EBSI-VECTOR
Education and work reloaded

D3.2 ESSIF specification for the new capabilities in EBSI (First Version)

Project title:	**EBSI-VECTOR** - EBSI enabled VErifiable Credentials & Trusted Organisations Registries
Grant Agreement No.	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Deliverable Title	D3.2: ESSIF specification for the new capabilities in EBSI (First version)
Version:	1.0
Date:	31/01/2024
Responsible Partner:	DANUBETECH
Authors:	Markus Sabadello (DANUBETECH), Samuel Gomez (Gataca), Steffen Schwalm (MSG), Helmut Nehrenheim (Govpart)
Contributing Partners:	DANUBETECH, Gataca, MSG, Logalty
Reviewers:	Matjaž Tercelj (Protokol), Katie Phillips (Protokol), Žan Kovač (Protokol), Ivan Basart (ValidatedID), Andreas Abraham (ValidatedID), Ignacio Alamillo (Logalty)
Dissemination Level:	PU – Public

Project co-funded by the European Union under the Digital Europe Programme. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document Change History

Version	Date	Author (organisation)	Description
v0.1	25/10/2023	Multiple Authors	Work-in-progress
v0.2	10/01/2024	Multiple Authors	For internal review
v0.3	24/01/2024	Multiple Authors	Incorporated review feedback
v1.0	31/01/2024	Multiple Authors	Final version

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

LIST OF FIGURES

List of Tables

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

List of Terms and Abbreviations

Abbreviation	Definition
API	Application Programming Interface
ARF	Architecture and Reference Framework
CAB	Conformity Assessment Bodies
CWT	Concise Binary Object Representation (CBOR) Web Token
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
EBIP	EBSI Improvement Proposal
EBSI	European Blockchain Service Infrastructure
EDIC	European Digital Infrastructure Consortium
eIDAS	electronic Identification, Authentication and Trust Services
ELM	European Learning Model
ETSI	European Telecommunications Standards Institute
EUDIW	EU Digital Wallet
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JSON-LD	JSON for Linking Data
JWT	JSON Web Token
MFA	Multi Factor Authentication
MITM	Man in the Middle
MS	Member State
OCSP	Online Certificate Status Protocol

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

OID4VC	OpenID for Verifiable Credentials
PID	Personal Identification
PKI	Public key infrastructure
PR	Pull Request
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualified Electronic Signature
QTSP	Qualified Trust Service Provider
RFC	Request for Comments
TS	Technical Specification
VC	Verifiable Credential
W3C	World Wide Web Consortium
WG	Working Group
WP	Work Package

Executive Summary

In the EBSI-VECTOR project, task T3.1 – as part of work package WP3 – has been tasked with further defining the specifications of the current European Self Sovereign Identity Framework (ESSIF) capabilities to be built in EBSI. The scope of task T3.1 is to act as a bridge on one hand between the technical work package WP3 and the use case work packages WP4 (Education) and WP5 (Social Security), and on the other hand between EBSI-VECTOR and the EBSI Core Team.

This document D3.2 presented here is the second deliverable of task T3.1. The first deliverable D3.1 was an evaluation of the current ESSIF implementation and legal/governance framework. Expanding on that, D3.2 now contains a list of topics discussed by task participants over the last few months. Each section in this document contains a description of the activities and insights the participants have developed on the specific topic, and many references to external content are included for further details. Some topics (the ones developed far enough) also contain concrete recommendations, technical guidelines, and examples on how to realize a specific capability identified by T3.1 participants.

In general, many of the topics we explored in this document are related to a desired alignment between EBSI and the EU Digital Identity Wallet's Architecture Reference Framework (ARF). This strategic objective has been articulated repeatedly by T3.1 participants and has already been identified and discussed in our previous deliverable D3.1. Besides topics that are specifically relevant to the alignment of EBSI with the ARF, other topics have also been worked on in task T3.1 and are also included in this deliverable.

Most of the topics presented in this document have been selected by participants of task T3.1 themselves, based on their professional experience and analysis of the current technical and legal landscape inside and outside the EBSI ecosystem. This identification and selection of topics, however, has so far occurred mostly without too much input from other EBSI-VECTOR work packages. This is not ideal, since T3.1's scope should primarily be to process concrete business requirements from the use case work packages, i.e. WP4 and WP5. Notable exceptions are topics related to the "binding of attestation credentials", and to "verification proofs", which have both been brought forward by participants of EBSI-VECTOR WP5.

The "Introduction" section contains further information about the background and structure of this deliverable, and about the mode of work of task T3.1 that resulted in this deliverable. The

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

"Conclusions" section summarizes the current state of work in this task, and envisions next steps, including closer alignment with the requirements of the use case work packages, and plans for the next deliverable D3.9.

The authors of this deliverable D3.2 hope that as an initial version, it contains useful information on new capabilities that should be specified and developed by EBSI, in order to help implement the use cases successfully, and to advance the EBSI ecosystem as a whole.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Introduction

After deliverable D3.1, which has been submitted in 2023, this document presented here is the second deliverable D3.2 of task T3.1. The scope of T3.1 continues to be to act as a bridge on one hand between the technical work package WP3 and the use case work packages WP4 (Education) and WP5 (Social Security), and on the other hand between EBSI-VECTOR and the EBSI Core Team. The goal is to ensure that the use cases' requirements can be successfully implemented given the capabilities provided by EBSI.

Deliverable D3.1 included the evaluation of current ESSIF capabilities and a list of recommendations for improved and new capabilities. This deliverable D3.2 presented here goes one step further by discussing selected new capabilities in greater technical depth, and by approaching possible technical solutions to concrete challenges. We also assume at this point that deliverable D3.2 constitutes the initial version of what will be a living document for the remaining duration of the EBSI-VECTOR project and will later culminate in a final version as deliverable D3.9. This deliverable D3.2 can also be considered a “snapshot” of the current state of various topics that have been identified in task T3.1 and will continue to be worked on.

The mode of work in T3.1 in the last few months has heavily involved the use of the EBSI Ecosystem Gitlab platform, which also serves as the basis for the content presented in this deliverable: https://code.europa.eu/ebsi/ecosystem. On this platform, T3.1 participants have raised and commented on issues and pull requests (PRs), and labels have been used for tagging issues relevant to the EBSI-VECTOR project. This has proven to be an effective way of communicating asynchronously not only within T3.1, but also externally with the EBSI Core Team.

In addition to the work on the EBSI Ecosystem Gitlab platform, T3.1 also continued to hold regular weekly calls. During these calls, several topic-focused discussions were conducted based on presentations delivered by individual T3.1 partners, for example on the topic of “WP5 Social Security” on 16th October 2023, by DRV-BUND.

Besides those regular weekly calls, when necessary, additional conference meetings were also held with external experts to consult on specific issues. For example, on 27th September 2023, EBSI-VECTOR T3.1 met with SD-JWT expert Kristina Yazuda to discuss the topic of compatibility of SD-JWT with JAdES. And on 30th October 2023, EBSI-VECTOR T3.1 met with Juan Carlos Cruellas Ibarz of the Electronic Signatures and Infrastructures (ESI) Technical Committee (TC) to discuss topics related to JAdES. In addition, we held an alignment meeting on 6th December 2023 with participants from both WP4 and WP5, to share common open points, interdependencies and develop a common vision. Meetings were generally recorded, and notes were taken and shared.

