Using MultiBase Anchors within a Personally-Issued Endorsement Credential to Corroborate Attributes in an Existing Issued Credential

Authors: Phillip D. Long, Dmitri Zagidulin, Kerri Lemoie

A credential (either issued by an institution or self-issued) makes an assertion about the subject's knowledge, skills or abilities. The subject wishes to have a third-party corroborate this credential to give it greater credibility. The subject asks a selected third-party to "endorse" their credential, confirming the claims in the credential, and add additional supporting information about it.

For the purposes of VC-EDU, a practical use case is in the context of an endorser creating an endorsement single assertion Verifiable Credential (VC) that is cryptographically linked to an independently issued VC held by a holder. Here a MultiBasehash-linked approach to connect the two independent VCs is necessary to link the two in a tamper evident way.

Use Cases

1. Personally-Issued Credential + Third-party Personal Endorsement
2. Classic Organization-issued Credential + Third-party Personal Endorsement

The above use cases are actually equivalent, differing only in the original issuer. Note that the design intention, at least initially, is to enable third-party endorsements by individuals. ### Verifiable Endorsement

VCs by themselves are not sufficient to serve the endorsement use case - the Resource Anchoring and Hashlink mechanism is required.

A VerifiableEndorsement Credential is an application of the VC Data Model and a resource anchoring mechanism (via `digestMultibase`). It describes the bona fides of the endorser and enables them to convey their affirmation of support for an assertion made by an independently issued third-party credential (institutionally issued or self-issued) with sufficient granularity to endorse the entire credential or elements within it about which their expertise and their knowledge of the subjects expertise specifically pertains.

Conformance characteristics (of what makes a VerifiableEndorsement VC):

- VC Data Model 1.1 credential, of type `VerifiableEndorsement` and using the context `https://w3id.org/endorsement/v1`
- (Required) Refers to any third party VC (such as an OBv3 achievement), to a skill or statement within a VC, or to a non-VC artifact, by setting the endorsement's `credentialSubject.id` property *to the id of the target credential, claim, or artifact.*

- Defines a required `credentialSubject.endorsement` property, with the following sections:
  - An optional (but recommended) `endorser` property, used to specify `endorser.relevance`, which describes the endorser's bona fides and expertise in the domain in which they're making the recommendation, as well as the relationship of the endorser to the endorsee
  - An optional (but recommended) `evidence` property that lists various links, credentials and artifacts that support the endorsement, such as:
    * links to other relevant credentials
    * links to joint projects
    * listed from general domain to specific attributes associated with concrete endorsement
- Uses the `digestMultibase` Anchoring and Hashlinking mechanism to cryptographically bind the endorsement VC with any relevant evidence objects (Achievement credentials, non-VC objects such as PDFs, images, videos and so-on).

(See issue https://github.com/w3c/vc-data-model/issues/831 of the Verifiable Credentials Working Group 2.0 for more details on the anchoring and linking mechanism.) ### Related Work

This Verifiable Endorsement proposal adds to the space of general endorsements, by giving a granular, specific structure for making claims (by an endorser, of an endorsee). #### Open Badges v2

The OpenBadges v2 specification has a concept of an Endorsement type, which focuses on single assertion achievements. It enables endorsements of Achievements/Badge Classes, Assertions, Profiles, and CLRCredentials.

For example (see the Endorsement Examples section of the OBv2 spec):

1. To indicate trust in an email address.
2. As a comment to express approval of a Badge Class (the abstract achievement type), indicating that it is a "good representation of the achievement it describes".
3. As support for a single OBv2 achievement earned by a unique individual (by linking to an Assertion via claim.id). #### Open Badges v3

An Open Badges v3.0 (OBv3 for short) credential is a W3C VC that conforms to the 1EdTech's Open Badges v3.0 Specification. It is a VerifiableCredential that has either the "OpenBadgeCredential" or the "AchievementCredential" type (the two types are synonyms).

Each OBv3 VC has three components relevant to this paper:

1. A top-level optional VC.endorsement property (containing one or more full VCs of type "EndorsementCredential")
2. A top-level optional VC.evidence property ("A description of the work that the recipient did to earn the achievement. This can be a page that links out to other pages if linking directly to the work is infeasible.")

3. One or more VC.credentialSubject.achievement objects (of type "Achievement"). ##### OBv3 `endorsement` objects In addition to the top-level VC.endorsement property (which "[allows endorsers to make specific claims about the credential, and the achievement and profiles in the credential."), each achievement can have an optional endorsement property itself,

The endorsement property (either the top-level belonging to the VC, or belonging to a particular achievement) contains one or more full `EndorsementCredential` VCs (they are embedded in the overall OpenBadgeCredential VC).

