Schemas

Suggest Edits

The following schemas are used in Verite's implementation.

KYC/AML Attestation

Purpose

Represents an attestation a KYC/AML process has been performed according to a specified defined process. A KYC/AML process is defined at the country-level, referenced as linked data.

The KYC/AML attestation structure is intended to address regulatory compliance only, and not filtering on additional personal data attributes. An example of the latter is filtering out users based on state residence for idiosyncratic compliance purposes. This distinction helps reduce required attributes about the credential subject (and finer-grained personal data) within the credential.

Example

JSON { "type": "KYCAMLAttestation", "process": "https://verite.id/definitions/processes/kycaml/0.0.1/usa", "approvalDate": "2021-08-25T02:13:43.387Z" }

Attributes

"type" Attribute

The "type" attribute MUST be "KYCAMLAttestation". Use of this attribute is REQUIRED.

"process" Attribute

The "process" attribute is used to define which KYC/AML process was performed. The "process" attribute value is a stringOrURI referencing the KYC process performed. Use of this attribute is REQUIRED.

"approvalDate" Attribute

The "approvalDate" attribute is used to define the date of KYC/AML process completion, which may be on or before the issuanceDate of the credential (in the outer VC wrapper). The "approvalDate" attribute value is an ISO 8601-formatted string. If not present, then the attribute value is assumed to be the same as the Verifiable Credential issuance date. Use of this attribute is OPTIONAL.

Recommendations

- Issuers take responsibility for revoking issued credentials due to updates to sanctions lists
- Verifiers must ensure they update verification results per updated issuer actions
- Verifiers are expected to determine fitness-for-purpose based on awareness of process definitions
- Additional details obtained during the KYC/AML process should not be included in the attestation. For example, service provider scores are not needed and will leak personal information.
- Support for use cases that require additional data (such as residency information) should be accomplished in ways that enable the subject to provide the least amount of data required. This may be accomplished with ZKPs or by issuing separate credentials containing the additional attributes, enabling wallet aggregation of minimal required data.

Verite's initial release contained only one sample USA KYC/AML process definition intended to cover all data points checked by at least the Pareto-majority of (if not all) US issuers (referred to in sample credentials ashttps://github.com/circlefin/verite/blob/main/packages/docs/static/definitions/processes/kycaml/0.0.1/usa .>Additional process definitions are expected to be developed based on existing practices/requirements per country or jurisdiction, as needed, by issuers moving to production on the basis of Verite semantics. While interoperability is best helped by a single, minimalist process definition that applies to a common set of checks and data points most or all KYC providers in a given jurisdiction, it may some day be necessary for issuers to publicize additional processes per jurisdiction should business processes differ significantly between issuers interested in participating.

Additional Considerations

This schema does not include attributes about the authority that executed the KYBP process, which may be separate from the issuer of the claim. This design enables minimal disclosure of data while satisfying use cases in which a relying party considers the issuer authoritative for KYBP credentials it issues. It allows relying parties to differentiate among which

country-specific KYBP process the credential applies to, but not learn anything else about the executing authority.

This pattern is well-suited for approaches in which allow-lists of trusted issuing authorities is available, but is available as a general, non-centralized, pattern that allows implementors to decide whom to trust.

KYBP/AML Attestation

Purpose

Represents an attestation that a Know-Your-Business-Partner process, which includes a KYC/AML check on any named representative individuals (see above), has been performed according to a specified, defined process. Like the KYC/AML processes it automatically entails, each KYBP process is defined at the country-level, referenced as linked data.

The KYBP/AML attestation structure is intended to address regulatory compliance only, and not filtering on additional personal data attributes. An example of the latter is filtering out users (in this case, legal persons) based on incorporation jurisdiction for more specific compliance purposes like tax reporting or jurisdiction-specific regulations. This distinction helps reduce required attributes about the credential subject (and finer-grained personal data) within the credential. It is assumed in our design that should such finer-grained filters need to be applied, they would happen at a later stage or process; additional credential types and flows can be established over time to address such cases.