The content of this deliverable D3.2 is organized as a relatively straightforward list of topics that have been identified and selected during discussions between T3.1 participants. An outline of some of the topics is presented here:

- JAdES and remote e-sealing: This is likely to become important in scenarios where an Issuer of attestations interacts with a QTSP to produce JAdES conformant signatures. See section 3 for more details.
- Incompatibilities between SD-JWT and JAdES: This is important considering the widespread interest in the SD-JWT(-VC) data model as the basis for attestations. See section 4 or more details.
- Protect data integrity when an issuer is issuing a new SD-JWT VC: This explores several important technical details related to the integrity of an attestation issuance process that supports selective disclosure. See section 5 for more details.
- JSON-LD VCs are NOT "just JSON": This is a recurring topic that is important for aligning different data models used by EBSI and the EU Digital Wallet Architecture Reference Framework (ARF) in a secure way. See section 6 for more details.
- Binding between an "attestation" credential and "identity" credential: This is important in scenarios in which an "attestation" credential is only valid if it is presented together with an "identity" credential that has been issued to the same person. See section 7 for more details.
- Certification of QTSP for Electronic Ledger using EBSI: This is an important aspect of aligning the EBSI ledger with eIDAS2 on the legal and technical level. See section 8 for more details.
- Certification of QTSP using EBSI: This is an important aspect of aligning the issuing of EBSI-conformant attestations with eIDAS2 on the legal and technical level. See section 9 for more details.
- Verification Proofs: This refers to the requirement that when a VC is verified, a proof of this verification process is created that can be later used to trace, audit, etc. a verification process. See section 11 for more details.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Each of the sections in this document describes the specific topic, and contains various conclusions, next steps, and recommendations. For the most part, the sections can be read individually; it is not necessary to read this document in a sequential way, and it is possible to read only a subset of topics that are of interest to the audience.

Last, the document presents a conclusion of the overall, current state of the work on new capabilities for EBSI, as identified by T3.1.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

JAdES and remote e-sealing

See https://code.europa.eu/ebsi/ecosystem/-/issues/20

Description

We discussed the topic of JAdES and remote e-sealing. JAdES is a technical specification (ETSI TS 119 182-1) for electronic signatures and infrastructures. Producing JAdES conformant signatures is important for issuing QEAAs. Annex V Letter g eIDAS 2.0 requires QES or QSeal on each QEAA by the QTSP issuing QEAA. Annex VIa point (1)(g) of eIDAS 2.0 requires QES or QSeal for each EEAs issued by an authentic source.

The group understood that with JAdES, today you send the payload to the remote e-sealing service that constructs the header and creates the signature. The question was whether it is an option to send only a digest of the payload[1]. This can be useful for privacy reasons, since only a digest – rather than the full contents of an attestation – have to be transmitted to an e-sealing service.

We discussed aspects of section 5.2.8.3.3 of ETSI TS 119 182 v1.1.1. We furthermore discussed other APIs, including Digital Signature Service (DSS)[2] and the Cloud Signature Consortium API[3].

On 30th October 2023, EBSI-VECTOR T3.1 met with Juan Carlos Cruellas Ibarz to discuss topics related to JAdES. Juan Carlos is active in Electronic Signatures and Infrastructures (ESI) Technical Committee (TC). He is also leader of ETSI STF 645, which is looking at emerging technologies including ledgers, for recording evidence that certain things have happened.

Notes from the meeting were taken[4]. One of the insights from the meeting was that remote e-sealing is supported, where you don't want to reveal the payload.

Further questions remain after the meeting and have been formulated by the EBSI team[5]:

- *Additional question for remote e-sealing: since constructing the protected/unprotected header is the most complex operation (constructing the chains, timestamps, revocation*

[1] https://code.europa.eu/ebsi/ecosystem/-/issues/20#note_72725
[2] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Digital+Signature+Service+-++DSS
[3] https://cloudsignatureconsortium.org/resources/download-api-specifications/
[4] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_75179
[5] https://code.europa.eu/ebsi/ecosystem/-/issues/20#note_75181

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

info, ...), is there a possibility that a remote service creates the headers, returns the headers to the clients to compute the digest of protected header + payload, a digest is then sent to the remote e-sealing service?

- *Another case we had in mind is using detached signatures (using sigD), but JAdES currently covers the case where the payload is hosted elsewhere (via HTTP or URI, if I'm not mistaken); would it be possible to use the detached signature mechanism to create a signature by sending the digest of the payload, and the remote service creates the headers and signature?*

Conclusions, Next Steps and Recommendations

As not all the questions related to this topic have been answered at this time, further conversation with JAdES experts is required.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Incompatibilities between SD-JWT and JAdES

See https://code.europa.eu/ebsi/ecosystem/-/issues/19

Description

We discussed the topic of potential incompatibilities of SD-JWT and JAdES. Such incompatibilities could arise from the fact that SD-JWT and JAdES are both based on JSON Web Signature (JWS), but make different assumptions about the payload and the constraints of the payload that is signed.

EBSI has published examples that show patterns and profiles of SD-JWT compliant selective disclosure:

https://code.europa.eu/ebsi/ecosystem/-/blob/feat/sd-jwt-examples/drafts/sd-examples.md

Concerns about poor performance have been expressed, e.g. in a situation when all entries in a Diploma schema with 3000 different properties should be hidden[6].

Concerns have also been expressed about mixing JSON-LD and JWS/(SD-)JWT concepts, e.g. in the "Presenting the credential using Verifiable Presentation(s)" section[7]:

https://code.europa.eu/ebsi/ecosystem/-/blob/feat/sd-jwt-examples/drafts/sd-examples.md#presenting-the-credential-using-verifiable-presentations

We recognize the value of using JSON-LD in payloads, which can enable use cases to benefit from "post-processing" activities like internationalization or semantics. If a JSON-LD payload is protected using JWS, then checking the schema and the signature of a VC is an activity that is done in the same way in a pure JSON VC or in a JSON-LD VC[8].

We discussed feedback from the EBSI team about JSON-LD, JWS, and SD-JWT being different layers, and how both JSON and JSON-LD can be protected using JWS or JAdES. This includes the possibility to securely reference or transport/embed the actual `@context` values and perform full -LD processing[9].

[6] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_72711
[7] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_72712
[8] See https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_72713
[9] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_72714

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

We identified and reviewed relevant Pull Requests (PRs) on SD-JWT and SD-JWT-VC specifications, e.g.:

- https://github.com/oauth-wg/oauth-selective-disclosure-jwt/pull/344

On 27th September 2023, EBSI-VECTOR T3.1 met with SD-JWT expert Kristina Yazuda to discuss compatibility of SD-JWT with JAdES. One of the the conclusions was that SD-JWT should support the JWS JSON Serialization in addition to Compact Serialization[10].

On 30th October 2023, EBSI-VECTOR T3.1 met with Juan Carlos Cruellas Ibarz to discuss topics related to JAdES. Juan Carlos is active in Electronic Signatures and Infrastructures (ESI) Technical Committee (TC). He is also leader of ETSI STF 645, which is looking at emerging technologies including ledgers, for recording evidence that certain things have happened.

Notes from the meeting were taken[11]. They are copied here for reference:

- *Discussion about SD-JWT and JAdES.*
- *SD-JWT compact serialization contains JWS plus extra data including ~ tilde, therefore not compatible with JAdES?*
- *The part in SD-JWT could be JAdES.*
- *ETSI is working on profiles, one profile is based on SD-JWT.*
- *JAdES is JWS with additional constraints.*
- *JAdES can be serialized in the same way as JWS (compact, JSON extended, JSON flat).*
- *JAdES supports augmented signatures, put additional material into unprotected header, mandates that this must be serialized as JSON.*
- *Why are the disclosures in the unprotected header? Because implementers want to use compact serialization.*
- *But maybe the issuer wants to sign the whole payload, for liability reasons, so that the wallet can't deny later.*
- *Maybe do two signatures - one with disclosures in unprotected header, and one that signs the whole thing.*
- *Is remote e-sealing supported, where you don't want to reveal the payload, only digest? Yes it's supported.*

[10] https://github.com/oauth-wg/oauth-selective-disclosure-jwt/pull/289

[11] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_75179

- *Can JAdES be used to sign W3C VCDM? It's one of the candidates for a profile.*
- *Pointers and links from the discussion:*
- *ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI)*
- *https://www.etsi.org/deliver/*
- *https://www.etsi.org/standards-search#page=1&search=ts%20119%20432&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-10-30&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1*
- *https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.01.01_60/ts_119432v010101p.pdf*
- *Steffen (msg) is a member of ETSI and can potentially present to ESI.*
- *Juan Carlos will approach Nick Pope (nick.pope@secstanassoc.com), chair of ESI, to introduce him to VECTOR. Check how a relationship can be established, similar to EUDI Wallet LSPs.*

The above notes from the meeting were further updated and partially corrected in subsequent comments, especially with regard to signing SD-JWT disclosures[12].