Each of these embedded VCs of type `EndorsementCredential` have the following payload (based off the EndorsementCredential schema in OBv3) that are relevant to this paper:

1. A `credentialSubject.id`, which is "The identifier of the individual, entity, organization, assertion, or achievement that is endorsed."
2. A `credentialSubject.endorsementComment`, which is a human-readable comment in Markdown format. ##### OBv3 `evidence` objects The OBv3 `evidence` property contains one or more objects of type "Evidence" that have the following properties (based on the OBv3 Schema):

- An evidence `id` property, which is "The URL of a webpage presenting evidence of achievement or the evidence encoded as a Data URI."
- Several narrative properties that describe the evidence: `name`, `description` and/or `narrative`
- Also `genre` and `audience` properties (to further specify the evidence)

OBv3 summary The OBv3 spec defines an `EndorsementCredential` VC type, which are full VCs, always embedded in an `endorsement` property, either at the top level of a OBv3 VC, or inside a particular achievement.

These embedded `EndorsementCredential`s link to individuals, entities, assertions or achievements via `credentialSubject.id`, and also contain a human-readable endorsement descriptions in the `credentialSubject.endorsementComment` field.

Additionally, the OBv3 spec defines a top-level `evidence` property, which has one or more `Evidence` objects which link to and describe the work the subject did to earn the overall AchievementCredential. #### Difference between Verifiable Endorsements and the OBv3 `EndorsementCredential` mechanism

The VerifiableEndorsement proposal is inspired by the Open Badges v3.0 (OBv3 for short) specification. Our main motivation is to address what the OBv3 `EndorsementCredential` mechanism does not cover, and to provide a general-purpose anchoring, cryptographic binding, and endorsement mechanism available to the general VC community, including those outside of the education sphere.

This paper removes the limits of the OBv3 `EndorsementCredential` mechanism in the following ways:

Defines a *standalone* Verifiable Endorsement VC type, which does not have to be embedded in an OBv3 VC or achievement. Allows credentialSubject.id to reference non-VC artifacts such as PDFs, images, code repositories, and many others. Introduces the `endorser.relevance` property, which allows for specifying fine-grained bona fides on the part of the endorser. Whereas the OBv3 `evidence` property refers to various external evidence of the overall AchievementCredential, the `endorsement.evidence` property in this paper refers to external evidence of the endorsement itself. Adds a general-purpose `digestMultibase` cryptographic binding mechanism, used to anchor any sort of links (in `relevance`, `evidence` and any other sections) to their destination's exact contents.

In addition to being a more general-purpose standalone mechanism (unrelated to achievements or Open Badges), the Verifiable Endorsement proposal outlined in this paper attempts to serve a different Trust Model than that of the OBv3 spec. Due to its roots in the Issuer/Publisher model, Open Badges requires that the `EndorsementCredential` VCs (endorsing a particular achievement) are gathered before the issuing of the badge itself. That is, the Issuer of the badge embeds the endorsement VCs and signs over them in the main VC, and so they must be present at the time of issuing (when they are cryptographically "sealed").

In contrast, Verifiable Endorsements allow for obtaining endorsements after the issuance of the source material. That is, first a VC (describing an achievement, or any other domain) is issued or a PDF is created, and then the subject can go around asking relevant third parties to endorse it (or any components within it). We are aiming to model generic human trust relationships (such as when an individual calls on a third party to support or recommend their skills or abilities – see, for example, the References section in a resume), in addition to the more traditional trust in issuing institutions.

One of the side-effects (and in fact, the initial motivation for) the proposed model is that it enables self-issued claims and assertions to flourish as an ecosystem (supported by endorsements). ### Verifiable Endorsement Semantics

Verifiable Endorsements are intended to be a general purpose endorsement mechanism for the VC ecosystem. They are standalone Verifiable Credentials that can use the 'digestMultibase' anchor mechanism to endorse any other VC, claim, or non-VC artifact. In addition, Verifiable Endorsements have several supporting metadata sections that enhance the endorsement process, such as the `endorser.relevance` (providing the bona fides of the endorsing party), and a focus on the `endorsement.evidence` section (providing specific evidence artifacts that relate to the endorsement). ### Data Model Examples

We anticipate the wide adoption of OpenBadges v3 credentials as the format for skill or achievement assertions, either self-asserted or institutionally issued.

Example Self-issued OBv3 Credential:

```
{
  "@context": [
```

```
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/openbadges/v3"
  ],
  "type": [
    "VerifiableCredential",
    "OpenBadgeCredential"
  ],
  "issuer": {
    "type": "Profile",
    "id": "did:key:z6MkrHKzgsahxBLyNAbLQyB1pcWNYC9GmywiWPgkrvntAZcj",
    "name": "Alice Jones"
  },
  "issuanceDate": "2022-05-01T00:00:00Z",
  "credentialSubject": {
    "type": "AchievementSubject",
    // Note that the subject of the VC is the issuer, hence self-issued
    "id": "did:key:z6MkrHKzgsahxBLyNAbLQyB1pcWNYC9GmywiWPgkrvntAZcj",
    "achievement": {
    "id": "urn:uuid:e8096060-ce7c-47b3-a682-57098685d48d",
     "type": "Achievement",
     "name": "UAV Control System for Drone Navigation",
     "description": "<description goes here>",
     "criteria": {
        "type": "Criteria",
        "narrative": "<narrative>"
      }
    }
  },
  "proof": {
    // Signature goes here
  }
}
```