Example

JSON { "type": "KYBPAMLAttestation", "process": "https://verite.id/definitions/processes/kycaml/0.0.1/generic--usa-legal_person", "approvalDate": "2021-08-25T02:13:43.387Z" }

Attributes

"type" Attribute

The "type" attribute MUST be "KYBPAMLAttestation". Use of this attribute is REQUIRED.

"process" Attribute

The "process" attribute is used to define which KYC/AML process was performed. The "process" attribute value is a stringOrURI referencing the KYC process performed. Use of this attribute is REQUIRED.

"approvalDate" Attribute

The "approvalDate" attribute is used to define the date of KYC/AML process completion, which may be on or before the issuanceDate of the credential (in the outer VC wrapper). The "approvalDate" attribute value is an ISO 8601-formatted string. If not present, then the attribute value is assumed to be the same as the Verifiable Credential issuance date. Use of this attribute is OPTIONAL.

Recommendations

- Issuers take responsibility for pro-actively revoking issued credentials due to updates of sanctions lists
- Verifiers must ensure they update verification results per updated issuer actions (e.g. periodically re-querying status properties of revocable credentials)
- Verifiers are expected to determine fitness-for-purpose based on awareness of process definitions per use case & per context, and/or check issuers against allowlists or registries
- Additional details obtained during the KYBP/AML process should NOT be included in the attestation. For example, service provider scores are NOT needed and will leak personal information.
- Support for use cases that require additional data (such as residency information) should be accomplished in ways that enable the subject to provide the least amount of data required. This may be accomplished with ZKPs or by issuing separate credentials containing the additional attributes, enabling wallet aggregation of minimal required data.

Note that the KYBP credential assumes that a KYC process has been run on listed representatives; for this reason, the process defition for KYBP includes a section defining the constituent checks run on said representatives (seehttps://github.com/circlefin/verite/blob/main/packages/docs/static/definitions/processes/kycaml/0.0.1/generic--usa-legal_person . Additional process definitions are expected to be developed based on existing practices/requirements per country or jurisdiction, as needed, by issuers moving to production on the basis of Verite semantics. While interoperability is best helped by a single, minimalist process definition that applies to a common set of checks and data points most or all KYC providers in a given jurisdiction, it may some day be necessary for issuers to publicize additional processes per jurisdiction should business processes differ significantly between issuers interested in participating.

Additional Considerations

This schema does not include attributes about the authority that executed the KYC process, which may be separate from the issuer of the claim. This design enables minimal disclosure of data while satisfying use cases in which a relying party considers the issuer authoritative for KYC credentials it issues. It allows relying parties to differentiate among which country-specific KYC process the credential applies to, but not learn anything else about the executing authority.

This pattern is well-suited for approaches in which allow-lists of trusted issuing authorities is available, but is available as a general, non-centralized, pattern that allows implementors to decide whom to trust.

When used as inputs by verifiers into verification registries, the auditing/forensics flow would look like this:

- Auditor flags record or set of records in the registry by uid(s)
- Verifier looks up (offline) the original VCs corresponding to the uids
- Each VC contains its id and information about its issuer. Information needed to contact the issuer must be resolvable in one of the following ways:* DID method
-
    - Issuer properties in the VC (i.e., in the "issuer" object of the VC)
-
    - Other "registry" information stored by verifiers when deciding which issuer VCs to accept
- Lastly, auditor contacts the issuer(s) for subject data corresponding to the VC id.

[See further discussion of registry forensics flows]

Address Ownership

Purpose

Expresses proof of ownership of an address for any chain that uses public-private key cryptography in address ownership.

This schema avoids arbitrary signatures and promotes an interoperable approach to proving address ownership. It is useful when embedded in other schemas and protocols (such as the counterparty exchange protocol and the credit score schema).

Proofs of control using both single-key and multiple-key ("multi-sig") variants are supported.

