verifiable LEI (vLEI) Ecosystem Governance Framework Technical Requirements Part 2: vLEI Credentials

verifiable LEI (vLEI) Ecosystem Governance Framework Credential Technical Requirements

This Controlled Document will cover all policies regarding the technical requirements for the vLEI family of Authentic Chained Data Container (ACDC) Credentials, v0.1.

I. CREDENTIAL SPECIFICATIONS

The following policies are necessary to achieve, in order of priority, the security, performance and usability requirements for the vLEI Ecosystem.

A. Specification References

vLEI Credentials rely on the following specifications.

1. JSON Required https://datatracker.ietf.org/doc/html/rfc7159
2. JSON Schema Version 2020-12 https://json-schema.org/draft/2020-12/json-schema-core.html
3. Composable Event Streaming Representation (CESR) Specification https://github.com/WebOfTrust/cesr
4. Attributable Identifiers (AIDs) (also known as Autonomic Identifiers) for Issuers and Holders using the did:keri Method (secure attribution) https://github.com/WebOfTrust/aid
5. KERI Decentralized Identifiers (AIDs) did:keri Specification https://github.com/WebOfTrust/did-keri
6. Self Addressing Identifiers (SAIDs) https://github.com/WebOfTrust/said
7. Schema Immutability Specification (SIS) https://github.com/WebOfTrust/sis
8. Composable Event Streaming Representation (CESR) Proof Format https://github.com/WebOfTrust/cesr-acdc-proof
9. ToIP Authentic Chained Data Container (ACDC) Specification https://github.com/trustoverip/TSS0033-technology-stack-acdc
    I. (Informative) JSON required as defined in https://www.w3.org/TR/vc-data-model/#json
        i. Exception @context MUST NOT be included.
10. Issuance Exchange Protocol Specification for ACDC and KERI (Key Event Receipt Infrastructure) https://github.com/WebOfTrust/keripy/blob/master/docs/Peer2PeerCredentials.md
11. Presentation Exchange Protocol Specification for ACDC and KERI
        i. WACI PEx https://github.com/decentralized-identity/waci-presentation-exchange

12. Public Transaction Event Log (PTEL) Specification

B. SPECIFICATION VERSION UPGRADES

These policies govern migrating to revisions of the Credential specifications.

Previous versions explicitly cited by policies in this document MUST be supported for a period 18 months.

New versions MUST be implemented within a period 12 months after final approval of the new version, unless otherwise superseded by revised policies in a new version of the vLEI Ecosystem Governance Framework.

After upgrading to a new version, implementers MUST NOT begin using any breaking changes until the end of the time period required to adopt new versions. For example, v2.0 must be compatible with v1.0 until the end of the v2.0 adoption period. So v2.0 must be used in a v1.0 compatible mode.

II. SECURITY AND PRIVACY

Required Cryptographic Suites and Security

- All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.
- All vLEI Credential schema MUST be SIS compliant.
- All instantiated vLEI Credentials MUST be ACDC compliant.
- All SAIDs MUST use the cryptoBlake3-256 digest.

The Legal Entity Engagement Context Role vLEI Credentials MAY include PII (personal identifying information) and may therefore require some form of privacy protection.

In the future, this privacy protection MAY be provided by the combination of three mechanisms:

- Chain link confidentiality imposed by the ACDC rules section of the vLEI.
- Hidden attributes ACDC.
- Hidden TEL revocation registry for that credential.

Alternatively, vLEI credentials issued using a KERI tunnel on an Indy compliant ledger may use AnonCreds1 and the Indy revocation registry.

III. REQUIREMENTS FOR VLEI ACDCS

The ACDC specification is provided here: https://www.w3.org/TR/vc-data-model/#json

1. Issuer and Holder Identifiers MUST be KERI AIDs that use the did:keri Method.
2. All vLEI Credentials MUST include an ACDC version string field.
3. All vLEI Credentials MUST support JSON serialization.

3.1 Additional serializations MAY be introduced at a later time.

4. All vLEI Credentials MUST include a SAID (as evidence of immutablity).
5. The following ACDC sections MUST include a SAID.
   - Attribute (data payload) section
   - Schema section
   - Rules section
6. Subsections of the preceding sections MAY include a SAID.
7. All source links MUST include the SAID of the referenced ACDC.
8. ACDCs have three primary forms that MUST be supported separately by Issuers, Holders and Verifiers using the following rules.

   Form 1 – the Fully-expanded Form in which the schema, attributes and rules are fully expanded and embedded.

   Form 2 – the Fully-compressed Form in which only the SAID of each major section is included.

   Form 3 – Schema-compressed Form so the only the SAID of the schema section is included.
9. Issuers MUST support the issuance of vLEI Credentials in any or all three forms.
10. Issuers MUST provide the SADs at issuance to Holders when issuing forms 2 and 3, by either including the SAD in the presentation or including a reference to the highly-available service endpoint from which the SAD can be retrieved.
11. Verifiers SHOULD support the verification at presentation of vLEI Credentials in any of the three forms.
12. Holders SHOULD provide the SADs to Verifiers when presenting forms 2 and 3, by either including the SAD in the presentation or including a reference to the highly-available service endpoint from which the SAD can be retrieved.
13. vLEI Credential Issuers SHOULD use the Rules section of the credential in accordance with the ACDC specification to impose restrictions on the use of the credential or its attributes.
14. vLEI Credential Issuers SHOULD use the Sources section of the credential in accordance with the ACDC specification to impose delegated authorization restrictions on the use of the credential and/or in conjuction with policy statement 13 above.

IV. VLEI CREDENTIAL SCHEMA

1. vLEI Credential schema MUST be compliant the SAID and SIS specifications.
2. All vLEI Credential schema MUST include a SAID (as evidence of immutablity).
3. Each vLEI Credential MUST be in compliance with its specific vLEI Credential Govenance Framework.

3.1 Each vLEI Credential MUST be chained to its source(s), if any, as required by the applicable vLEI Credential Govenance Framework in accordance with the ACDC specification.

V. COMPOSABLE EVENT STREAMING REPRESENTATION (CESR)

1. The Proof Format for vLEI Credentials MUST comply with the Composable Event Streaming Representation (CESR) Proof Format specificiation.

   1.1 Additional proof formats MAY be introduced at a later time.

VI. CREDENTIAL ISSUANCE AND REVOCATION REGISTRY REQUIREMENTS

1. Each vLEI Credential Issuer MUST maintain a highly-available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.
2. Infrastructure for the available issuance and registration registries MAY be shared.
3. Support for privacy-preserving issuance and revocation MAY be supported at a later time.

VII. EXCHANGE PROTOCOLS

1. vLEI Credential Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.
2. vLEI Credential Holders SHOULD comply with the Issuance Exchange Protocol Specification for ACDC and KERI.
3. vLEI Credential Holders and Verifiers SHOULD comply with the Presentation Exchange Protocol Specification for ACDC and KERI.