Example VerifiableEndorsement of the above VC (or rather, of the achievement within it):

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/endorsement/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "type": [
    "VerifiableCredential",
    "VerifiableEndorsement"
  ],
  "issuer": {
```

```
  "id": "did:web:bob.com",
  "name": "Bob"
},
"issuanceDate": "2010-01-01T00:00:00Z",
"expirationDate": "2020-01-01T00:00:00Z",
"credentialSubject": {
  // Note that the credentialSubject.id is the id of an individual Achievement in the targ
  // It could just as readily be the id of the VC, but the authors wanted to highlight tha
  "id": "urn:uuid:e8096060-ce7c-47b3-a682-57098685d48d",
  "digestMultibase": "zb1B1M6Bve5JEaNqeJSmuE",
  "endorsement": {
     "statement": "This is an endorsement regarding Alice's 'UAV Control System for Drone
    "endorser": {
      "id": "did:web:endorser.example.com",
      // the endorsing entity's bona fides, tailored to the specific endorsement area or d
      "relevance": [
         // Generic expertise claims (such as CV / resume / degrees)
         {
           "id": "https://SmartResume.com",
           "type": "SmartResumeProfile"
         },
         {
           "id": "https://linkedin.com/Bob",
           "type": "LinkedInProfile"
         },
         {
           // link to a credential I received saying I have a degree to this subject
           "id": "https://example.edu/degrees/class-of-2021/bob",
           "name": "University Degree Credential"
         },
         {
           "id": "https://sigspatial.acm.org/members/12345",
           "description":
                    "https://www.acm.org/special-interest-groups/sigs/sigspatial",
           "name": "SigSpatial Membership Credential"
         },
         // Specific expertise item tailored to the endorsement
         {
           "id": "https://example-journal.com/my-article.pdf",
            // optional hashlink (note that 'multibase' is a part of the in-progress
            // IETF spec https://datatracker.ietf.org/doc/html/draft-multiformats-multibas
           "digestMultibase":"zQmdfTbBqBPQ7VNxZEYEj14VmRuZBkqFbiwReogJgS1zR1n",
           "name": "Control Systems in Unmanned Flight",
           "citation": "...",
           "description": "I have published an article in a peer-reviewed journal."
         },
```

```
            // TODO: Add a CID / Ceramic link as an example.
          ]
        }
      }
    },
    "evidence": [
      {
        "id": "https://github.com/example-org/control-test-suite",
        "type": ["EndorsementEvidence"],
        "name": "Control System Test Suite",
        "description": "The code used to control a UAV delivering packages to an address.",
        "digestMultibase": "..."
      },
      {
         "id": "https://control-systems-journal.example.com/12345.pdf",
         "digestMultibase": "zQmdfRKkx7Uf8Rpr079Uh",
          "name": "Geopositioning in Control Systems",
          "citation": "...",
          "description": "A particularly insightful implementation of geopositioning with prec
      }
    ],
    "proof": {
      // Signature goes here
    }
}
```

Example Workflow / Protocol

TBA: Add a description + swimlane diagram for how Alice would request the endorser for the endorsement.

Q: If Alice issues a self-issued VC, and later gathers endorsements (from Bob), and later applies for a job, how does the verifier (HR software) collate / put together the original VC and its endorsements?

A: Several options, depending on the workflow:

Workflow 1. Bob sends his VerifiableEndorsement VCs directly to Alice. This way, Alice can submit a VerifiablePresentation as a bundle that contains *both* the self-issued VC and Bob's endorsement. Then, the HR/verification software verifies both credentials.

Workflow 2. Bob uploads his VerifiableEndorsement to his Google Drive, and just sends Alice a link to the uploaded endorsement. In this case, Alice has several options: a) she can just download the endorsement, and present it in the VerifiablePresentation just like in step 1. Or, b) she can include the link to the endorsement in the 'anchoredResource' section of the VerifiablePresentation that she presents to the verifier.

Workflow 3. Same as 2, but Bob sends the link to the endorsement directly to the verifier. In this case, the receiving HR person would add the link to their verification software, which would proceed as in variants 1 and 2. ### Notes on Tooling

We expect that adding endorsements to VCs will be another feature offered by various wallets. A marketplace of authoring services we hope to see develop that offers options for endorsement credential authoring and connects to wallets via the Issuer API.

Standalone Verification Software vs Integrated Verifiers <discuss the difference between verification built in directly into existing HR suites etc, vs HR person using an external standalone app (website or mobile).>

Notes on Wallets <discuss what features need to be added to the wallets to support workflows 1 and 2 above. (for example, an extra textbox where Alice can add links to endorsements when making the Verifiable Presentation)>

Summary

This example of endorsement is intended to convey one of several potential use cases for the evidence-based corroboration of statements made in one credential by an endorser authoring a VC that allows the granular affirmation of elements within the endorsee's issued credential using a proofing method that links the two credentials together, based on the affirmation of the endorser's selection about which they are knowledgeable. It provides context for the endorser's relevance or background to make those judgements and encourages the inclusion of evidence from the endorser's own direct experience and artifacts relevant to the endorsee"s claim.