Example

JSON { "type": "AddressOwner", "chain": "ethereum-goerli", "address": "0x967af20D190EE4558Fd218A8B0be4065beEfCAce", "proof": "xyz" }

Attributes

"type" Attribute

The "type" attribute MUST be "AddressOwner". Use of this attribute is REQUIRED.

"chain" Attribute

The "chain" attribute is used to define which blockchain the attestation is applicable to. The "chain" attribute value is a case-insensitive string containing the full name of the chain. The full name of the chain MUST be formed by concatenating the primary name (e.g., "ethereum"), hyphen ("-"), and the testname name (e.g., "goerli"); e.g., "ethereum-goerli"). Use of this attribute is REQUIRED.

"address" Attribute

The "address" attribute is used to define the address on the indicated chain. The "address" attribute value is a string containing the chain address, formatted according to the requirements of the corresponding chain. Use of this attribute is REQUIRED.

"proof" Attribute

The "proof" attribute is used to define the proof of address ownership. The "proof" attribute value is generated by first concatenating the chain, the address, and the claim issuanceDate, then signing the result with the private key, or combination of keys, that owns the public chain address. Use of this attribute is REQUIRED.

Recommendations

- A credential containing an
- AddressOwner

- attestation SHOULD be considered a snapshot of address ownership at a point in time.
- Issuers SHOULD prefer setting a quick expiration on an
- AddressOwner
- attestation credential (rather than rely on credential revocation)

Counterparty Compliance

Purpose

Describes an attestation of Counterparty PII used for originators and beneficiaries of transactions that trigger counterparty exchange requirements, such as the US Travel Rule and the FATF InterVASP message requirements.

Example

JSON { "type": "CounterpartyAccountHolder", "legalName": "Some Account Holder", "address": { "type": "PostalAddress", "addressCountry": "United States", "addressLocality": "Mountain View", "addressRegion": "CA", "name": "Some Account Holder", "postOfficeBoxNumber": "321", "postalCode": "12345" }, "accountNumber": "12345678" }

Attributes

"type" Attribute

The "type" attribute MUST be "CounterpartyAccountHolder". Use of this attribute is REQUIRED.

"legalName" Attribute

The "legalName" attribute is used to define the legal name of the subject entity, referred to as 'name of transmittor | recipient' in Travel Rule terminology. The "legalName" attribute value is a string containing the subject's full legal name. Use of this attribute is REQUIRED.

"address" Attribute

The "address" attribute is used to define the postal address of the subject entity. The "address" attribute value is of type schema.org/PostalAddress. Use of this attribute is REQUIRED.

"accountNumber" Attribute

The "accountNumber" attribute is used to define the subject's account number with the issuer/provider or on-chain. If on-chain, this MUST be a public address (e.g., an eth account) and duplicated from the data in the accompanying transaction. The "accountNumber" attribute value is a string. Use of this attribute is REQUIRED.

"accountSource" Attribute

The "accountSource" attribute is used to define the context for the account, with the name of issuer, provider, or chain. This corresponds to 'identity of the financial institution' in Travel Rule terminology. If omitted, it is the issuer DID in the VC. This property provides context for the accountNumber property. The "accountSource" attribute value is a string. Use of this attribute is OPTIONAL.

"legalID" Attribute

The "legalID" attribute is used to define the identifier of the subject. The "legalID" attribute value is a string containing either a DID or a provider-specific customer ID. If omitted, it is assumed to be the subject DID in the encompassing VC. Use of this attribute is OPTIONAL.

Recommendations

A credential containing an CounterpartyAccountHolder attestation contains sensitive personal information. In current uses, it SHOULD be generated dynamically in the context of transactions and shared only between valid counterparties. Updated5 months ago * Table of Contents * * KYC/AML Attestation * * * Purpose * * * Example * * * Attributes * * * Recommendations * * * Additional Considerations * * KYBP/AML Attestation * * * Purpose * * * Example * * * Attributes * * * Recommendations * * * Additional Considerations * * Address Ownership * * * Purpose * * * Example * * * Attributes * * * Recommendations * * Counterparty Compliance * * * Purpose * * * Example * * * Attributes * * * Recommendations