Lightweight Verifiable Credential Schema Version 1.0

Committee Specification 01

23 May 2025

This stage:
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/cs01/lvcs-v1.0-cs01.docx (Authoritative)
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/cs01/lvcs-v1.0-cs01.html
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/cs01/lvcs-v1.0-cs01.pdf

Previous stage:

https://docs.oasis-open.org/lvcsp/lvcs/v1.0/csd02/lvcs-v1.0-csd02.docx (Authoritative)
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/csd02/lvcs-v1.0-csd02.html
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/csd02/lvcs-v1.0-csd02.pdf

Latest stage:
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/lvcs-v1.0.docx (Authoritative)
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/lvcs-v1.0.html
https://docs.oasis-open.org/lvcsp/lvcs/v1.0/lvcs-v1.0.pdf

Technical Committee:
OASIS Lightweight Verifiable Credential Schema and Process (LVCSP) TC

Chairs:
Alan Bachmann (AABachmann@cvshealth.com), Aetna

Editors:
Don Sheppard (donshep333@gmail.com), Individual Member
Stefan Hagen (stefan@hagen.link), Individual Member

Additional artifacts:
None

Abstract:
This document defines lightweight schemas for Verifiable Credentials to support digital (also known as electronic) “Know Your Customer” (eKYC) processes, based on the W3C and related Verifiable Credential (VC) standards. Through adoption of this standard, individuals are able to share verified identity claims across different digital platforms and services. This standard is referred to as a "Lightweight Verifiable Credential Schema," abbreviated as LVCS, because it provides basic schemas and formats, without significant options or conditions.

Status:
This document was last revised or approved by the OASIS Lightweight Verifiable Credential Schema and Process (LVCSP) TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=lvcsp#technical.

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/lvcsp/.

This document is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this document, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/lvcsp/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Key words:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

Citation format:

When referencing this document, the following citation format should be used:

[LVCS-v1.0]

Lightweight Verifiable Credential Schema Version 1.0. Edited by Don Sheppard and Stefan Hagen, 23 May 2025. OASIS Committee Specification 01. https://docs.oasis-open.org/lvcsp/lvcs/v1.0/cs01/lvcs-v1.0-cs01.html. Latest stage: https://docs.oasis-open.org/lvcsp/lvcs/v1.0/lvcs-v1.0.html.

Notices:

Table of Contents

1 Introduction

This section is informative.

This document defines a series of schemas that enable individuals to share Verifiable Credentials and Claims for “electronic Know Your Customer” (eKYC) processes.

The goal of this document is to facilitate verifiability, extensibility and semantic interoperability for user-controlled eKYC credentials.

This document defines schemas that are based on the W3C Verifiable Credential Data Model 2.0 [W3C DM2] and the W3C Verifiable Credentials JSON Schema Specification [W3C VCJS]. The schemas defined herein are also aligned with related OpenID Foundation standards [OIDC] and recommendations of the ITU-T [ITUT1252, ITUT1254].

1.1 Changes from earlier versions

This is the first version of the document.

1.2 Glossary, Acronyms and Conventions

This section is not normative.

1.2.1 Definition of Terms

attribute

information bound to an entity that specifies a characteristic of the entity

Note: An attribute is a synonym for a claim.

Biometrics Credential Issuer

entity that verifies, maintains, manages and can create and assign the biometrics information of other entities

Note: Biometrics-based claims or credentials can include templated information for fingerprints, retina scans, facial recognition and other characteristics of a person.

claim

assertion made about a Subject

credential

set of one or more claims made by an Issuer

Note: The claims in a credential can be about different subjects.

Credential Issuer / Issuer

entity that asserts claims about Subjects and issues Verifiable Credentials

Note 1: Issuer functions include claim proofing, VC storage, and VC life cycle management (updates, revocations)

Note 2: Issuers deliver VCs to Holders or to a Holder-controlled credential repository.

Credential Schema

data model used to verify the structure and semantics of the set of claims specified in a credential

Decentralized Identifier (DID)

portable URL-based identifier associated with an entity

Note 1: An example of a DID is “did:example:123456abcdef”.

Note 2: DIDs are most often associated with a Subject in a Verifiable Credential.

Decentralized Identifier document (DIDdoc)

file containing information related to a DID

Note: DIDdocs are accessible from a verifiable data registry.

electronic Know Your Customer (eKYC)

digital process for remotely verifying the identity of individuals or businesses

Note 1: eKYC processes may have varying levels of validity assurance.

Note 2: Remote validation can include in-person evidence collection.

Note 3: Customer knowledge can vary from a simple self-asserted name to in-depth investigations for regulatory purposes.

entity

thing that can be referenced in statements as an abstract or concrete noun

Note 1: Entities include but are not limited to people, organizations, physical things, documents, abstract concepts, numbers, and strings.

Note 2: An entity can perform a role in an ecosystem if it is capable of doing so – some entities fundamentally cannot take actions, for example, the string "abc" cannot issue credentials.

Holder

entity that processes and consents to the presentation of Verifiable Credentials

Note 1: The Holder is often, but not always, the Subject of the VC being processed.

Note 2: Holders store their credentials in credential repositories.

identity

representation of an entity as one or more attributes that allow the entity or entities to be sufficiently distinguished within a context

Identity Credential Issuer

entity that verifies, maintains, manages and can create and assign identity information of other entities

Note 1: An Identity Credential Issuer is also known as an identity provider (IdP) or identity service provider (IdSP).

presentation

claim data derived from one or more credentials

Note 1: Credentials are issued by one or more Credential Issuers.

Note 2: A presentation is delivered to a Verifier.

Service Provider (SP)

entity that offers products or services to qualified users

Note 1: A Service Provider is often referred to as a “relying party”.

Note 2: A Verifier is a role of the Service Provider. Other business roles could include a shopping cart, payment processor, service delivery, etc.

Subject

thing about which claims are made

User / End User

entity that requests a product or service from a Service Provider

Note 1: A User is often referred to as a “customer”, “client”, or “buyer”.

Note 2: A User can perform the role of Holder or Subject.

verifiable credential (VC)

tamper-evident credential that has authorship that can be cryptographically verified

verifiable data registry

role for mediating the creation and verification of identifiers, keys and other data relevant to the use of VCs

Note 1: Relevant data can include but is not limited to VC schemas, revocation registries, and issuer public keys.

Verifiable Presentation (VP)

tamper-evident presentation whose authorship can be trusted after completing a process of cryptographic verification

Note 1: Certain types of VPs include data that is synthesized from, but does not contain, the original VCs (for example, zero-knowledge proofs).

verification

process for determining whether a verifiable credential or verifiable presentation is an authentic and timely statement from an Issuer or User

Note 1: The verification process checks the VC or VP for compliance to an associated schema, that the proof method is satisfied and, if present, that the status check succeeds.

Note 2: Verification of a credential does not imply a successful evaluation of the truth of the claims encoded in the credential.

Verifier

entity that receives Verifiable Credentials and Verifiable Presentations for verification

1.2.2 Acronyms and Abbreviations

CI	Credential Issuer
DID	Decentralized Identifier
DIDdoc	Decentralized Identifier document
DIE	Digital Identity Ecosystem
eKYC	electronic Know Your Customer
IdP	Identity Provider
IdSP	Identity Service Provider
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union – Telecommunications Standardization Sector
JSON	JavaScript Object Notation
JWT	JSON Web Token
SD-JWT	Selective Disclosure JWT
NIST	National Institute of Standards and Technology
SP	Service Provider
URL	Uniform Resource Locator
VC	Verifiable Credential
VP	Verifiable Presentation
W3C	World Wide Web Consortium

1.2.3 Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

2 Verifiable Credentials Overview

This section is informative.

