Message Formats & Samples

Suggest Edits

Credentials

Verifiable Credential

The following represents the "intermediate" did-jwt-vc decoded form of a JWT-encoded verifiable credential, i.e., the form with mandatory JWT payload properties duplicated and translated into their VC data model equivalents for interoperability with non-JWT VCs:

JSON { "nbf": 1674267289, "iss": "did:key:z6MkmaeU7gzC8xhemRVEgSs1fz4fWxJJGcYHhwiFd6jJsWRZ", "sub": "did:key:z6MktPy7D89A4S3Nrvw6cRh4V9LQGpidTdgKXtA4m13sv58t", "exp": 1679451289, "vc": { "@context": ["https://www.w3.org/2018/credentials/v1", { "@vocab": "https://verite.id/identity/" }], "type": ["VerifiableCredential", "KYCAMLCredential"], "credentialSubject": { "id": "did:key:z6MktPy7D89A4S3Nrvw6cRh4V9LQGpidTdgKXtA4m13sv58t", "KYCAMLAttestation": { "type": "KYCAMLAttestation", "process": "https://verite.id/definitions/processes/kycaml/0.0.1/usa", "approvalDate": "2023-01-21T02:14:49.270Z" } }, "issuanceDate": "2023-01-21T02:14:49.270Z", "issuer": { "id": "did:key:z6MkmaeU7gzC8xhemRVEgSs1fz4fWxJJGcYHhwiFd6jJsWRZ" }, "credentialSchema": { "id": "https://verite.id/definitions/schemas/0.0.1/KYCAMLAttestation", "type": "KYCAMLAttestation" }, "expirationDate": "2023-03-22T02:14:49.270Z" } } With JWT Header:

JSON { "alg": "EdDSA", "typ": "JWT" }

Verifiable Credential with status

This extends the above to add credential status. Note that the credential status has not been dereferenced (i.e., "fetched" as a bitstring and validated), which some systems might want to do before processing and/or storing the credential.

JSON { "nbf": 1674267289, "iss": "did:key:z6MkmaeU7gzC8xhemRVEgSs1fz4fWxJJGcYHhwiFd6jJsWRZ", "sub": "did:key:z6MktPy7D89A4S3Nrvw6cRh4V9LQGpidTdgKXtA4m13sv58t", "exp": 1679451289, "vc": { "@context": ["https://www.w3.org/2018/credentials/v1", { "@vocab": "https://verite.id/identity/" }], "type": ["VerifiableCredential", "KYCAMLCredential"], "credentialSubject": { "id": "did:key:z6MktPy7D89A4S3Nrvw6cRh4V9LQGpidTdgKXtA4m13sv58t", "KYCAMLAttestation": { "type": "KYCAMLAttestation", "process": "https://verite.id/definitions/processes/kycaml/0.0.1/usa", "approvalDate": "2023-01-21T02:14:49.270Z" } }, "issuanceDate": "2023-01-21T02:14:49.270Z", "issuer": { "id": "did:key:z6MkmaeU7gzC8xhemRVEgSs1fz4fWxJJGcYHhwiFd6jJsWRZ" }, "credentialSchema": { "id": "https://verite.id/definitions/schemas/0.0.1/KYCAMLAttestation", "type": "KYCAMLAttestation" }, "credentialStatus": { "id": "http://192.168.1.11:3000/api/demos/revocation/22364811-e75d-4877-a5ca-b906527f5f98#97903", "type": "StatusList2021Entry", "statusPurpose": "revocation", "statusListIndex": "97903", "statusListCredential": "http://192.168.1.11:3000/api/demos/revocation/22364811-e75d-4877-a5ca-b906527f5f98" }, "expirationDate": "2023-03-22T02:14:49.270Z" } } With JWT Header:

JSON { "alg": "EdDSA", "typ": "JWT" }

Encoded JWT

The JWT encoded version of the previous example is below:

eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2Nzk0NTEyODksInZjIjp7IkBjb250ZXh0IjpbImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L2NyZWRlbnRpYWxzL3YxIix7IkB2b2NhYiI6Imh0dHBzOi8
HDLdVS9iW3kP0-12Qm8de56boNbRtowVVFlpmSJk4piNmHVQysN_iWTfCw

Issuance

Credential Offer

Verite's Credential Offer structure is a simple JWM wrapper around a DIF Credential Manifest.