The EBSI team did additional work to show how an SD-JWT-like approach (salted hases of the attributes) can be applied to the W3C VCDM and signed with JAdES, without the need for the extra serialization:

- https://code.europa.eu/ebsi/ecosystem/-/blob/EBIP-SD-JWT/drafts/sd-jws.md
- https://code.europa.eu/ebsi/ecosystem/-/blob/feat/sd-jwt-examples/drafts/sd-examples.md

[12] https://code.europa.eu/ebsi/ecosystem/-/issues/19#note_75180

Conclusions, Next Steps and Recommendations

Based on the above, it appears SD-JWT and JAdES can be compatible, and a detailed specification with the approach should be developed.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Protect data integrity when an issuer is issuing a new SD-JWT VC

See https://code.europa.eu/ebsi/ecosystem/-/issues/25

Description

This issue refers to the issuance process. In the current ODIC4VCI the credentials are being issued directly because data integrity is protected by the VC signature. In the case of SD-JWT credentials, that mechanism to transport the credentials is not enough because the issuer is sending also the disclosures (not including into the VC):

```
{
  "credentials": [
    {
      "mediaType": "OPTIONAL. Credential media type",
      "credential": "{protected JSON with _sd claim}",
      "disclosures": [
        "disclosure 1",
        "disclosure 2",
        "..."
      ]
    }
  ]
}
```

This new mechanism to send the information implies new validations:

- To check that the sender has sent all disclosures
  - One by one (performance problem in credentials with many disclosures): As there is no restriction into the number of disclosures this process could be heavy in terms of performance (wallet also has to scan the entire JSON tree).
  - Counting the total of `_sd` and matching the disclosures (user verifies the number of disclosures, but not the integrity. Depending of the type of disclosure to find them (One `_sd` list by JSON level), it's also heavy in terms of performance)
- To check that they are correct.
  - One by one (performance problem in credentials with many disclosures and some levels in the JSON tree): This mechanism implies validating one by one the

disclosures included into the VC. This process implies a hash operation for each disclosure.

- To check that there is no MITM
  - Store in the VC the hash of all disclosures (do not verify that it's complete, nor that it's correct).
  - Including a signature (We could use a presentation).

Other issues:

- How to manage disclosures in schemas:
  - Is it predefined?
  - Is it similar in all the MS?
  - How to manage complex credentials from the issuer side? (e.g. Diploma)

Samuel (VECTOR T3.1) analyzed that the best way to do it is including a signature into the structure but the validation "user receives all the required disclosures", should be performed disclosure by disclosure[13].

Alen (EBSI Team) suggested that JSON pointers could be used as presented here[14]:

- https://code.europa.eu/ebsi/ecosystem/-/blob/EBIP-SD-JWT/drafts/sd-jws.md?ref_type=heads

Samuel (VECTOR T3.1) replied that It should be faster in case you want to verify all the disclosures sent are valid, but you should scan the whole JSON to verify ALL the disclosures are included into the list[15].

Further points related to this feature that were discussed by the EBSI Team and VECTOR T3.1 include[16]: Data integrity, avoiding risk of MITM, requirement to check all disclosures, hiding the claims, hiding the structure, unlinkability, combining claims from different VCs.

[13] https://code.europa.eu/ebsi/ecosystem/-/issues/25#note_75030
[14] https://code.europa.eu/ebsi/ecosystem/-/issues/25#note_75033
[15] https://code.europa.eu/ebsi/ecosystem/-/issues/25#note_75038
[16] https://code.europa.eu/ebsi/ecosystem/-/issues/25#note_75082

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Conclusions, Next Steps and Recommendations

While we have gained a good overview and understanding of the topic described above, further exploration and specification are necessary going forward.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

JSON-LD VCs are NOT "just JSON"

See https://code.europa.eu/ebsi/ecosystem/-/issues/18

Description

Markus (EBSI-VECTOR T3.1) has expressed concerns about securing JSON-LD data with JWS, and performed experiments about JSON-LD VC payloads secured by JWS vs. Data Integrity:

- https://medium.com/@markus.sabadello/json-ld-vcs-are-not-just-json-4488d279be43
- https://github.com/peacekeeper/json-ld-vcs-not-just-json

The main results of these experiments are:

- It's possible to have changes in a JSON-LD document and/or the underlying data model that are "detected" by JWS but not Data Integrity, and vice versa.
- JWS secures a JSON document, Data Integrity secures the JSON-LD data model.

The experiments can be summarized as follows:

Depending on your perspective, you could interpret the results in different ways. You could call Data Integrity insecure, since it depends on information outside the JSON document. You could also call JWS insecure, since it fails to secure the JSON-LD data model.

The real point of this article is however NOT to say that any of the mentioned data models or proof mechanisms are inherently insecure, but rather to raise awareness of the nuances. To say "JSON-LD is JSON" is correct on the document layer, and wrong on the data model layer. Certain combinations of data models and proof mechanisms can lead to surprising results, if they are not understood properly.

Related article: https://tess.oconnor.cx/2023/09/polyglots-and-interoperability

Quotes from this article include:

- "Two data models means twice the work!"
- "It would have been much clearer to define two proof verification algorithms, one for JSON's data model, and one for the RDF data model."

Related discussions in VC WG:

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- https://github.com/w3c/vc-data-model/issues/1315
- https://github.com/w3c/vc-data-model/pull/1302

Alen (EBSI Team) replied that we need to be more precise on what's been protected (or not)[17]. What the experiment is showcasing (implicitly) is what happens when the RDF is not protected. Not protecting the RDF results with invalid signature and invalid interpretation. RDF could be protected with JWS (either fully dereferenced context is put in the protected header, or digest of dereferenced context in the protected, and full payload in the unprotected header, when needed). In that case, the semantics is also secured when JWS is used. At the end of the day, `@context` needs to be secured.

We agreed that securing the semantics when JWS is used is important and should be explored more. We also considered the following related discussions in the W3C Verifiable Credential Working Group:

- https://github.com/w3c/vc-data-model/issues/1315 ("Consider abandoning drafts for non-data-integrity-proof securing formats")
- https://github.com/w3c/vc-data-model/issues/1327 ("Consider mandating securing RDF graph for all securing mechanisms")

Alen (EBSI Team) summarized three different approaches of achieving the goal of protecting the `@context`[18]:

- Approach 1: Using the inline/embedded context - context files are directly embedded in the VCs
- Approach 2: Using permalink (e.g., Trusted Schemas Registry) or other repositories
- Approach 3: Protecting the digest of the context definition using new claim `https://www.w3.org/TR/vc-data-model-2.0/#integrity-of-related-resources`

Alen (EBSI Team) also provided examples of each of the approaches, which can be parsed using https://jwt.io/:

Approach 1: Inline/embedded:

[17] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_73861
[18] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74857

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

```
eyJhbGciOiJIUzI1NiIsImN0eSI6InZjK2xkK2pzb24ifQ.eyJAY29udGV4dCI6eyJuYW1lIjoia
HR0cDovL3NjaGVtYS5vcmcvbmFtZSIsImRlc2NyaXB0aW9uIjoiaHR0cDovL3NjaGVtYS5vcmcvZ
GVzY3JpcHRpb24iLCJpbWFnZSI6eyJAaWQiOiJodHRwOi8vc2NoZW1hLm9yZy9pbWFnZSIsIkB0e
XBlIjoiQGlkIn0sImdlbyI6Imh0dHA6Ly9zY2hlbWEub3JnL2dlbyIsImxhdGl0dWRlIjp7IkBpZ
CI6Imh0dHA6Ly9zY2hlbWEub3JnL2xhdGl0dWRlIiwiQHR5cGUiOiJ4c2Q6ZmxvYXQifSwibG9uZ
2l0dWRlIjp7IkBpZCI6Imh0dHA6Ly9zY2hlbWEub3JnL2xvbmdpdHVkZSIsIkB0eXBlIjoieHNkO
mZsb2F0In0sInhzZCI6Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hIyJ9LCJuYW1lI
joiVGhlIEVtcGlyZSBTdGF0ZSBCdWlsZGluZyIsImRlc2NyaXB0aW9uIjoiVGhlIEVtcGlyZSBTd
GF0ZSBCdWlsZGluZyBpcyBhIDEwMi1zdG9yeSBsYW5kbWFyayBpbiBOZXcgWW9yayBDaXR5LiIsI
mltYWdlIjoiaHR0cDovL3d3dy5jaXZpbC51c2hlcmJyb29rZS5jYS9jb3Vycy9nY2kyMTVhL2Vtc
GlyZS1zdGF0ZS1idWlsZGluZy5qcGciLCJnZW8iOnsibGF0aXR1ZGUiOiI0MC43NSIsImxvbmdpd
HVkZSI6IjczLjk4In19.IOOrMxmeoUHuOFSoBm92k569nMhp-5gcNP9MA5ukrNI
```