2.1 Introduction

Modern information systems depend on rapid and continuous access to authentic, accurate digital identity information regardless of location, technology, or type. Users, in contrast, want to control access to and use of their identity and personal data. User control is deemed to be a fundamental requirement for most digital transformation initiatives. This is the impetus for decentralizing the management of identities and for creating a “zero trust” environment for system access control.

Verifiable Credentials (VCs), as defined by the W3C [W3C DM2], support digital identity ecosystems that are standards-based, interoperable, privacy-preserving, de-centralized and trustworthy. Interoperability is critical since digital identity ecosystems are typically multi-vendor, multi-user and multi-purpose. Trust and data protection are also essential characteristics, especially for critical infrastructures and social networks.

This document specifies JSON schema templates for Verifiable Credentials that can help to accelerate the transition to electronic Know Your Customer (eKYC) services, processes and practices. The eKYC concept is broadly applicable to assurance levels ranging from self-attested statements to fully-vetted, legally-accepted credentials.

This document describes VC schemas covering eKYC for persons (i.e., individuals); it does not include non-human entities such as abstract objects, animals, organizations, or sensors.

2.2 Claims and Credentials

A claim is a statement of fact about a human Subject. Other Subject types – application agents, chatbots, IoT devices, and OT endpoints, for example – are for future consideration.

Claims include but are not limited to:

- *attributes*: features or characteristics of the Subject, especially permanent or long-lasting characteristics such as a name, date of birth or eye color;
- *contextual*: information that describes or frames a Subject including family relationships, employers, current residence, education, physical limitations, unique features, experiences, etc.;
- *eligibilities*: permissions or rights assigned to a Subject for a period of time (e.g., permission to drive a car or to practice medicine).

Credentials are sets of claims. Credentials are data objects that form the payloads for transactions in the Digital Identity Ecosystem. To ensure scalability, interoperability and efficiency, credentials must be verifiable, trustworthy, meaningful, accepted by, and useful to the Digital Identity Ecosystem participants.

The goal for Credential Issuers is to generate and issue credentials that meet (or exceed) the functional and quality requirements of Service Providers with little or no variation and processing. This can be facilitated by adopting the common credential schemas that are defined in this document.

Credentials include but are not limited to:

- a reference to the Subject (for example, a photo or name);
- the type of credential (for example, a Dutch passport, an US driving license, or a Canadian health card);
- a reference to the credential schema (the structure and contents of the credential);
- a unique Subject identifier (such as a social security number, a DID, or an arbitrary serial number);
- one or more claims being asserted by recognized authorities (for example, the nationality of the Subject at birth, vehicle types the Subject is allowed to drive, the date of birth);
- the name of the accredited issuer (e.g., a city government, a national agency, or a certified issuer); and
- constraints on the credential (for example, its validity period or terms of use).

For example, Figure 1 illustrates the user data of an unsecured payload for an identity credential that includes the Subject's name and age.