JSON { "id": "4487e7d1-7d10-4075-a923-bae9332266c1", "type": "CredentialOffer", "from": "did:key:z6Mkgw8mPijYRa3TkHSYtQ4P7S2HGrcJBwzdgjeurqr9Luqb", "created_time": "2021-09-14T01:22:05.816Z", "expires_time": "2021-10-14T01:22:05.816Z", "reply_url": "http://example.com/api/issuance/eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MzE1ODI0MjUsImV4cCI6MTYzMTU4NjAyNSwic3ViIjoiMTUxOGNkNjEtNGFlNC00YmYwLTgzZDAtMjllMTE1N "body": { "challenge": "d273da29-74dd-46de-a53c-1677c51cc700", "manifest": {} } } Details:

- from
- : who the message is from; in this case, the issuer
- reply_url
- : the URL the wallet should send the credential application to
- body.challenge
- : a challenge the wallet should sign when proving control, to prevent replays
- body.manifest
- : this follows the DIF Credential Manifest spec

Credential Manifest

Example DIF Credential Manifest for a KYCAMLAttestation issued by a fictional issuer, Example Inc. Notice the descriptive text found in the output descriptors, which can be used by wallets to render details about the credential being issued. The presentation definition describes the inputs necessary to receive a credential. In this case, it is a Verifiable Presentation with no credentials, which is sufficient to prove control over the presentation holder's did.

JSON { "id": "KYCAMLManifest", "version": "0.1.0", "issuer": { "id": "did:web:demos.verite.id", "name": "Verite", "styles": {} }, "format": { "jwt_vc": { "alg": ["EdDSA"] }, "jwt_vp": { "alg": ["EdDSA"] } }, "output_descriptors": [{ "id": "KYCAMLCredential", "schema": "https://verite.id/definitions/schemas/0.0.1/KYCAMLAttestation", "name": "Proof of KYC from Verite", "description": "Attestation that Verite has completed KYC/AML verification for this subject", "display": { "title": { "text": "Verite KYC Attestation" }, "subtitle": { "path": [".approvalDate", ".vc.approvalDate"], "fallback": "Includes date of approval" }, "description": { "text": "The KYC authority processes Know Your Customer and Anti-Money Laundering analysis, potentially employing a number of internal and external vendor providers." }, "properties": [{ "label": "Process", "path": [".KYCAMLAttestation.process"], "schema": { "type": "string" } }, { "label": "Approved At", "path": [".KYCAMLAttestation.approvalDate"], "schema": { "type": "string", "format": "date-time" } }] }, "styles": { "thumbnail": { "uri": "http://192.168.2.3:3000/img/kyc-aml-thumbnail.png", "alt": "Verite Logo" }, "hero": { "uri": "http://192.168.2.3:3000/img/kyc-aml-hero.png", "alt": "KYC+AML Visual" }, "background": { "color": "#EC4899" }, "text": { "color": "#FFFFFF" } } }], "presentation_definition": { "id": "ProofOfControlPresentationDefinition", "format": { "jwt_vp": { "alg": ["EdDSA"] } }, "input_descriptors": [{ "id": "proofOfIdentifierControlVP", "name": "Proof of Control Verifiable Presentation", "purpose": "A VP establishing proof of identifier control over the DID.", "constraints": { "fields": [{ "id": "holder", "path": [".holder"], "purpose": "The VP should contain a DID in the holder, which is the same DID that signs the VP. This DID will be used as the subject of the issued VC" }] } }] } }

Credential Application

What follows is a JSON object containing the same contents as a Verifiable Presentation in JWT form; there is no proof object, because it would be signed and transmitted as a JWT.

JSON { "@context": ["https://www.w3.org/2018/credentials/v1"], "credential_application": { "id": "2ce196be-fcda-4054-9eeb-8e4c5ef771e5", "manifest_id": "KYCAMLManifest", "format": { "jwt_vp": { "alg": ["EdDSA"] } } }, "presentation_submission": { "id": "b4f43310-1d6b-425d-84c6-f8afac3fe244", "definition_id": "ProofOfControlPresentationDefinition", "descriptor_map": [{ "id": "proofOfIdentifierControlVP", "format": "jwt_vp", "path": ".holder" }] }, "verifiableCredential": [], // Credential would be found here, as a JWT, i.e. ["eyJhbG..."] "holder": "did:key:z6MkjFFeDnzyKL7Q39aNs1piGo27b12upMf1MmSDQcABJmmn", "type": ["VerifiablePresentation", "CredentialApplication"] }

Credential Fulfillment

What follows is a JSON object containing the same contents as a Verifiable Presentation in JWT form; there is no proof object, because it would be signed and transmitted as a JWT.

