI Specifications -*. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Diploma+Schema (last accessed: 09 July 2023).

European Commission *Verifiable attestation*, *Verifiable Attestation - EBSI Specifications* -. Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Attestation (last accessed: 09 July 2023).

European Learning Model v3 *european-commission-empl/European-Learning-Model* Edited by European Commission. Available at: https://github.com/european-commission-empl/European-Learning-Model

F. Camilleri, A. (2023) *European learning model*, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/European_learning_model (last accessed: 13 July 2023).

Peroni, S. and Garijo, D. (2023) *Europass Learning Model Ontology. Revision: 3.1.0.*, *Language selection*. Available at: https://europa.eu/europass/elm-browser/documentation/rdf/ontology/documentation/elm.html (last accessed: 09 July 2023).

Sporny , M., Longley , D. and Chadwick , D. *Verifiable credentials data model V1.1*, *W3C*. Available at: https://www.w3.org/TR/vc-data-model/#abstract (last accessed: 08 July 2023).

Sporny, M. *et al. Decentralized identifiers (DIDs) v1.0*, *W3C*. Available at: https://www.w3.org/TR/did-core/ (last accessed: 08 July 2023).

Walt.id ,*Walt.id Wallet Kit*, *walt.id*. Available at: https://github.com/walt-id/waltid-walletkit (last accessed: 08 July 2023).