Payload in Approach 1:

```
{
  "@context": {
    "name": "http://schema.org/name",
    "description": "http://schema.org/description",
    "image": {
      "@id": "http://schema.org/image",
      "@type": "@id"
    },
    "geo": "http://schema.org/geo",
    "latitude": {
      "@id": "http://schema.org/latitude",
      "@type": "xsd:float"
    },
    "longitude": {
      "@id": "http://schema.org/longitude",
      "@type": "xsd:float"
    },
    "xsd": "http://www.w3.org/2001/XMLSchema#"
  },
  "name": "The Empire State Building",
  "description": "The Empire State Building is a 102-story landmark in New
York City.",
  "image":      "http://www.civil.usherbrooke.ca/cours/gci215a/empire-state-
building.jpg",
  "geo": {
    "latitude": "40.75",
    "longitude": "73.98"
  }
}
```

Approach 2: Using a permalink:

```
eyJhbGciOiJIUzI1NiIsImN0eSI6InZjK2xkK2pzb24ifQ.eyJAY29udGV4dCI6Imh0dHBzOi8vZ
2lzdC5naXRodWJ1c2VyY29udGVudC5jb20vYWxlbmhvcnZhdC9iYjA3YWNiN2ZhYTU0YzVkOTEyZ
WY5NjhkZWVhZTlmMy9yYXcvZmMzZmNjMDVlYTMwNjc5M2JmYWRkMzM5ZTNmN2Y3NzAyNjQ1NzlmM
y9wbGFjZS5qc29ubGQiLCJuYW1lIjoiVGhlIEVtcGlyZSBTdGF0ZSBCdWlsZGluZyIsImRlc2Nya
XB0aW9uIjoiVGhlIEVtcGlyZSBTdGF0ZSBCdWlsZGluZyBpcyBhIDEwMi1zdG9yeSBsYW5kbWFya
yBpbiBOZXcgWW9yayBDaXR5LiIsImltYWdlIjoiaHR0cDovL3d3dy5jaXZpbC51c2hlcmJyb29rZ
S5jYS9jb3Vycy9nY2kyMTVhL2VtcGlyZS1zdGF0ZS1idWlsZGluZy5qcGciLCJnZW8iOnsibGF0a
XR1ZGUiOiI0MC43NSIsImxvbmdpdHVkZSI6IjczLjk4In19.nuvgD6Y4a1AY8luC9_sLtYPgo5CX
rAdxj07w3arsMmA
```

Payload in Approach 2:

```
{
 "@context":
"https://gist.githubusercontent.com/alenhorvat/bb07acb7faa54c5d912ef968deeae
9f3/raw/fc3fcc05ea306793bfadd339e3f7f770264579f3/place.jsonld",
  "name": "The Empire State Building",
  "description": "The Empire State Building is a 102-story landmark in New
York City.",
"image":        "http://www.civil.usherbrooke.ca/cours/gci215a/empire-state-
building.jpg",
  "geo": {
    "latitude": "40.75",
    "longitude": "73.98"
  }
}
```

Approach 3: Protecting the digest:

```
eyJhbGciOiJIUzI1NiIsImN0eSI6InZjK2xkK2pzb24ifQ.eyJAY29udGV4dCI6Imh0dHBzOi8vZ
2lzdC5naXRodWJ1c2VyY29udGVudC5jb20vYWxlbmhvcnZhdC9iYjA3YWNiN2ZhYTU0YzVkOTEyZ
WY5NjhkZWVhZTlmMy9yYXcvZmMzZmNjMDVlYTMwNjc5M2JmYWRkMzM5ZTNmN2Y3NzAyNjQ1NzlmM
y9wbGFjZS5qc29ubGQiLCJuYW1lIjoiVGhlIEVtcGlyZSBTdGF0ZSBCdWlsZGluZyIsImRlc2Nya
XB0aW9uIjoiVGhlIEVtcGlyZSBTdGF0ZSBCdWlsZGluZyBpcyBhIDEwMi1zdG9yeSBsYW5kbWFya
yBpbiBOZXcgWW9yayBDaXR5LiIsImltYWdlIjoiaHR0cDovL3d3dy5jaXZpbC51c2hlcmJyb29rZ
S5jYS9jb3Vycy9nY2kyMTVhL2VtcGlyZS1zdGF0ZS1idWlsZGluZy5qcGciLCJnZW8iOnsibGF0a
XR1ZGUiOiI0MC43NSIsImxvbmdpdHVkZSI6IjczLjk4In0sInJlbGF0ZWRSZXNvdXJjZSI6eyJpZ
CI6Imh0dHBzOi8vZ2lzdC5naXRodWJ1c2VyY29udGVudC5jb20vYWxlbmhvcnZhdC9iYjA3YWNiN
2ZhYTU0YzVkOTEyZWY5NjhkZWVhZTlmMy9yYXcvZmMzZmNjMDVlYTMwNjc5M2JmYWRkMzM5ZTNmN
2Y3NzAyNjQ1NzlmMy9wbGFjZS5qc29ubGQiLCJkaWdlc3RTUkkiOiJzaGEyNTYtYWNiODYzMWRlZ
jc1NTRiMTUwZGVhZjJlZDM3MjA3NjAwOWUyYzVhNDYyNmQzZGVkZGI2YjU0NDQ1Nzg2M2IxZCJ9f
Q.2zM7dCHLOGrwo-7gErUpaFGhkqRzrM_p8fRd6NjOdy8
```

Payload in Approach 3:

```
{
```

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

```
  "@context":
"https://gist.githubusercontent.com/alenhorvat/bb07acb7faa54c5d912ef968deeae
9f3/raw/fc3fcc05ea306793bfadd339e3f7f770264579f3/place.jsonld",
  "name": "The Empire State Building",
  "description": "The Empire State Building is a 102-story landmark in New
York City.",
  "image":      "http://www.civil.usherbrooke.ca/cours/gci215a/empire-state-
building.jpg",
  "geo": {
    "latitude": "40.75",
    "longitude": "73.98"
  },
  "relatedResource":                                                       {
    "id":
"https://gist.githubusercontent.com/alenhorvat/bb07acb7faa54c5d912ef968deeae
9f3/raw/fc3fcc05ea306793bfadd339e3f7f770264579f3/place.jsonld",
  "digestSRI":
"sha256-acb8631def7554b150deaf2ed372076009e2c5a4626d3deddb6b544457863b1d"
  }
}
```

We discussed advantages and disadvantages of the different approaches:

- In Approach 1, the size of the VC grows linearly with the size of the `@context`, whereas in Approaches 2 and 3, the size of the VC is independent of the size of the `@context`.
- In Approach 2 and Approach 3, the `@context` files can be shared in the unprotected header of the signature, the same way same as other protected external resources.
- One potential problem with Approach 2 could be that permalinks to `@context` files are just a convention and not really verifiable (unless e.g. in the concrete Github example where you could theoretically verify the Git commit history of the permalink). On the other hand, if a Trusted Schemas Registry is used like in EBSI, then there's no issue with versioning of `@context` files. This makes Approach 2 dependent on a specific ecosystem, whereas Approaches 1 and 3 are ecosystem-independent.