JSON { "@context": ["https://www.w3.org/2018/credentials/v1"], "type": ["VerifiablePresentation", "CredentialResponse"], "holder": "did:key:z6Mkgw8mPijYRa3TkHSYtQ4P7S2HGrcJBwzdgjeurqr9Luqb", "credential_fulfillment": { "id": "5f22f1ea-0441-4041-916b-2504a2a4075c", "manifest_id": "KYCAMLManifest", "descriptor_map": [{ "id": "KYCAMLCredential", "format": "jwt_vc", "path": ".verifiableCredential[0]" }] }, "verifiableCredential": [] // Credential would be found here, as a JWT, i.e. ["eyJhbG..."] }

Presentation Exchange

Presentation Request

JSON { "id": "1308e77f-9ab0-4de7-97a8-ad2111b585bf", "type": "VerificationRequest", "from": "did:key:z6MkizuwMHiYpZrBAn64ZnbS2cz5og7iGqAa3nV3EuTj4aaZ", "created_time": "2021-09-14T20:19:32.655Z", "expires_time": "2021-10-14T20:19:32.655Z", "reply_url": "http://example.com/api/verification/1308e77f-9ab0-4de7-97a8-ad2111b585bf/submission", "body": { "status_url": "http://example.com/api/verification/1308e77f-9ab0-4de7-97a8-ad2111b585bf/callback", "challenge": "e0e52794-7889-451c-bb05-28d8cff9ed13", "presentation_definition": { "id": "KYCAMLPresentationDefinition", ... } } } Details:

- from
- : who the message is from; in this case, the issuer
- reply_url
- : the URL the wallet should send the credential submission to

- body.challenge
- : a challenge the wallet should sign when proving control, to prevent replays
- body.presentation_definition
- : this follows the DIF Presentation Definition spec
- body.status_url
- : url returning verification results when complete

Presentation Definition

JSON { "id": "KYCAMLPresentationDefinition", "input_descriptors": [{ "id": "KYCAMLCredential", "name": "Proof of KYC", "purpose": "Please provide a valid credential from a KYC/AML issuer", "constraints": { "statuses": { "active": { "directive": "required" } }, "is_holder": [{ "field_id": ["subjectId"], "directive": "required" }], "fields": [{ "path": [".credentialSubject.KYCAMLAttestation.process", ".vc.credentialSubject.KYCAMLAttestation.process", ".KYCAMLAttestation.process"], "purpose": "The KYC/AML Attestation requires the field: 'process'.", "predicate": "required", "filter": { "type": "string" } }, { "path": [".credentialSubject.KYCAMLAttestation.approvalDate", ".vc.credentialSubject.KYCAMLAttestation.approvalDate", ".KYCAMLAttestation.approvalDate"], "purpose": "The KYC/AML Attestation requires the field: 'approvalDate'.", "predicate": "required", "filter": { "type": "string" } }, { "id": "subjectId", "path": [".credentialSubject.id", ".vc.credentialSubject.id", ".id"], "purpose": "We need to ensure the holder and the subject have the same identifier" }, { "id": "credentialSchema", "path": [".credentialSchema.id", ".vc.credentialSchema.id"], "filter": { "type": "string", "pattern": "https://verite.id/definitions/schemas/0.0.1/KYCAMLAttestation" }, "purpose": "We need to ensure the credential conforms to the expected schema" }, { "path": [".issuer.id", ".issuer", ".vc.issuer", ".iss"], "purpose": "We can only verify credentials attested by a trusted authority.", "filter": { "type": "string", "pattern": "^did:key:z6MkwMmraBRtV4ZyJsTQY7NW52YACpHm6ErKAaicZFuTxcHN" } }] }, "format": { "jwt_vp": { "alg": ["EdDSA"] }, "jwt_vc": { "alg": ["EdDSA"] } } }] }

Presentation Submission

JSON { "@context": ["https://www.w3.org/2018/credentials/v1"], "presentation_submission": { "id": "d885c76f-a908-401a-9e41-abbbeddfe886", "definition_id": "KYCAMLPresentationDefinition", "descriptor_map": [{ "id": "KYCAMLCredential", "format": "jwt_vc", "path": ".verifiableCredential[0]" }] }, "verifiableCredential": [{ "type": ["VerifiableCredential", "KYCAMLCredential"], "credentialSubject": { "id": "did:key:z6Mkjo9pGYpv88SCYZW3ZT1dxrKYJrPf6u6hBeGexChJF4EN", "KYCAMLAttestation": { "type": "KYCAMLAttestation", "process": "https://verite.id/definitions/processes/kycaml/0.0.1/usa", "approvalDate": "2021-09-14T02:00:07.540Z" } }, "issuer": { "id": "did:web:verite.id" } }] } Response

JSON { "status": "approved" } Updated5 months ago * Table of Contents * * Credentials * * * Verifiable Credential * * * Verifiable Credential with status * * * Encoded JWT * * Issuance * * * Credential Offer * * * Credential Manifest * * * Credential Application * * * Credential Fulfillment * * Presentation Exchange * * * Presentation Request * * * Presentation Definition * * * Presentation Submission