LVCSP TC Meeting Minutes V3

Meeting date: October 24, 2023

Note: Revised standard format for this version with minor updates.

1 Call to order

Quorum: yes

Attendees: Alan Bachmann (Chair), Abbie Barbir (Secretary), Don Sheppard (Editor), Stefan Hagen (Editor), Chris Dotson, Spencer Yezo, Hiroshi Takechi, Charles Hart, Ryan Rowcliffe

2 Approval of agenda

Approved – no detailed agenda, no items added

3 Approval of previous minutes

Previous minutes approved as written

3.1 Review of action items

No list of actions from the previous meeting available.

4 Topic Discussions

4.1 Update from the editor

- Don is now attending meetings - first 3 meetings were September 26, October 10 and October 24
- Don has reviewed the TC charter, scope and deliverables
- Stefan and Michael volunteered to be editors
- Don established email connections with the editor team (Don, Stefan and Michael)
- A quick review of available meeting minutes determined that these minutes were not very useful for compiling existing working agreements
- Don's initial reading suggests that the goal of the current work is to provide one (1) document that:
    - Specifies a schema for a lightweight VC (LVC) that is issued after completion of an identity verification process
    - Provides a security analysis of the LVC schema
    - Describes how a Relying Party would verify the LVC
    - Provides example use cases
- It was not yet clear to the editor what makes this "lightweight" – this could be included in an introduction to the standard.

4.2 Background update

Abbie provided a verbal summary of the TWG's prior agreements that will be the basis for the current work.

See below for a summary of agreed concepts and principles.

4.3 KYC Form

Abbie introduced a sample KYC in-person form for individuals and reviewed the fields contained in the form. Abbie recommended that the group examine this form and decide what items need to be included in the VC for LVCSP and be prepared to discuss in-depth at the next meeting.

https://www.camsonline.com/Investors/Service-requests/Service-Request-Forms/CAMSKRA-KYC-Non-Individuals

5 Meeting outputs

5.1 Motions approved

Motion 1:

The LVCSP TC requests the OASIS administration to create a GitHub repository https://github.com/oasis-tcs/lvcsp to manage LVSCP spec related work products including schema files, specification prose, test files, minutes of meeting, issues, peer reviews, IANA requests and others.

Moved: Stefan Hagen Seconded: Abbie Barbir **Approved**

Motion 2:

The LVSCP TC requests Stefan Hagen to submit the relevant form at

https://www.oasis-open.org/project-administration-support-requests/form-request-a-tc-github-version-control-instance-be-created/ such that OASIS administration can create the repository and enable the maintainers access. The initial maintainer shall be Stefan Hagen.

Moved: Stefan Hagen Seconded: Abbie Barbir **Approved**

5.2 Agreements on topics

Use cases were discussed briefly in relation to the KYC form (see 4.3 above). The proposed standard should include 3 use cases: General/Core, Healthcare, and Financial

See list below.

5.3 Actions arising from this meeting

See list below

6 Other business

No other business

7 Next meeting

November 7, 2023, at 0930 ET

8 Close of meeting

Meeting ended at 1023 EDT

Attachment 1 Actions list

1. Stefan to submit form to OASIS admin to initiate GitHub request and become maintainer
2. OASIS admin to establish a GitHub repository

3. The TWG members should examine the CAMSKRA KYC form to decide what items need to be included in the VC for LVCSP and be prepared to discuss in-depth at the next meeting. Members to consider the elements of the KYC VC using the CAMSKRA form as a starting point.

4. Don to publish the minutes of the meeting

Attachment 2 Consensus agreements list

1. The standard will include 3 use cases: General/Core, Healthcare, and Financial

Attachment 3 Overview of basic principles (provided by Abbie)

<u>General assumptions</u>

- Start with JSON and will not use JSON-LD
- Scheme changes are not negotiable – credentials do not have optional elements
- Work with OpenID format
- Use cases will use JWT tokens
- Base core schema is to be based on IANA
- A meta decision is that you cannot trust the VC presenter
- Atomic credentials/Oracle credentials are based on templates with the minimum number of attributes needed
- Assurance Level of the template will be based on OpenID – the Issuer will have levels 1,2 and 3
- Specifications from DIF include a Manifest and a Verifiable Presentation – LVCSP has dropped the Manifest as it will lead to complex claims and only needs to worry about the Verifiable Presentation
- The anchor of trust is based on what the credential is used for – we are looking for the minimum viable solution
- Our core assumption is that we will depend on trust in the Issuer
- Elements in the core credential are specified and should be designed to work with 90% of the use cases
- If a required element is not in the credential, then the Issuer can attest it, and the Verifier can choose to accept the Issuer's attestation – this simplifies the wallet
- What makes our proposed standard "lightweight"?
    - The credential has only the core elements
    - The wallet is not "heavy"
    - We don't need governance
    - The subject (user?) should already have a DID
- Need to place emphasis on protecting PII – ask for the minimum information needed to do the job, not a full blown generic solution
- We won't rely on meeting all the W3C needs
- We should allow a credential broker so that the Issuer cannot track all uses of the credential (refer to the ADIA spec.)

<u>Wallet assumptions</u>

- User wallet cannot be trusted to do anything except present a subset of its credentials.
- Verifier will have restrictions and should not have to trust the user's wallet
- The Verifier MUST not accept anything from the wallet except VC's from the Issuer
- The wallet presents the VC to the Verifier
- PKI security is anchored on the wallet, but the wallet does not make changes to anything

KYC assumptions

- There are 2 kinds of KYC – Individual and non-Individual
- KYC can be achieved in 2 ways – in-person and remote
- Credentials should say what process was used to determine KYC
- The CAMSKRA for has 2 parts – the actual identity, and the proof of identity
- (for example – residence address, and proof of residence)