The approaches mentioned above are well established in the context of advanced digital electronic signatures (https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v01

0101p.pdf). With the new `relatedResources` claim in the VCDM, the VCDM v2 offers a very nice solution to the problem[19]:

- https://www.w3.org/TR/vc-data-model-2.0/#integrity-of-related-resources

We also discussed whether it would be easier to just do Data Integrity from the start, than doing JWS plus additional mechanisms to secure the `@context`[20]. We agreed that canonicalization and signing over N-Quads is more complex than signing over a JSON document[21]. On the other hand, canonicalization is a single well-defined step which has a W3C spec and multiple implementations[22]:

- https://w3c.github.io/rdf-canon/spec/

Matti (EBSI Team) commented that the `relatedResource` has been added into the EBSI Verifiable Attestation schema[23]:

- https://code.europa.eu/ebsi/json-schema/-/blob/main/schemas/ebsi-attestation/2023-10/schema.json

The approach is following the architectural boundaries of JAdES, where the JWS Header contains information about signature and signer, while the JWS payload itself handles the integrity of its contained external references (like referenced JSON-LD context, and other cases). Some clarifications would still be beneficial. Trusted references like EBSI links do not need to be protected, as the content itself is under the trust umbrella. Thus `@context` stored in EBSI does not need this kind of protection.

Another topic is how the three different approaches would work with SD-JWT[24]. There may be a difference between selectively disclosing parts of the JSON document, and disclosing parts of the RDF graph. It may be necessary to always disclose the entire `@context`, even if only parts of a VC are selectively disclosed. This could potentially leak too much information, or could require a complex process to determine which parts of the `@context` need to be disclosed, and how.

[19] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74996
[20] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74883
[21] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74888
[22] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74888
[23] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_75481
[24] https://code.europa.eu/ebsi/ecosystem/-/issues/18#note_74883

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Conclusions, Next Steps and Recommendations

Based on the above, it appears JSON-LD can be sufficiently secured in combination with SD-JWT, if the nuances are properly understood and appropriate steps are taken. Further work is recorded to create a detailed specification of how to achieve this, using one or more of the approaches described above.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Binding between an “attestation” credential and “identity” credential

See https://code.europa.eu/ebsi/ecosystem/-/issues/26

Description

We have discussed a few times the need for the possiblity to have a binding between an "attestation" (such as diploma or social security pass) and an "identity" credential (e.g. PID). This discussion was to a large part motivated by business requirements explained to VECTOR T3.1 by VECTOR WP5.

Maybe the "attestation" wouldn't have a DID or public key in it, but instead a reference to an ARF-Type-1 compatible PID.

There was also a session related to this at the Internet Identity Workshop 37 (but it doesn't seem to have notes):

- https://docs.google.com/document/d/1KgL0k2bFrEv2FOEzRXBO6LRR0P0R3CQUhyI2mE4q39U/

In our 6th Nov 2023 VECTOR T3.1 weekly meeting, we did some brainstorming in a HackMD pad and developed initial examples:

- https://hackmd.io/dnaYtecXQlmu0ho3eQsiZQ

Alen (EBSI Team) commented that this approach falls in the category of “contextual binding”, and that either the VC is bound to another VC or a subset of information in another VC so that identity matching is easy/well-defined[25]. Some discussion on this topic can be found here:

- https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

Summary[26]:

- “cryptographic binding” - I prove to the verifier that the VC belongs to me by proving (sole) control of a private key

[25] https://code.europa.eu/ebsi/ecosystem/-/issues/26#note_75336
[26] https://code.europa.eu/ebsi/ecosystem/-/issues/26#note_75339

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- "contextual binding" - I prove to the verifier that the VC belongs to me by providing additional physical/digital documents, the verifier recognises and compares the contextual information (name, surname, address, ...)

Markus (VECTOR T3.1) replied that in his opinion, options for this topic will depend on whether and how a PID will contain a unique identifier that could potentially be referenced from other attestations[27]. The final eIDAS Regulation will NOT mandate a unique and persistent identifier for everyone, due to privacy concerns associated with that. See the following document for an analysis on legal aspects of this and other topics:

- https://epicenter.works/en/content/eu-digital-identity-reform-the-good-bad-ugly-in-the-eidas-regulation

Samuel (VECTOR T3.1) noted that what we are trying to build is a VC chain, in which the VC origin is the PID and the rest of VCs are "slaves". In real life however when you are presenting your Driver's License you don't need the PID to be allowed to continue driving[28]. However, the problem comes when you request multiple VCs, you must validate each VC separately, but also you must validate both VCs belong to the same person.

This could be achieved following this mechanism:

- When a user creates a wallet, indirectly, the user is creating a new DID (Identity).
- When a user requests a PID, he is requesting it on behalf of the previous DID.
- When a user requests another QEAA, he is requesting it using the same DID.
- When a user wants to be authenticated in a service, he is requesting for the last to VCs, so he is sending both VCs also signed with the same private key (DID). So the third party could verify both VCs and also, both VCs belong to the same person.

If the user wants to preserve his identity better, he can create a new DID and then collect the VCs with the new Identity.

[27] https://code.europa.eu/ebsi/ecosystem/-/issues/26#note_75708
[28] https://code.europa.eu/ebsi/ecosystem/-/issues/26#note_76074

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Matti Taimela (EBSI Team) replied that this falls into the cryptographic binding and is a very good approach, and that requesting single credential for multiple DIDs is also supported by the OID4VCI out of the box, the same capability is supported by EBSI[29]:

- https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html#section-7-3

Verification Path of Identity-Bound Credentials

An interesting aspect of the binding with Identity is the handling in the verification of the credention.

In a scenario where we have a Credential (Issued by public Service) and this linked to another Identity-Credential (Issued by public Identity-Service) we pace two independent valdidty status.

A requirement for public service is that the validity of this Credential is not lmited or affected by the validity of the (bound-to or linked-to) Identity Credential. This implies from the fact that although we operate in a digital world is remains always on the choice of the citizen to use other Identification means (including non-digital Ones like peronal ID-Card or Passport).

The technicasl solution of the verificaton of the Credential should reflect the fact that there are more than bool verifation results, which increases with the number of contained credentials.

Conclusions, Next Steps and Recommendations

Examples that have been created related to this topic can be found in this HackMD: https://hackmd.io/dnaYtecXQlmu0ho3eQsiZQ

Some of the examples, which show how a European Health Insurance Card (EHIC) can potentially reference a PID, are also reproduced here. Note that the focus of the examples is to explore structures for referencing a PID, not the correctness of the EHIC or PID data models.

Reference to PID unique ID, included in `credentialSubject`:

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://insurance.example/credentials/1872",
```

[29] https://code.europa.eu/ebsi/ecosystem/-/issues/26#note_76298

```
  "type": ["VerifiableCredential", "EuropeanHealthInsuranceCard"],
  "issuer": "did:example:12334",
  "validFrom": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "pid" {
      "uniqueIdentifier": "123456"
    },
    "insuranceStatus": "active"
  }
}
```

Reference to PID unique ID, outside of `credentialSubject`:

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://insurance.example/credentials/1872",
  "type": ["VerifiableCredential", "EuropeanHealthInsuranceCard"],
  "issuer": "did:example:12334",
  "validFrom": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "insuranceStatus": "active"
  },
  "confirmationMethod": {
    "type": "PidConfirmation",
    "pid" {
      "uniqueIdentifier": "123456"
    }
  }
}
```

Reference to PID public key, included in `credentialSubject`:

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://insurance.example/credentials/1872",
  "type": ["VerifiableCredential", "EuropeanHealthInsuranceCard"],
  "issuer": "did:example:12334",
  "validFrom": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "pid": {
      "cnf": {
        "jwk" {
          "kty": ..,
          "crv": ..,
          "x": ..,
          "y": ..
        }
      }
    },
    "insuranceStatus": "active"
  }
}
```

Reference to PID public key, outside of credentialSubject:

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://insurance.example/credentials/1872",
  "type": ["VerifiableCredential", "DiplomaCredential"],
  "issuer": "did:example:12334",
  "validFrom": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "insuranceStatus": "active"
  },
  "confirmationMethod": {
    "type": "VerificationKeyConfirmation",
    "pid" {
      "cnf": {
        "jwk" : {
          "kty": ..,
          "crv": ..,
          "x": ..,
          "y": ..
        }
      }
    }
  }
}
```

Reference to PID attributes, outside of credentialSubject:

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://insurance.example/credentials/1872",
  "type": ["VerifiableCredential", "EuropeanHealthInsuranceCard"],
  "issuer": "did:example:12334",
  "validFrom": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "familyName": "Sabadello",
    "firstName": "Markus",
    "dateOfBirth": "...",
    "insuranceStatus": "active"
  },
  "confirmationMethod": [{
    "type": ["PidConfirmation"],
    "pid" {
      "uniqueIdentifier": "123456"
    }
  }, {
    "type": ["PidConfirmation", "PidConfirmationAT"],
    "pid" {
      "familyName": "Sabadello",
      "firstName": "Markus G.",
      "dateOfBirth": "...",
      "placeOfBirth": "Vienna"
    }
  }]
}
```

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Certification of QTSP for Electronic Ledger using EBSI

See https://code.europa.eu/ebsi/ecosystem/-/issues/23

Description

With Section 11 eIDAS 2.0 introduces (qualified) trust services on Electronic Ledger (Art. 45 h following). It defines that qualified ledgers "are created and managed by one or more qualified trust service provider or providers, establish the origin of data records in the ledger, ensure the unique sequential chronological ordering of data records in the ledger and record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time". Although the regulation is technology neutral the description in Art. 45i is in line with the definition of DLT in international standards like ISO 22739:2020 and contains core properties of DLT.

It has to be stated that Section 11 focus on all use cases not covered by EUDI Wallet or all other (qualified) trust services so e.g. (qualified) signatures, seals, timestamps, attestations electronic delivery etc. Means that DLT can be used as infrastructure for any EUDI Wallet as well as any other QTSP too – the security will be proven within the conformity assessment of the CAB, but there's no need to use QTSP for Ledger as precondition to provide another (qualified) trust service nor an EUDIW. So it has to be differentiated between:

- QTSP for Ledger using EBSI
- EUDI Wallet Providers and QTSP using EBSI

The table below shows differentiation and applicability of Section 11

#	Use Case Type	Examples Use Cases	Section 11 applicable
1	EUDI Wallet	● Infrastructure for ○ PID ○ (Q)EAA (with QTSP)	no

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

#	Use Case Type	Examples Use Cases	Section 11 applicable
		○ QES (with QTSP) ● Trusted Issuer Registries ● Trust List/Trust Anchors Verifiable Data Registry	
2	Other QTSP	● QES ● QSeal ● QTimestamp ● eDelivery and registered mail ● Remote signing ● Validation ● Preservation ● Archiving ● Trusted Issuer Registries Trust List/Trust Anchors	no
2	QTSP for Electronic Ledger	● Cryptocurrencies ● Supply chain ● Data traceability ● Product traceability ● Document traceability Web 3	yes
3	Use cases in non-regulated domains	Dito	yes

Table 1: differentiation and applicability of Section Section 11 eIDAS 2.0

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Much more complex in case of DLT is the portfolio of a QTSP for Electronic Ledger using EBSI as the main nodes remain in responsibility of member states and so the possible QTSP has to deal with already existing authorities taking one main task in the DLT network – running the main nodes - per default. One possibility could be that the QTSP provides only the validating nodes and so controls the execution of transactions in the network, similar approach would be the provision of the consensus mechanism and/or the responsibility for the whole security and trust in the network. As EBSI is designed as pan-European network it’s also thinkable that 1-n QTSP may provide certain parts like validating nodes or sub-nodes or e.g. the implementation and operation of special applications like smart contracts. The portfolio has to be elaborated further and will determine the certification requirements for Conformity Assessment Bodies. Production of training materials and provision of appropriate communication measures together with WP 7 will be necessary.

The certification shall differentiate between fundamental requirements relevant for all QTSP laid down in ETSI EN 319 401 and the trust service specific requirements for QTSP for ledger.

Conclusions, Next Steps and Recommendations

With DIN TS 31648 (developed e.g. by German National Cybersecurity Authority) and ISO TR 24332 first standards exists. With ISO AWI TS 2353 a correspondign Standard on Auditing Guidelines for DLT is under developmet in ISO Tc 307. Similar developments are plannend in CEN. As the ETSI EN 319 401 is relevant for each QTSP its adoption and contribution on possible adjustions according to QTSP for Ledger is one next step. Afterwards the identification and development of specific policies and security requirements applicable to this specific trust service on Electronic Ledger, appropriate for each technical registration mechanism and aligned with applicable standards will be done in close collaboration with relevant standardization bodies (e.g. ETSI ESI, CEN JTC 19) will be developed in alignment with ETSI EN 319 403. Based on those results the governance and secifications of EBSI will be adjusted.

A liaison with the EBSI-NE project has been established. Task 3.7 of the EBSI-NE project deals with the production of the materials for a future qualification of EBSI. The objective of the task is to prepare validator nodes on the EBSI ledgers (both Besu and Fabric) to be qualified according to the requirements of this new trust service contained in eIDAS 2.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Criteria Catalogue of DIN should be one input and correlated to EBSI. Description can be found below. This issue affects any DLT based project including VECTOR.

https://code.europa.eu/ebsi/ecosystem/uploads/3ffeda3fb818352e48fbb26d00255a74/DIN_TS_31648_en-GB.pdf

Certification of QTSP and EUDIW Provider using EBSI

(no corresponding Gitlab issue)

Description

QTSP as well as EUDI Wallet Providers could offer their services using EBSI capabilities and services. One example would be a QTSP issuing qualified electronic attestations of attributes relying on EBSI Trusted Registries or mechanisms in support of privacy-enhanced revocation. Under the eIDAS Regulation, the QTSP offering the trust service is liable for the service, with a strict liability model when offering a qualified trust service.

One main task is the transformation of EBSI Governance into eIDAS 2.0. One possibility is given below:

EBSI	eIDAS Trust Framework
Member State	Same (e.g. National Supervisory Body or National Cybersecurity Authority)
Root Trusted Accreditation Organization	Accreditation Body
Sub Trusted Accreditation Organization (to issue accreditations to legal entities)	Depends on Member State
Business registry authority	Business registry Authority of Member State (if existent) as authentic source which only acts as authentic source Issuance done by certified PID Provider or certified QTSP
Public Body as Authentic source (issues credential for citizens) resp. Trusted Issuer	To be differentiated into: • Authentic source (providing data to be attested by QTSP for QEAA)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

EBSI	eIDAS Trust Framework
	• PID Provider (issuing PID for citizens) QTSP (issuing credential/services depending on kind of QTSP)
Accredited Privated Actor (issues credentials for legal entity) resp. Trusted Issuer	• PID Provider (issuing PID for legal entities) QTSP (issuing credential/services depending on kind of QTSP)
Trusted Issuer Registry	Trust List
Relying Party/verifier Registry	Listed Relying Party
Wallet Providers Registry (in roadmap)	Trust List
Trusted Schema Registry	Trust List resp. does not exist in eIDAS Trust Framework

Table 2: Transformation of EBSI Governance into eIDAS 2.0

Conclusions, Next Steps and Recommendations

In the EBSI model, the QTSP would be a user of the EBSI services. As such, proper interfaces, procedures and agreements are needed, and conformity assessment materials aligned with the eIDAS 2 Regulation requirements, thus allowing a QTSP using EBSI services to fulfil its legal obligations in an easy and seamless manner. These will be produced mainly in EBSI-VECTOR in the context of the liaison with the EBSI-NE project. This work will include the contribution on adjustment of existing standards for QTSP to be used with EBSI as well as contribution on standardization for EUDI Wallet. As the ETSI EN 319 401 is relevant for each QTSP its adoption and contribution on possible adjustions according to QTSP or EUDI Wallet Providers is another task. The in alignment with ETSI EN 319 403 is needed too. Based on those results the governance and secifications of EBSI will be adjusted.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Authenticate the wallet provider to prove the conformity

See https://code.europa.eu/ebsi/ecosystem/-/issues/28

Description

This feature attempts to authenticate the wallet provider for each transaction made with the user wallet, in order to:

- Ensure the certification achieved by the wallet provider / version
- Allow other features as Push Notifications or custom features provided by specific providers

In this way, all the participants of the data exchange could validate the conformity of the wallet, avoiding frauds or misuses of the wallet and protecting the privacy and security of the interchange.