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema#",
  “title”: “exampleSchema”,
  “description”: “Example of a Minimal Schema”,
  "type": "object",
  "properties": {
    "name": {
      "type": "string"
    },
    "age": {
     "type": "integer"
    }
  },
  "required": ["name", "age"]
}
```

In this example:

- $schema - specifies the JSON Schema version.
- title - an optional title property.
- description - an optional description property.
- type - indicates that the data structure is an object.
- properties - defines the properties (i.e., claims) “name” and “age” and their data types.
- required - lists the properties that must be present in the object.

Figure 1: Example of an Identity Credential Schema

Claims about a Subject can be divided into:

– *Subject identifier information* – information that can be used to distinguish one person from another with a specified assurance of uniqueness within a specified domain (e.g., a country). In general, an individual's common name is not sufficient to be a unique identifier.
– *Subject-related information* – additional facts about the Subject that are context- or application-dependent. Restrictions on a driver's license (e.g. must wear glasses) is an example.

Identity claims include the person's age, birth city, birth date, eye color, hair color, name, parent's names, etc. One objective is to use just enough claims to ensure uniqueness without unnecessarily disclosing personal information. Identity claims that are stable, help to minimize re-issuance requirements (e.g., a birth date rarely changes).

Related data includes any information that is needed by a requester (usually a Service Provider). For example, claims could refer to different, unrelated Subjects such as claims about a parent and their children. A credential need not include any claims about the Subject's identity. For example, a parent may be the Subject of a credential in which all the claims are about the children.

An organization that supplies credentials is serving in the Credential Issuer role. This role is responsible for signing and issuing a credential to its approved Holder. The same organization may also perform other roles including acquiring and validating the claims and packaging the claims into verifiable credentials. Organizations must be authorized to issue the credential type; for example, a driver's license is normally only issued by a specific government department.

Example

A physical driver's license (see Figure 2) is an example of a credential that includes multiple claims. The main purpose of the driver's license is to state that the named individual (the Subject) is legally allowed to operate a motor vehicle, possibly with restrictions such as "must wear glasses" or "applies only for passenger vehicles." Many driver's licenses also include a date of birth, an address that was valid at the time of issuance, a picture and a signature, all of which have been validated by a government office through physical presence and examination of evidence.

Figure 2: Example of a Driver's License Credential

2.3 Digital Identity Ecosystem

People can be uniquely identified and differentiated by collecting and validating ("proofing") claims about them, including but not limited to their address, age, eye color, gender, height, name, and nationality. Although the assurance of uniqueness increases with the number of claims and the robustness of the validation process, a relatively small set is usually sufficient for identification within a context, geographic region, or specific scope. For example, in a city there would typically be only one person with a given first name, last name, phone number, and possibly age (four claims). Addition of a verified address and driver's license would increase the assurance of the person's uniqueness to a national or global level.

A Digital Identity "ecosystem" is a set of actors and technology platforms used for digital identification processes including ingesting and validating identity claims, packaging validated claims into VCs, and presenting the VCs to organizations that have a "need to know." Figure 3 illustrates the parties in a Digital Identity Ecosystem – in practice, there will be many Subjects/Holders and many Service Providers with a smaller number of Credential Issuers, Verifiers and Platforms.

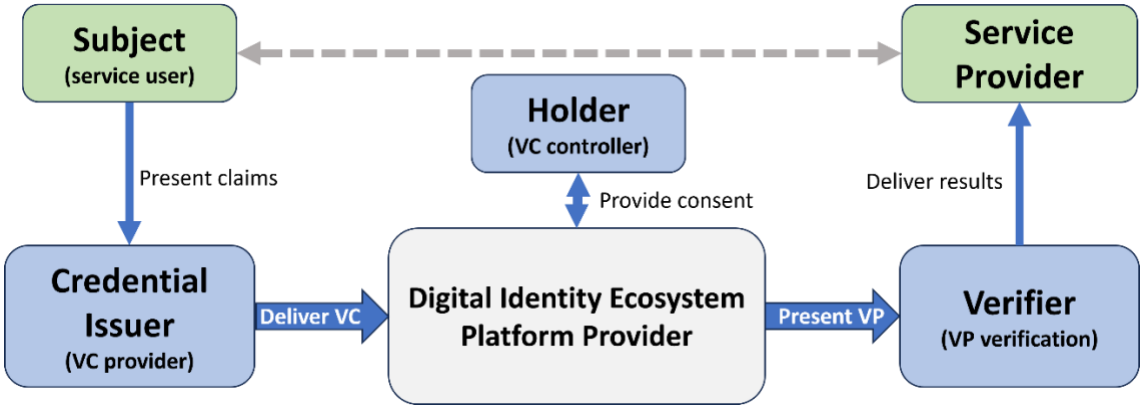

Figure 3: Parties in a Digital Identity Ecosystem

2.3.1 Subject

A Subject can be an individual, organization, device or any other object that has independent existence and is separately identifiable. The User of the products and services offered by the Service Provider is usually the Subject that is to be identified.

Note: This standard currently applies only to human Subjects.

A Digital Identify Ecosystem enables Subjects to digitally identify themselves in a robust, reliable and re-usable manner. It also allows for secure delivery of related digital information that complements the identity.

2.3.2 Holder

A Holder is an individual or their proxy that is responsible for handling credentials on behalf of an associated Subject. A Holder can also be the Subject, but this is not mandatory.

The Holder interacts with the Credential Issuer to acquire VCs and with the Service Provider to agree on which credentials are required for a specific business transaction. The Holder consents to the presentation of credentials when available.

2.3.2.1 Holder Wallet

A Holder's device or system includes a role to securely and privately store VCs and other information of concern to the Digital Identity Ecosystem. This role is typically referred to as a "wallet."

A Wallet can be a role of a Holder's device or be provided by a third party (such as the platform provider).

2.3.3 Credential Issuer / Issuer

A Credential Issuer (CI) is an accredited organization that generates, certifies and issues validated credentials.

A CI is responsible for acquiring claims from a Subject, assessing evidence of claim validity, assigning validation assurance levels, packaging claims into Verifiable Credentials in accordance with governance policies, and issuing the Verifiable Credentials to authorized Holders.

A CI can be an independent organization or a role within an organization (for example, a Service Provider that performs CI functions for its customers).

2.3.3.1 Identity Credential Issuer

An Identity Credential Issuer is a specialized Issuer that only issues core identity-related credentials. Identity Credential Issuers are also known as Identity Providers (IdP) or Identity Service Providers (IdSP) [ITUT1252]

An Identity Credential Issuer can be a role of a Credential Issuer or be a separate third-party organization.

2.3.3.2 Biometric Credential Issuer

A Biometric Credential Issuer is a specialized Issuer that generates biometric information, creates biometric templates and issues biometric claims or credentials.

Government agencies that issue biometric passports, private companies that offer facial recognition-based services, and similar service providers are examples of Biometric Credential Issuers.

A Biometric Credential Issuer can be a role of a Credential Issuer or can be a separate third-party organization. Biometric Credential Issuers can specialize in different forms of biometrics (e.g., fingerprints or facial recognition).

2.3.4 Service Provider

A Service Provider (SP) is an organization that supplies products or services to a Subject.

An SP is responsible for defining which credentials are required, verifying presented credentials, meeting regulatory and legal requirements (such as age restrictions) and then delivering the requested products or services. To meet its obligations, the Service Provider needs specific context-dependent information from the Holder.

The choice of products or services offered by the Service Provider and the information required is outside the scope of the Digital Identity Ecosystem.

2.3.4.1 Verifier

A Verifier provides VC/VP verification functions. An alternate name for a Verifier is a Relying Party.

A Verifier can be a Service Provider role or be a service offered by a separate third-party organization.

2.3.5 Platform Provider

A platform provider in a Digital Identity Ecosystem provides services such as the verifiable data registry [W3C DM2].

The W3C defines a Verifiable Data Registry as:

> "A role a system might perform by mediating the creation and verification of identifiers, verification material, and other relevant data, such as verifiable credential schemas, revocation registries, and so on, which might require using verifiable credentials. Some configurations might require correlatable identifiers for subjects. Some registries, such as ones for UUIDs and verification material, might act as namespaces for identifiers."

Platform Providers also provide services for entity enrollment, safe storage and transfer of VCs, and enforcement of governance policies.

2.3.5.1 Platform-based Wallet

A platform provider can optionally offer wallet-like functions as an alternative to or in cooperation with the Holder's device.

Platform-based wallets can facilitate the acquisition, storage, and management of Verifiable Credentials and, if used, play a critical role in securing these credentials. These wallets incorporate robust authentication mechanisms, such as password/PIN and biometric unlock, to ensure that verifiable presentations are generated only by the rightful owner. Secure wallet implementations are foundational to building trust in digital identity ecosystems.

Platform-based wallets include functions for acquiring VCs, selecting claims for disclosure to SPs, and brokering consent to disclose the various claims in VPs.

2.4 Verifiable Credentials and Presentations

A credential is said to be verifiable (VC) when a trusted Credential Issuer has cryptographically signed it.

A VC consists of metadata, one or more validated claims, and the Credential Issuer's digital signature (see Figure 4). The digital signature makes the VC tamper-evident and trustworthy but does not support confidentiality.

Although the authorship of a VC can be cryptographically verified, there is no built-in guarantee that the claims contained within the VC are valid or accurate. The Verifier trusts the Credential Issuer to perform sufficient due diligence to make the claims "fit for purpose" as represented by a VC Assurance Level (see Section 2.6).

Similarly, a Verifiable Presentation (VP) consists of metadata, one or more VCs, and the Holder's digital signature (see Figure 4). The signatures in the VP certify that both the Credential Issuer and the Credential Holder are vouching for the claims.

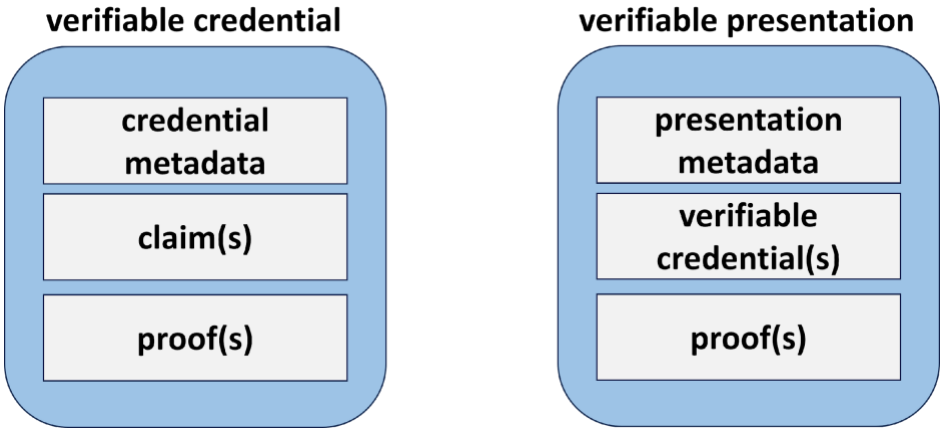

Figure 4: Structure of a VC and a VP

The Holder consents to the inclusion in the VP of one or more VCs that they possess or can acquire. The Verifier receives the VP and performs verification functions that are based on rules defined by the Service Provider. A VP is verifiable when it:

- is signed and presented by the expected Holder;
- conforms to a specific VC schema or a presentation definition;
- includes the required cryptographic signatures; and
- meets the Service Provider's criteria for business acceptability and risk.

The JSON metadata contains general characteristics of the information included in the VCs and VPs, including but not limited to:

- assurance level
- credential identifier
- Credential Issuer
- credential schema
- revocation mechanism
- time period
- validity date
- verification material

2.4.1 Biometric Verifiable Credentials

Biometrics refers to the identification and verification of individuals based on unique physical or behavioral traits. Biometrics can include but is not limited to:

- behavioral (gait analysis, keystrokes)
- facial recognition
- fingerprints
- iris patterns
- liveness test
- palm scan
- picture (basic or templated)

- voice recognition

Biometric systems employ the concept of “biometric templates” to generate a digital representation of the individual's biometric data. The basic steps in the process are:

a) **Data Capture**: The raw biometric data is captured by a sensor (e.g., fingerprint scanner, camera).

b) **Preprocessing**: The raw biometric data is processed to enhance quality and remove noise.

c) **Feature Extraction**: Key features are extracted from the preprocessed data. For example, this might include points such as ridge endings and bifurcations in a fingerprint.

d) **Template Creation**: The extracted features are converted into a digital representation, thereby creating the biometric template.

e) **Storage**: The template can be securely stored in a user-controlled database, in a Holder’s wallet or in a device such as a smart card.

Biometric templates can be incorporated into a VC as specialized claims and be linked to the individual's digital identity to provide a strong form of authentication. Biometric-specific metadata provides additional information such as the time and location of capture, the quality of the biometric sample, and the device used for capture. This metadata ensures the integrity and authenticity of the biometric data and results in a higher level of security, as it is challenging to forge both the biometric data and the associated metadata.

Fingerprints and facial recognition are widely used for accessing smartphones and laptops. Multiple biometric attributes can be used for increased confidence in the identification process.

A photograph (e.g., a JPEG or GIF) can be treated as a form of biometric, although picture files are more often used for in-person visual verification than for automated biometric matching.

The Common Biometric Exchange Formats Framework **[**CBEFF**]** provides a comprehensive set of data elements (i.e., VC claims) that can be used for biometric interoperability. Key VC claims include:

- **Biometric Identifier**: Numeric data elements used to identify biometric objects within biometric data records;
- **Biometric Feature**: Defines the type of biometric data (e.g., fingerprint, face, voice);
- **Challenge-Response Field**: Used for security purposes to verify the authenticity of the biometric data;
- **Creator Field**: Identifies the product or entity that created the biometric data;
- **Index Field**: Associates a specific instance of biometric reference data**;**
- **Validity Period**: Specifies the time period during which the biometric data is valid; and
- **Payload Field**: Contains the actual biometric data.

Interoperability data standards are essential for ensuring that different biometrics systems and devices can work together seamlessly. Standards that help to achieve this goal include:

- ISO/IEC 19794 outlines the formats for the interchange of biometric data including fingerprints, facial images, iris images, and voice data.
- ISO/IEC 30107 focuses on presentation attack detection (PAD), ensuring that biometric systems can distinguish between genuine biometric traits and artificial representations used to spoof the system.
- ANSI/NIST-ITL 1-2011 provides guidelines for the exchange of biometric data and is commonly used by law enforcement agencies.
- ICAO Doc 9303, developed by the International Civil Aviation Organization, specifies the use of biometrics in travel documents, such as e-passports, to facilitate international travel.

When required, a Holder can present their biometric VC to a Verifier. The Verifier cryptographically verifies the VC's authenticity and integrity to ensure the biometric data matches the Subject’s real identity.

Appendix F.5 illustrates how CBEFF fields can be represented as VC claims.

2.5 Verifiable Credential Schemas

A Verifiable Credential (VC) Schema is a JSON-based format for describing the structure of JSON data. The JSON Schema asserts what a JSON document must look like, ways to extract information from it, and how to interact with it.

VCs are written as JSON objects, with their contents described by a JSON Schema (see Figure 1). Although the claim content is dictated by the Service Provider, some claims will be common to many credential types (e.g., the name of the Subject) and are widely used.

Schemas facilitate interoperability by defining the structure of the VC. The W3C Verifiable Credentials JSON Schema Specification [W3C JS] is a standard for VC schemas that can be used to ensure maximum compatibility.

Two types of schema are of particular interest: (a) data verification schemas for verifying that the structure and contents of a credential or verifiable credential conform to a published schema, and (b) data encoding schemas that map the contents of a VC to alternative representation formats, such as a format used in a zero-knowledge proof.

Standardized VC/VP schemas can benefit participants in the Decentralized Identity Ecosystem by providing:

- well-known and well-accepted specifications for the VCs that the Credential Issuer generates, thereby enhancing consistency and completeness.
- a means to pre-define information that the Verifier needs, thereby increasing efficiency for high-volume SP transactions.
- a simplification in how VCs can be transformed into VPs, thereby reducing reliance on the Holder application.
- a reduction in “friction” associated with collecting, proofing, notarizing, consenting and presenting information to the Service Provider.

For some use cases, a simplified “lightweight” VC is sufficient. A VC can be considered lightweight if it:

- is formatted as a JSON Web Token (JWT), optionally with selective disclosure;
- adopts IANA reserved names to the maximum extent possible;
- excludes arrays and optional claims;
- accepts VC Assurance Levels as stated by the Credential Issuer: and
- does not require trusted processing in the Holder’s wallet.

The functions and processes associated with VC schemas continue to evolve as the standards and technologies for Decentralized Identity Ecosystems mature.

2.6 Assurance Levels

An assurance level is a “level of confidence in the binding between an entity and the presented identity information” [ITUT1252].

Three types of assurance level have been defined by the NIST [NIST SP800-63]:

- Identity Assurance Level (IAL) – degree of confidence in the processes put in place to verify a Subject’s association with their real-world identity (i.e., the identity proofing process),
- Authentication Assurance Level (AAL) – degree of confidence in the authentication process, i.e., the processes put in place to verify that a claimed identity is the same as the one that participated in the registration process and has previously been authenticated by the system.
- Federation Assurance Level (FAL) refers to the federation process when the Service Provider is connected to a Credential Issuer through a federated protocol.

An IAL rating is statement of the robustness of the Credential Issuer’s claim validation processes. It includes the level of confidence in the User making the VC claims, the Credential Issuer processes for examining the evidence concerning the VC claims, and the credibility of the resulting VC itself.

Identity assurance is described using one of three IALs:

- IAL1: Linking the Subject to a specific real-life identity is not required. Any claims provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted (including attributes a CI asserts to an SP). Self-asserted claims are neither validated nor verified.
- IAL2: Evidence supports the claimed identity and that the VC Subject is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.
- IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

The VC metadata includes a claim whose value is aligned with NIST SP 800-63-A.

Assurance Levels are intended to provide minimum guidance only. Credential Issuers are not restricted as to how, when or where to prove the claims presented by a User.

3 Know Your Customer Credentials

This section is informative.

3.1 Introduction

Note: In KYC systems a “customer” is equivalent to a “Subject” in a Digital Identity Ecosystem.

The phrase “Know Your Customer” (KYC) typically refers to vetting a person to whom products or services may be offered in order to:

- confirm their identity to a desired level of certainty; and
- evaluate the legal, regulatory and financial risks associated with the transaction.

For example, KYC, when used by financial services organizations, helps to verify who the customer is and verify that they intend to use their account only for legal purposes (i.e., not for money laundering).

In today’s world of deep fakes, phishing and identity theft, KYC can support a wide range of customer-supplier interactions including but not limited to:

- setting up an online shopping cart;
- filling a medical prescription at a pharmacy;
- subscribing to an age-restricted social network;
- subscribing to an online newspaper; or
- obtaining a university transcript.

Although collecting and retaining KYC information is not always legally required, it can still be useful for various business purposes including assuring safety, promoting efficiency and improving the customer experience. For example, customer preferences, purchase history and current context all provide valuable insights for marketing and product management.

KYC aims to increase accountability at all stages of the identification process:

- The Credential Issuer generates a valid VC with an acceptable level of assurance in both the evidence and the validation process.
- The KYC VC schema includes the structure, contents and metadata needed to facilitate verifiability and to increase trust in the Credential Issuer.
- The customer (Subject/Holder) has control over the VCs for which they are the subject and can determine who is allowed to have access to the claims.
- The supplier is able to dictate what it needs to know about the prospective customer.

One general caveat related to both physical and digital KYC is that “knowing too much” about a customer often leads to security and privacy issues including inappropriate use and retention of personal data.

3.2 eKYC Processes

Traditionally, KYC was based on physical, in-person inspection of trustworthy documents (e.g., a driver’s license or a birth certificate). Opening a bank account, for example, would involve a meeting with a bank manager to take a copy of reference documents for use as evidence. Paper documents and “signature cards” were held by the bank branch for cheque verification.

Online eKYC represents the digital transformation of KYC processes to allow online presentation of identity credentials. eKYC requirements can vary widely depending on the needs of the Service Provider. Credential sources range from online inspection of remote evidence to full in-person data capture.

