CCI Verifiable Credentials Flavors Explained (Infographic)

Verifiable Credentials (VCs) are a standardized data model with broad expressive capacity (see how VCs work on the right). They can be used by many different industries and contexts. Credentials created for one narrow purpose can be used for another at the discretion of their holder or subject of the credentials, requiring no technical federation to the originating issuers.

VCs were standardized by W3C, an international community that develops open standards to ensure the long-term growth of the Web. The VC data model 1.0, published in 2019, offers optionality for credential formats, with the three predominate ones JSON-JWT, JSON-LD with LD Signature, and ZKP(Zero Knowledge Proof)-CL. A year ago, JSON-LD ZKP with BBS+ was innovated to bridge the gap between the the most promising formats, JSON-LD with LD Signature and ZKP-CL, and reconciled the technical differences between two while managing to retain their key merits. Kaliya Young, CCI's Ecosystems Director, wrote a paper explaining the different formats (https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf), based on which we created this infographic to provide a simplified view of why we believe the community should converge on JSON-LD ZKP with BBS+.

Verifiable Credential
- Credential Metadata
- Claim(s)
- Proof(s)

Verifiable Credential

Holder

Verifiable Presentation

Trust
No direct integration or third party intermediary

Issuer

Verifier

Verifiable Presentation
- Presentation Metadata
- Verifiable Credential(s)
- Proof(s)

	JSON - JWT	JSON-LD with LD Signature	ZKP- CL	JSON-LD ZKP with BBS+
Summary	**Simplicity:** Simplest among all **Privacy Preserving: No** - Selective Disclosure: No - Zero Knowledge Proof: No - Need to Reveal Persistent Identifier: Yes **Semantic Disambiguation: No**	**Simplicity:** Relatively simple **Privacy Preserving: No** - Selective Disclosure: No - Zero Knowledge Proof: No - Need to Reveal Persistent Identifier: Yes **Semantic Disambiguation:** Yes	**Simplicity:** Most complicated among all **Privacy Preserving:** Yes - Selective Disclosure: Yes - Zero Knowledge Proof: Yes - Need to Reveal Persistent Identifier: No **Semantic Disambiguation:** No	**Simplicity:** Complicated **Privacy Preserving:** Yes - Selective Disclosure: Yes - Zero Knowledge Proof: Not yet - Need to Reveal Persistent Identifier: No **Semantic Disambiguation:** Yes
Verifiable Credential (Issued by the issuer)	Persistent DID **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **JWS in a JWT** Entire credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	Linked Data Context — Points to unambiguous IRI references for terms in the credential Persistent DID **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **LD Signature** Entire credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	an Indy Ledger LINK SECRET **CREDENTIAL DEFINITION** **SCHEMA DEFINITION** — Both posted to **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **CL Signature** **CL Signature** **CL Signature** Each claim on credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	Linked Data Context — Points to unambiguous IRI references for terms in the credential LINK SECRET **@Context: URLs to find definitions** **@Type; Job** **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **BBS+ Signature** **BBS+ Signature** **BBS+ Signature** Each claim on credential signed by issuer with its private key, associated with the paired public key pair in DID Document.
Verifiable Presentation (Presented to the Verifier)	Persistent DID **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **JWS in a JWT** Signed by the holder with a nonce from the verifier so that it can't be replayed. The holder can only present the entire credential as a verifiable presentation even if some data attributes are not needed for the verification.	Linked Data Context — Points to unambiguous IRI references for terms in the credential Persistent DID **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **LD Signature** Signed by the holder with a nonce from the verifier so that it can't be replayed. The holder can only present the entire credential as a verifiable presentation even if some data attributes are not needed for the verification. The verifer can choose to (but not necessarily have to) expand terms in the credential with the IRI references.	an Indy Ledger LINK SECRET **CREDENTIAL DEFINITION** **SCHEMA DEFINITION** — Both posted to **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director **CL Signature** **CL Signature** The holder can only present the data attributes in the needed for the verification instead of the entire credential. The verifier uses the Credential Definition and Schema Definition from the ledger and the public keys found in the DID Document of the issuer to do the crytographic calculations needed for verification.	Linked Data Context — Points to unambiguous IRI references for terms in the credential LINK SECRET **@Context: URLs to find definitions** **@Type; Job** **Name: Value Pairs** Name: Kaliya Organization: CCI **BBS+ Signature** **BBS+ Signature** The holder can only present the data attributes the needed for the verification instead of the entire credential. The verifer can choose to (but not necessarily have to) expand terms in the credential with the IRI references.