The importance of this lies in preventing a wallet that has not passed the pertinent compliance controls (both legal and technical) from being used in a regulated and highly controlled environment such as that of digital identity.

Trust levels aside, it is necessary to create an environment of trust around this technology so that both citizens and companies can feel it and adopt its benefits as quickly as possible.

To ensure greater security and compliance with the requirements requested by the wallet certifier, it is necessary to have a mechanism to verify that the wallet/provider has gone through a certification process for each transaction executed.

This mechanism makes it possible to control, first in a technical way and then in a regulatory way, that the provider is complying with the framework and, therefore, is protecting the user.

The mechanism consists in the creation of an application registry, which will allow the authentication of previously certified wallets and will provide tokens to be used in the different transactions with third parties, which these parties can use to verify the compliance of the wallet with which they are interacting.

In addition, by using this token, a neutral service (hosted by EBSI?) could be managed that would allow wallet providers to interoperate using push notifications as well (with an initial scope to their own technology).

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

This possible service is just the beginning of greater interoperability, and would allow different technology providers to increase the scope of their services.

Conclusions, Next Steps and Recommendations

While we have gained a good overview and understanding of the topic described above, further exploration and specification are necessary going forward.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Data Agreements between Holders and Third Parties, and Verification Proofs

See https://code.europa.eu/ebsi/ecosystem/-/issues/27

Description

Data agreements are agreements between different parties for the exchange of information in a controlled and secure manner. These agreements set a controlled environment so that both the subject(s) sharing the information and the subject(s) receiving the information are bound to certain conditions in such exchange.

This allows the subject sending the information to control their information and therefore their privacy by providing them with the ability to limit the scope, duration and use of the information exchanged.

This functionality is very important for the citizen, and also for the organizations, since one of the major problems of previous architectures was very much related to privacy, and this functionality tries to minimize that negative impact, giving the user control of his own data.

During the EBSI-VECTOR Workshop in Rome on 18th-19th December 2023, a requirement described as "verification proofs" has been formulated by VECTOR WP5 leaders. This means that when a VC is verified, a proof of this verification process is created that can be later used to trace, audit, etc. a verification process. This could also work for an auditing process according to one of the latest functionalities related to the limitation of verifiers to request specific credentials instead of everyone being able to request the credentials they want at any given time.

At this time, we assume that such a "verification proof" can itself be modeled as a VC, issued by the Verifier of the original VC. Exact requirements need to be explored further, but an initial list of information included in a verification proof could look like this:

- Who verified the VC?
- Which VC was verified? The verification proof could include an identifier of the VC, or a hash, or a copy of the entire VC.
- When was the VC verified?
- What was the result of the verification process?

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Additional metadata about the verification process
- Use as mechanism by the user and third party to control what is happening with the agreement. When any of them whats to revoke the sharing agreement it could be done through this structure. So, is it public (anonymized)? Where is anchored?

Conclusions, Next Steps and Recommendations

While we have gained a good overview and understanding of the issues described above, further exploration and specification are necessary going forward.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Crypto Stability within EBSI

See https://code.europa.eu/ebsi/ecosystem/-/issues/24

Description

EBSI as every DLT use hash protection based on Merkle Trees for immutability and integrity. DLT hashes in father-son-principle but no rehashing nor independent Proof of Existence (independent from DLT) exists. Means: If the used hash algorithm becomes not suitable anymore they are in danger to be recalculated - means unperceived changes of on-chain records (e.g. transaction, DID) etc. Possible.

Possible solution is described in DIN TS 31648:

To ensure the long-term security of the cryptographic methods used in the system, mechanisms for periodically renewing the hash algorithms of the blockchain/DLT before their security suitability expires have been established. For this purpose, a procedure for preserving the value of evidence is used in accordance with DIN31647:2015-05, BSITR-03125 with/or. ETSITS119512 used. This can be part of the distributed ledger system or an external process that is linked to the DLT system.

In order to effectively preserve the evidentiary value, i.e. to preserve the authenticity and integrity of the transactions and records in the DLT, a new proof of existence is generated at periodic intervals through a time stamp renewal or hash tree renewal according to RFC4998 or RFC6283 before the security suitability of the underlying algorithms expires. Rehashing and resigning are also implemented in DIN31647:2015-05 or BSITR-03125 with/or. ETSITS119512 shown. The security suitability of the cryptographic algorithms used must be checked regularly by the person responsible for operating the blockchain/DLT using ETSITS119312 and the SOG-IS catalogs.

The re-hashing in a Merkle hash tree according to RFC4998 or RFC6283 must include all hash values of the cryptographic security of the transactions/blocks, including the included records, and is completed with a qualified timestamp according to ETSIEN319422 and RFC3161 of a qualified trust service according to eIDAS. In order to re-sign the qualified timestamp of the Merkle hash tree used to preserve evidentiary value in distributed ledger technology/blockchain, it is renewed before the security suitability of the underlying algorithms expires. The time stamp

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

renewal is carried out according to RFC4998 or RFC6283 as shown in DIN31647:2015-05, BSITR-03125 with/or ETSITS119512.

Technically, the timestamp renewal and hash tree renewal can be designed as follows. For the purpose of verifiability and to protect personal data, it is necessary that the content and its metadata are not stored in Blockchain/DLT. The transaction data in the blockchain/DLT only references the actual content and metadata. The content and its metadata are included

The relevant and technical evidence data is stored in a system suitable for preserving the value of evidence in accordance with BSITR-03125 with/or ETSITS119512 (Figure 1).

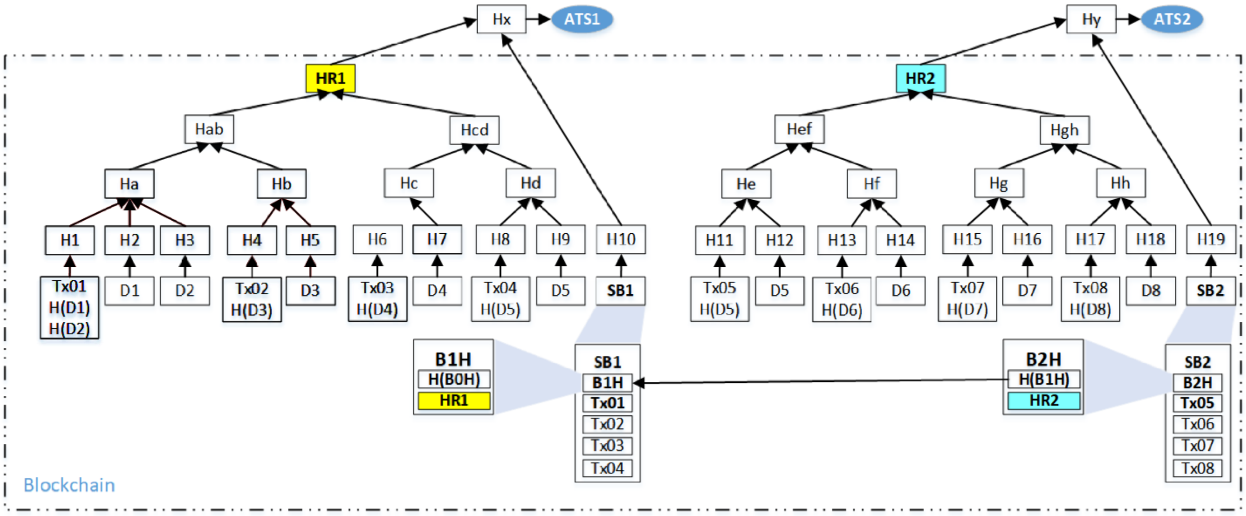

Figure 1: Evidence data storage in accordance with BSITR-03125 with/or ETSITS119512

The transactions, together with the associated (referenced) content and metadata, each form a data object group in the sense of RFC4998 (see RFC4998, Chapter 4.2), e.g. Tx01 with D1 and D2 or Tx05 with D5 (see Figure 1). A Merkle tree according to RFC4998 is built across all transactions and the associated content data, which ends with the root hash value (e.g. HR1). The calculated root hash value is stored in the associated block header (e.g. B1H) within the block description (en: serialized block) (e.g. SB1) and saved in the same hash tree, which gives the hash tree a new root element (e.g. Hx), which then corresponds to RFC4998 a qualified timestamp (e.g. ATS1). Proceed similarly with the following block (B2). The block header of B2H (S2B) contains the hash value calculated via the block header of block B1 (B1H), which ensures the desired chaining of the blocks. The evidentiary value is preserved in accordance with RFC4998; all headers as well as the transactions and the content data referenced by them are protected.

Conclusions, Next Steps and Recommendations

The following paper describes the issue and possible solutions. This shall be solved in EBSI to be used for regulated cases with retention periods between 10 and 100 years as they are typical in traceability cases. Adoption of solutions from preservation services acc. Art. 34 and 40 eIDAS, ETSI TS 119 511/512 is recommended. This issue affects EBSI-VECTOR and TRACE4EU projects, as well as potentially all other EBSI-based projects including Early Adopters. The further research and solution development will be aligned with the suggestion described in 12.1 as it was adopted by ISO DTR 24332.

https://code.europa.eu/ebsi/ecosystem/uploads/b2fe4052b6bf0b20b30aab81971e0969/2021-04-15_Contribution_Korte_Schwalm_Shamburger_final_v1.0.pdf

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