Justification for claim requirements includes business policies, operational constraints, jurisdictional considerations, and potential legal or regulatory restrictions. The spectrum of claim requirements ranges from almost nothing (e.g., simply a proof of age) to an extensive investigation into the Subject’s identity and intentions.

eKYC processes and data collection should be tailored to fit the particular use case, with the goal being to collect just enough information to allow the supplier to meet their legal requirements and to make a risk-based decision on accepting a customer request.

3.3 Steps in a Basic VC-based eKYC Process

Within the Decentralized Identity Ecosystem, eKYC is an interaction between the Service Provider and the Subject – the Service Provider defines a Verifiable Presentation that encompasses what they need in order to provide goods or services. The eKYC requirement can vary widely but will likely be well-defined and consistent within a sector.

For example, an alcohol retailer KYC might only require age verification while a bank would need full legal name, address, proof of residency, and a credit rating. In some cases, knowing your customer could involve explicit investigation of evidence to detect forgeries, etc.

Figure 5 illustrates the stages in a basic eKYC process that incorporates Verifiable Credentials:

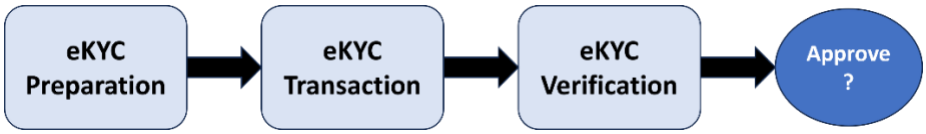

Figure 5: Stages in an eKYC Process

3.3.1 Preparation

The Service Provider determines the information needed for the transaction and the acceptable assurance levels for the credential and the issuer. eKYC information varies widely – from the most basic Zero Knowledge Proof of age to much more complex biometrics processing and evidence capture. For example, facial recognition systems can compare a face to a basic photograph or to a real-time image with liveness detection.

The Service Provider selects a standard eKYC VC schema (such as one of the Templates defined in Section 5). If necessary, the Service Provider can define and publish a custom eKYC schema. The Service Provider can also request additional information that goes beyond the scope of eKYC.

The VC schema is also used to establish policies and decision criteria for the Verifier, which could include data retention and legal reporting rules.

3.3.2 Transaction

The Service Provider requests the prospective customer (the Holder/Subject) to submit an eKYC VC that conforms to the chosen VC schema. A basic identity might include a photo, a scanned evidence document or a zero knowledge proof.

The Holder either has possession of the required claim information or has access to a Credential Issuer who can generate it.

The Holder consents to submit the eKYC VC using data from their wallet or a cloud vault and submits a Verifiable Presentation to the Verifier. The Verifier can be a Service Provider role or a 3rd party acting as a proxy.

Adoption of a standard eKYC VC schema that matches the SP requirements would eliminate unnecessary information, especially personal information, and processing. This minimizes the overhead associated with preparing and delivering a Verifiable Presentation.

3.3.3 Verification

The Verifier service receives and checks the VP against the schema(s). This includes checking the format and cryptographic signatures and also assessing both the VC Assurance Level and the reputation of the Credential Issuer. The Verifier then provides the verification results to the SP for their business decision.

The Service Provider decides whether or not to accept the prospective customer based on the verification results.

The Service Provider can also compare extracted data to other trusted data sources and watchlists to evaluate the risk and check for any red flags.

4 VC Schemas for eKYC

This section is informative.

4.1 Introduction

A JSON Schema is an agreement on the syntax, semantics, context and security of the information that is to be shared digitally between a consumer (requestor) and a supplier (provider).

Service Providers requiring eKYC information for their internal business processes can choose between a standard VC schema as defined in this standard or a custom VC developed by themselves, a Credential Issuer or a third party.

A basic eKYC VC can also be enhanced if the SP requests that other VCs also be supplied. As an example, a standard eKYC VC provided by a Credential Issuer might include a birth date that has not been proven with evidence, and which does not include a list of criminal convictions. To mitigate this deficiency, the SP could request a birth certificate from the Issuer and separately request a police record issued by a highly-trusted government agency.

Credentials for eKYC should include claims that:

- describe the person sufficiently to answer the question – Who is this person?
- provide statements that help to answer the question – Is this person acceptable as a customer?
- provide other predefined information to answer questions such as – What jurisdiction is the customer in?

4.2 Requirements for VC Schemas

There are many reasons why a Service Provider needs to collect information about their customers, but it is not an “all or nothing” choice. Some interactions just need a proof of age (or even just humanity), others need basic contact data, while still others involve extensive descriptions of a person’s skills and experience in addition to personal characteristics (such as a resume).

Some day-to-day interactions (both in person and electronic) can be anonymous with no requirement for a verified name. Examples include:

- attendance at a public event (need only age verification);
- completing polls and surveys (require just a location); and
- reserving a restaurant table (only requires a callback number).

Financial institutions, on the other hand, must use reasonable diligence to identify and retain the true identity of every customer and every person acting on behalf of those customers. Information for enforcing full financial eKYC can include:

1. Customer name, date of birth, address, and a government document number;
2. Customer due diligence, which verifies the identity of customers associated with open accounts. The core requirements are:
   - identify the customer and verify the identity, with ongoing monitoring for suspicious transactions;
   - identify and verify the identity of beneficial owners of companies opening accounts;
   - understand the nature and purpose of customer relationships to develop customer risk profiles.
3. Enhanced due diligence is required when high-risk factors have been identified. The information collected includes a source of wealth and funds check; additional identity research; and risk identification and assessment.

Multiple use cases have been targeted by the European eIDAS 2.0 and EUDI wallet developers **[**EUDI**]** including but not limited to:

- Access to government services;

- Digital education and social security credentials.
- ePrescriptions;
- eSignatures;
- Mobile driving licenses;
- Opening a bank account;
- Payment authorization by the wallet user;
- Registering for a SIM card; and
- Storage and display of digital travel credentials.

In all of these use cases, basic information about the requestor (i.e., the customer) is necessary before a transaction can be completed. The wallet lets people digitally identify themselves simply by using their smartphones. People control their own wallets and personal data and only share what they want with whom they want.

eKYC decisions are not a simple yes/no based on whatever information happens to be presented. One or more sources may be required to deliver the information needed by the Service Provider. Examples of information that may be needed includes (in order of relevance):

- Basic identification – what is my name?
- Personal description – how old am I? What do I look like? What are my distinguishing features (e.g. eye color)?
- Government documents – birth certificate, driver's license, marriage certificate, health card
- Situation – where am I located currently? Where do I live? Where was I born?
- Relationships – family members? associates? marital status?
- Memberships – what groups or societies do I belong to?
- Occupation – where do I work? What job do I have?
- Certificates – what licenses and certifications do I have? What degrees or diplomas do I have?
- Capabilities – what are my skills and training?
- Experiences – what have I done in the past? major accomplishments?
- Publications – books, articles, social posts, etc.
- Awards – prizes, recognitions, winnings
- Reputation – formal and informal rankings

There are three considerations when making eKYC information requests:

a) Claim suitability – These are the "attributes" of the customer that the Service Provider is asking to be provided. The request should be limited to what is really needed for the transaction and not include data that is not relevant. For example, an electronic driver's license would not need to include family members.

b) Assurance levels – Each Claim can be evaluated based on how well it has been tested for validity. At the lowest level, the Subject simply states that the Claim is authentic. eKYC processes aim to ensure that Claims are issued from a trusted source and can be validated.

c) Personal privacy – Service Providers should only request Claims that they need and should minimize the need to store PII. The Customer (i.e., the Holder) should also consent to the disclosure of information that they feel is warranted for the transaction.

4.3 Standards for eKYC VCs

The templates described in this standard are not designed to fully conform to specific industry standards. There are, however, a number of industry standards for KYC that may provide guidance:

- Healthcare: the HL7 FHIR US. IDENTITY-MATCHING integration;
- Financial Services: USA Federal Financial Institutions Examination Council (FFIEC) guidance, FIDO Alliance frameworks, and others; and

- European Union Payment Services Directive 2 for payment services anti-money laundering

There are only a few standardized formats for releasing electronic attestations of claims:

- ISO/IEC 18013-5 defines an attribute schema, data format and proof mechanisms for electronic drivers' licences, mDLs, which can be used also with other attribute schemas, see [ISO/IEC 18013-5].
- Selective Disclosure for JWTs (SD-JWT) defines a proof mechanism similar to [ISO/IEC 18013-5], but for a different data format, see [SD-JWT].
- W3C Verifiable Credentials Data Model – see [W3C VCDM2].

5 Templates for eKYC Schemas

5.1 Introduction

This section is informative.

Figure 6 is a simple example of a JSON-JWT that delivers an email address. Part 1 is the JWT and Part 2 is the corresponding JsonSchema as referenced by Part 1. In this example, the only claim is an email address written in the standard internet format.

Part 1 - Email Credential referencing a JsonSchema

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "https://example.com/credentials/3732",
  "type": ["VerifiableCredential", "EmailCredential"],
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "emailAddress": "subject@example.com"
  },
  "credentialSchema": {
    "id": "https://example.com/schemas/email.json",
    "type": "JsonSchema"
  }
}
```

Part 2 - JSON Schema for the Email Credential

```
{
  "$id": "https://example.com/schemas/email.json",
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "EmailCredential",
  "description": "EmailCredential using JsonSchema",
  "type": "object",
  "properties": {
    "credentialSubject": {
      "type": "object",
      "properties": {
        "emailAddress": {
          "type": "string",
          "format": "email"
        }
      },
      "required": [
        "emailAddress"
      ]
    }
  }
}
```

Source: [W3C VCJS] Section 2.1

Figure 6: Example of a JSON-JWT with a JSON Schema

The templates defined in sections 5.2 to 5.6 are similar to the example, with the number and variety of claims designed to fit the specific use cases. The goal is to have a set of schemas that cover common use cases on which the Credential Issuer, the Service Provider and the Holder can jointly agree.

The templates as defined in this document only include Claims that are required, not all possible claims. It is anticipated that the templates will be extended or modified over time.

The claims and examples provided in this document are based on the JsonSchema type which uses JSON schema documents. Schemas may also be packaged as Verifiable Credentials.

For the templates defined in sections 5.2 to 5.6, see [OIDC} and [IANA] for standard definitions of the claims.

5.2 Template 1 – Basic Personal Identity Schema

There are many situations when very basic customer information needs to be provided to allow a service provider to provide good customer service on an ongoing basis. This can be thought of as the equivalent of a "business card" for an individual. Examples of this scenario would include:

- A person meets a salesperson and wishes to provide just enough information to arrange a future meeting. The salesperson wants basic confirmation that the name and contact are correct;
- A person subscribes to a physical magazine or newsletter - the publisher wants to verify the name and postal address to avoid mis-deliveries.

The goal of Template 1 is to demonstrate that:

- the customer is a human (i.e., proof of personhood);
- the name provided has been verified to be the person;
- the contact information provided is correct and matches the person at a given point in time.

Template 1 Claims are typically public information and would not be subject to privacy restrictions related to storage or use. The Credential Issuer checks that the person is in fact a real human and validates the Claims by inspection of evidence.

Template 1 provides a schema for a simple JWT credential using IANA-registered claims and has no options or selective disclosure capabilities. Table 4 provides the claim details for Template 1 (See Appendix E for the full IANA listing).

Template 1			
Claim/Attribute	**Type**	**Source**	**Brief Description**
given_name	string	IANA	Usual first name of the Subject
family_name	string	IANA	Usual last name of the Subject
phone_number	string	IANA	Preferred telephone number including country codes (E.164 format is recommended)
email	string	IANA	Preferred email address (RFC 5322 address)
address	JSON object	IANA	Preferred postal address (Note 1)
Claims common to all Templates			
sub	string	IANA	Subject – Identifier for the End-User at the Issuer

issuer	string		Party that issued the VC
assurance_type	string		Assurance standard (e.g. NIST SP 800-63.3) (Note 2)
assurance_level	string		VC-AL1, VC-AL2, VC-AL3
assurance_evidence	string		URL for evidence relating to the VC assurance level
updated_at	number	IANA	Time of last update

Table 1: Basic Personal Identity VC Schema

Note 1: The address claim in Table 1 represents a physical mailing address and is a JSON structure containing some or all of the following represented as JSON strings:

- *formatted*: Full mailing address, formatted for display or use on a mailing label. This field MAY contain multiple lines, separated by newlines. Newlines can be represented either as a carriage return/line feed pair ("\r\n") or as a single line feed character ("\n").
- *street_address*: Full street address component, which MAY include house number, street name, Post Office Box, and multi-line extended street address information. This field MAY contain multiple lines, separated by newlines. Newlines can be represented either as a carriage return/line feed pair ("\r\n") or as a single line feed character ("\n").
- *locality*: City or locality component.
- *region*: State, province, prefecture, or region component.
- *postal_code*: Zip code or postal code component.
- *country*: Country name component.

Note 2: The assurance claims in Table 1 is a representation of the strength of identity proofing that was completed by the Credential Issuer in generating the VC. The following assurance levels are based on the IAL definitions contained in [NIST800]:

- VC-AL1: claims, if any, are self-asserted or should be treated as self-asserted.
- VC-AL2: claims, if any, require either remote or in-person identity proofing; verifying procedures are specified in [NIST800]
- VC-AL3: claims, if any, require in-person proofing that is verified by an authorized representative through examination of physical documentation.

5.3 Template 2 – Basic Age Disclosure Schema

In some situations, the primary concern is whether the customer is over a specific age, such as 19 or 21. It is not necessarily important to know the actual date of birth or gender, but these could be options. The service provider may also want to be able to verify that the customer is presenting the correct credentials (by examining a photograph).