OID4VC Interop Profiles Convergence

See https://code.europa.eu/ebsi/ecosystem/-/issues/22

Description

EBSI specifications are clear that the OID4VC suite of protocols should be used for transmission of Verifiable Credentials and Verifiable Presentations between Issuers, Holders, and Verifiers. However, various profiles of OID4VC exist, and it's not immediately obvious how they relate to each other, how compatible they are, etc. In the interest of interoperability between EBSI and other ecosystems, it appears important to clarify which profile of OID4VC EBSI should follow.

At the Internet Identity Workshop 37 there were sessions about comparing OID4VC interop profiles by DIF, DIIP, HAIIP:

- https://github.com/decentralized-identity/jwt-vc-issuance-profile
- https://github.com/decentralized-identity/jwt-vc-presentation-profile
- https://www.dutchblockchaincoalition.org/bouwstenen/diip-2
- https://vcstuff.github.io/oid4vc-haip-sd-jwt-vc/draft-oid4vc-haip-sd-jwt-vc.html

Conclusions, Next Steps and Recommendations

More analysis would be useful, especially with regard to compatibility of the various OID4VC interop profiles with EBSI.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Revocation Mechanisms

See https://code.europa.eu/ebsi/ecosystem/-/issues/21

Description

We have discussed the paper "What to do when good Verifiable Credentials go bad“ published by EBSI:

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+to+do+when+good+Verifiable+Credentials+go+bad

EBSI also has documentation about credential status strategies:

https://api-pilot.ebsi.eu/docs/specs/credential-status-framework/credential-status-strategies

One piece of feedback about the paper is that it describes that there shall be no connection between Verifier and Issuer in case of validation[30]. This won`t work in eIDAS where QTSP for QEAA/QES etc. responsible for issuance and revocation. Means revocation information needed to be received from QTSP which is liable for. Otherwise the Relying Party depends on holder to allow check of revocation which holder might not do (e.g. in case driver license was revoked). Means also revocation needed without participation of holder, only in interaction relying party and issuer. In order to ensure a wide adoption of eIDAS 2.0 and EBSI it´s necessary to achieve alignment with existing solutions focused on revocation mechanism independent from the use case resp. to separate the revocation protocol from the format of the revoked certificate or equivalent. Means that solutions like CRL, StatusList 2021 already discussed within EBSI (https://hub.ebsi.eu/vc-framework/credential-status-framework/vcs) should be reused and contributed to the technical framework eIDAS 2.0 ecosystem.

Another comment was also that the Issuer does control the revocations and the Verifier can pull this information directly or indirectly[31]. Directly has privacy issues as Issuer gains knowledge of Verifiers, while fetching indirectly this is protected (like through EBSI proxy). The revocation/status list is signed (it is a VCDM), thus it is transport medium agnostic and does not need to be directly fetched from the Issuer.

[30] https://code.europa.eu/ebsi/ecosystem/-/issues/21#note_74099
[31] https://code.europa.eu/ebsi/ecosystem/-/issues/21#note_75482

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Additional aspects of revocation mechanisms have been discussed in the corresponding Gitlab issue:

https://code.europa.eu/ebsi/ecosystem/-/issues/21

The topic of revocation has also been previously discussed in our first deliverable D3.1. In that document, a desire has been expressed to make revocation mechanisms independent of the used credential formats, and to potentially re-use existing protocols and infrastructures such as OCSP.

Having these, there can be no knowledge gained by the issuer or other unothorized parties about verifications or credential details. One open discussion remains as deletions seems to be required, while history of transactions needs to be preserved.

Conclusions, Next Steps and Recommendations

While we have gained a good overview and understanding of the issues described above, further exploration and specification are necessary going forward. Concrete input from the use case work packages regarding requirements for revocation mechanisms will be valuable.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Parental access for VC of minors or assisted persons

See https://code.europa.eu/ebsi/ecosystem/-/issues/29

Description

In everyday life, people may be given access to certificates on behalf of others. This can occur with parents in connection with minors, but also with people who look after another person. We should clarify whether and, if so, how this can be implemented in the digital world.

Conclusions, Next Steps and Recommendations

While we have gained an initial overview and understanding of the issue described above, further exploration and specification are necessary going forward.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Dealing with VCs in the case of name changes of persons or companies

See https://code.europa.eu/ebsi/ecosystem/-/issues/30

Description

Changes to attributes of natural persons (e.g. through marriage or change of gender) can have an impact on VCs that contain these attributes. We should therefore consider how to deal with such cases. The same applies to attributes of companies.

Conclusions, Next Steps and Recommendations

While we have gained an initial overview and understanding of the issue described above, further exploration and specification are necessary going forward.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Renewal of VC if the signatures become invalid

See https://code.europa.eu/ebsi/ecosystem/-/issues/31

Description

In cases where a VC contains the actual document (e.g. a school-certificate document (QEAA)), a long retention period is required depending on the legal basis. During this period, a signature originally used may become invalid for various reasons (no longer secure procedures, ...). We should consider how to proceed in such cases.

Conclusions, Next Steps and Recommendations

While we have gained an initial overview and understanding of the issue described above, further exploration and specification are necessary going forward.

Co-funded by
the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Conclusions

The authors of this EBSI-VECTOR deliverable D3.2 hope that it serves as a useful initial version of a document which explores new capabilities needed in the EBSI ecosystem. As mentioned before, the topics presented in this document have been mostly identified and selected by participants of tasks T3.1 themselves, with so far limited input about concrete business and technical requirements from the use case work packages WP4 and WP5.

The topics presented in this deliverable are at various stages of maturity when it comes to "being ready" for definitive specification and implementation of the new capabilities. Some topics have reached an advanced stage where they offer concrete solutions to the articulated problems (e.g. "JSON-LD VCs are NOT just JSON"). Others have reached intermediate approaches to solving problems that must be refined further (e.g. "Binding between an attestation credential and identity credential"). Yet others are at an early stage where a topic has been identified and possible solutions have been discussed, but no agreement has been reached yet on the exact nature of the new capabilities.

We intend that this deliverable D3.2 constitutes the initial version of what will be a living document for the remaining duration of the EBSI-VECTOR project and will later culminate in a final version as deliverable D3.9. In addition, we would like to remind readers that our first deliverable D3.1 should continue to be used as a reference regarding an evaluation of current EBSI capabilities and recommendations for improved and new capabilities.

As next steps, we are planning the following approach and priorities for our task T3.1:

- Continue to develop new capabilities that we have begun to explore in this document and that have not yet reached a final stage of specification and implementation.
- Continue to identify and select new capabilities that need to be developed.
- Contribute the new capabilities to EBSI in the form of structured EBSI Improvement Proposals (EBIPs) via the EBSI Ecosystem Gitlab platform[32].
- Align more closely with the use case work packages, to strictly prioritize new capabilities that will be prerequisites for the successful completion of EBSI-VECTOR. The business blueprint deliverables D4.1 and D5.1 by the use case work packages will serve as important input for this process. Also, the EBSI-VECTOR meeting in Rome on 18th – 19th

[32] https://code.europa.eu/ebsi/ecosystem/-/merge_requests/1

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

December 2023 has helped greatly to create a shared understanding of the alignment between use cases and new technical capabilities, and to improve organizational alignment and flow of information between the different tasks and work packages.

- Continue to align also with other relevant tasks of the EBSI-VECTOR project, e.g. T3.2 ("Develop an enterprise wallet and legal entities service) and T2.2 ("Interoperability").

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.