Examples of this scenario would include:

- A person attempts to buy restricted items at a retail outlet (e.g., cigarettes or alcohol). The salesperson requires basic confirmation that the customer is of legal age and hasn't "borrowed" another person's wallet.
- A person wants access to a bar or club. The door person needs to validate a photo of the person and be sure the person is in the correct age range.

In essence, the goal of Template 2 is to demonstrate that:

- the presenter of the credential is a human (i.e., proof of personhood);

- the presenter is the subject of the claims;
- the age claims are correct and matches the person at a given point in time.

Note that the minimum requirement is a name and “greater than” age from a trusted Credential Issuer. All other claims can be selectively consented by the Holder. Template 2 is a superset of Template 1.

Template 2 provides a schema for a SD-JWT VC using IANA-registered claims and has selective disclosure capabilities. Table 5 provides the claim details for Template 2 (See Appendix E for the full IANA listing).

Template 2			
Claim/Attribute	**Type**	**Source**	**Description**
given_name	string	IANA	Usual first name of the Subject
family_name	string	IANA	Usual last name of the Subject
picture	string	IANA	URL of the Subject’s profile picture pointing to an image file
gender	string	IANA	Gender of the Subject, including male, female and others
birthdate	string	IANA	Birthdate of the Subject in ISO 8601-1 format; 0000 to indicate omitted
is_over_18	boolean		True if over 18; otherwise, false
is_over_21	boolean		True if over 21; otherwise, false
is_over_65	boolean		True if over 65; otherwise, false
is_over_13_and_less_than_18	boolean		True if between 14 and 17; otherwise, false
sub	string	IANA	Subject identifier
issuer	string		Party that issued the VC
assurance_type	string		Assurance standard (e.g. NIST SP 800-63.3)
assurance_level	string		VC-AL1, VC-AL2, VC-AL3
assurance_evidence	string		URL for evidence relating to the VC assurance level
updated_at	number	IANA	Time of last update

Table 2: Basic Age Disclosure Schema

5.4 Template 3 – Financial Customer Schema

As noted in Section 4.2, financial institutions must use reasonable due diligence to determine and retain the identity of every customer and every person acting on behalf of those customers. Information required

for enforcing KYC regulations can vary by jurisdiction but typically includes customer name, date of birth, address, and an Identification Number.

Examples of situations where financial KYC could be applied include:

- Opening a bank account as a new customer;
- Applying for loans and other credit products; and
- Transferring large amounts of money especially across borders.

Financial KYC requirements will vary by jurisdiction and also by the risk management policies of the institutions. Enhanced due diligence requirements may be required for suspicious transactions, company ownership questions, and generally for developing customer risk profiles.

In the USA, Section 326 of the Patriot Act requires banks and other financial institutions to have a Customer Identification Program (CIP). Financial institutions must collect four pieces of identifying information about their customers including:

- Name
- Date of Birth
- Address
- Identification Number

Template 3 provides a schema for a simple JWT credential using IANA-registered claims and has no options or selective disclosure capabilities. Table 6.1 below provides the claim details for Template 3.

Template 3			
Claim/Attribute	**Type**	**Source**	**Description**
given_name	string	IANA	Usual first name of the Subject
middle_name	string	IANA	Middle name of the Subject
family_name	string	IANA	Usual last name of the Subject
phone_number	string	IANA	Preferred telephone number including country codes (E.164 format is recommended)
email	string	IANA	Preferred email address (RFC 5322 address)
address	JSON object	IANA	Preferred postal address (JSON RFC 8259 structure)
id_reference_type	string	IANA	Type of ID document (SSN, Resident ID, Aadhaar ID, etc.)
id_reference	string	IANA	Government-issued number
sub	string	IANA	Subject identifier
issuer	string		Party that issued the VC
assurance_type	string		Assurance standard (e.g. NIST SP 800-63.3) (Note 2)
assurance_level	string		VC-AL1, VC-AL2 or VC-AL3

assurance_evidence	string		URL for evidence relating to the VC assurance level
updated_at	number	IANA	Time of last update

Table 3: Financial Customer Schema

5.5 Template 4 – Basic Biometric VC Schema

A biometric VC can be used as a proof of personhood and would replace methods of testing for humanity such as CAPTCHA.

Interoperable biometrics require a set of standardized data elements to ensure seamless data exchange between different systems and components. The **Common Biometric Exchange Formats Framework [**CBEFF**]** provides a comprehensive set of these data elements. Here are some key elements:

1. **Biometric Identifier**: Numeric data elements used to identify biometric objects within biometric data records.
2. **Biometric Feature**: Defines the type of biometric data (e.g., fingerprint, face, voice).
3. **Validity Period**: Specifies the time period during which the biometric data is valid.
4. **Creator Field**: Identifies the product or entity that created the biometric data.
5. **Index Field**: Associates a specific instance of biometric reference data.
6. **Challenge-Response Field**: Used for security purposes to verify the authenticity of the biometric data.
7. **Payload Field**: Contains the actual biometric data.

Common Biometric Exchange Formats Framework

- ISO/IEC 19785-1:2020
- NIST IR 6529A (2004)

Template 4			
Claim/Attribute	**Type**	**Source**	**Description**
given_name	string	IANA	Usual first name of the Subject
family_name	string	IANA	Usual last name of the Subject
picture	string	IANA	URL of the Subject's profile picture pointing to an image file
biometric_method	string		Type of biometric
biometric_template	string		URL of the Subject's biometric template. This URL MUST refer to a biometric template (for example, a fingerprint), rather than to a Web page containing a file. Note that this URL SHOULD specifically reference a standards-based biometric

			template of the Subject suitable for comparing to an in-person biometric.
validity_period	string		Specifies the time period during which the biometric data is valid
biometric_creator	string		Identifies the product or entity that created the biometric data
sub	string	IANA	Subject identifier
issuer	string		Party that issued the VC
assurance_type	string		Assurance standard (e.g. NIST SP 800-63.3) (Note 2)
assurance_level	string		VC-AL1, VC-AL2 or VC-AL3
assurance_evidence	string		
updated_at	number	IANA	Time of last update

Table 4: Basic Biometric VC Schema

5.6 Template 5 – Expanded Personal Identity Schema

There will be situations for which the Service Provider wants or needs to gather a more complete customer profile. This could be useful for enhanced customer relationship management or to ensure variations in a customer description can be detected.

Table 5 provides a more extensive list of claims taken from the IANA list (extracted as of October 2024).

Claim/Attribute	Type		Description
sub	string	IANA	Subject - Identifier for the End-User at the Issuer.
name	string	IANA	End-User's full name in displayable form including all name parts, possibly including titles and suffixes, ordered according to the End-User's locale and preferences.
given_name	string	IANA	Given name(s) or first name(s) of the End-User.
family_name	string	IANA	Surname(s) or last name(s) of the End-User.
middle_name	string	IANA	Middle name(s) of the End-User.
nickname	string	IANA	Casual name of the End-User that may or may not be the same as the given_name. For instance, a nickname value of Mike might be returned alongside a given_name value of Michael
preferred_username	string	IANA	Shorthand name by which the End-User wishes to be referred to at the RP, such as janedoe or j.doe. This value MAY be any valid JSON string including

			special characters such as @, /, or whitespace. The RP MUST NOT rely upon this value being unique.
profile	string	IANA	URL of the End-User's profile page. The contents of this Web page SHOULD be about the End-User.
picture	string	IANA	URL of the End-User's profile picture. This URL MUST refer to an image file (for example, a PNG, JPEG, or GIF image file), rather than to a Web page containing an image. Note that this URL SHOULD specifically reference a profile photo of the End-User suitable for displaying when describing the End-User, rather than an arbitrary photo taken by the End-User.
website	string	IANA	URL of the End-User's Web page or blog. This Web page SHOULD contain information published by the End-User or an organization that the End-User is affiliated with.
email	string	IANA	End-User's preferred email address. Its value MUST conform to the RFC 5322 addr-spec syntax. The RP MUST NOT rely upon this value being unique.
email_verified	boolean	IANA	True if the End-User's email address has been verified; otherwise, false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this email address was controlled by the End-User at the time the verification was performed. The means by which an e-mail address is verified is context specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.
gender	string	IANA	End-User's gender. Values defined by this specification are female and male. Other values MAY be used when neither of the defined values are applicable.
birthdate	string	IANA	End-User's birthday, represented as an ISO8601-1 YYYY-MM-DD format. The year MAY be 0000, indicating that it is omitted. To represent only the year, YYYY format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.
zoneinfo	string	IANA	String from IANA Time Zone Database representing the End-User's time zone. For example, Europe/Paris or America/Los_Angeles.
locale	string	IANA	End-User's locale, represented as an RFC 5646 language tag. This is typically an ISO 639 language code in lowercase and an ISO 3166-1 country code in uppercase, separated by a dash. For example, en-US or fr-CA. As a compatibility note, some

			implementations have used an underscore as the separator rather than a dash, for example, en_US; Relying Parties MAY choose to accept this locale syntax as well.
phone_number	string	IANA	End-User's preferred telephone number. E.164 is RECOMMENDED as the format of this Claim, for example, +1 (425) 555-1212 or +56 (2) 687 2400. If the phone number contains an extension, it is RECOMMENDED that the extension be represented using the RFC 3966 extension syntax, for example, +1 (604) 555-1234;ext=5678.
phone_number_verified	boolean	IANA	True if the End-User's phone number has been verified; otherwise, false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this phone number was controlled by the End-User at the time the verification was performed. The means by which a phone number is verified is context specific, and dependent upon the trust framework or contractual agreements within which the parties are operating. When true, the phone_number Claim MUST be in E.164 format and any extensions MUST be represented in RFC 3966 format.
address	JSON object	IANA	End-User's preferred postal address. The value of the address member is a JSON RFC 8259 structure.
updated_at	number	IANA	Time the End-User's information was last updated. Its value is a JSON number representing the number of seconds from 1970-01- 01T00:00:00Z as measured in UTC until the date/time.
ID_reference_type	String		Type of ID document (SSN, Resident ID, Aadhaar ID, etc.)
ID_reference	String		Government-issued number
assurance_level	String		VC-AL1, VC-AL2 or VC-AL3
assurance_evidence	string		
updated_at	Number	IANA	Time of last update

Table 5: Expanded Personal Identity Schema

6 Conformance

Conformance Clause 1:

Implementations that conform to this standard MUST consume and produce documents that conform to the W3C Variable Credentials JSON Schema Specification and the W3C Variable Credentials Data Model v2.0 or later.

Conformance Clause 2:

An implementation that conforms to this standard MUST include all the claims specified in one of the templates in Section 5 of this document.

Specifically, the following claims are required:

- Template 1 includes all of the claims listed in Table 1.
- Template 2 includes all of the claims listed in Table 2.
- Template 3 includes all of the claims listed in Table 3.
- Template 4 includes all of the claims listed in Table 4.
- Template 5 includes all of the claims listed in Table 5.

Conformance Clause 3:

A document that conforms to this standard MUST be valid against the JSON Schema of the selected template and formatted as an SD-JWT or a JWT.

Appendix A. References

This appendix contains the normative and informative references that are used in this document.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long-term validity.

A.1 Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[RFC 2119]

Key words for use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>

[RFC 8174]

Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>

[IANA JWT]

JSON Web Token Claims, IANA, https://www.iana.org/assignments/jwt/jwt.xhtml

[OIDC]

OpenID Connect Core 1.0 incorporating errata set 2, December 15, 2023

https://openid.net/specs/openid-connect-core-1_0.html

[NIST 800-63]

Digital Identity Guidelines, NIST Special Publication 800-63-3

https://pages.nist.gov/800-63-3/

[RFC7519]

JSON Web Tokens (JWT), IETF 7519 May 2015

https://datatracker.ietf.org/doc/html/rfc7519

[RFC8259]

T. Bray, Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>

[W3C VCJS]

Verifiable Credentials JSON Schema Specification – JSON Schema for Verifiable Credentials – W3C Candidate Recommendation Draft 12 September 2024,

https://www.w3.org/TR/vc-json-schema/

[W3C VC DM2]

W3C Verifiable Credentials Data Model v2.0 – W3C Candidate Recommendation Draft, 26 January 2025,

https://www.w3.org/TR/vc-data-model-2.0/

[SD-JWT]

SD-JWT-based Verifiable Credentials (SD-JWT VC), draft-ietf-oauth-sd-jwt-vc-08

https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/

A.2 Informative References

The following referenced documents are not required for the application of this document but may assist the reader with regard to a particular subject area.

[EUDI]

The many use cases of **EU Digital Identity Wallets**

https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet

[RFC3552]

Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003,

https://www.rfc-editor.org/info/rfc3552

[ITUT1252]

Series X: Data Networks, Open system Communications and Security – Baseline identity management terms and definitions ITU-T X.1252

https://www.itu.int/rec/T-REC-X.1252-202104-I

[ITUT1254]

Series X: Data Networks, Open system Communications and Security – Entity authentication assurance framework ITU-T X.1254

https://www.itu.int/rec/T-REC-X.1254-202009-I/en

[OID-IA]

OpenID Connect for Identity Assurance 1.0, October 1, 2024

https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

[OID-IAS]

OpenID Identity Assurance Schema Definition 1.0, October 1, 2024

https://openid.net/specs/openid-ida-verified-claims-1_0-final.html

[OID-VCI]

OpenID for Verifiable Credential Issuance - draft 15, December 19, 2024

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[GFMCMARK]
GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C,
https://github.com/github/cmark
[GFMENG]
GitHub Engineering: A formal spec for GitHub Flavored Markdown,
https://githubengineering.com/a-formal-spec-for-github-markdown/

[ISO/IEC 18013-5]
Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application
https://www.iso.org/standard/69084.html

[CBEFF]
ISO/IEC 19785-1:2020 - Information technology — Common Biometric Exchange Formats Framework
https://www.iso.org/standard/77892.html

Appendix B. Security and Data Protection Considerations

Verifiable credential (VC) documents are based on JSON, thus the security considerations of [RFC8259] apply and are repeated here as service for the reader:

Generally, there are security issues with scripting languages. JSON is a subset of JavaScript but excludes assignment and invocation.

Since JSON's syntax is borrowed from JavaScript, it is possible to use that language's "eval()" function to parse most JSON texts (but not all; certain characters such as U+2028 LINE SEPARATOR and U+2029 PARAGRAPH SEPARATOR are legal in JSON but not JavaScript). This generally constitutes an unacceptable security risk, since the text could contain executable code along with data declarations. The same consideration applies to the use of eval()-like functions in any other programming language in which JSON texts conform to that language's syntax.

In addition, VC documents may be rendered by consumers in various human-readable formats like HTML or PDF. Thus, for security reasons, VC producers and consumers SHALL adhere to the following:

- VC producers SHOULD NOT emit messages that contain HTML, even though GitHub-flavoured Markdown is permitted. To include HTML, source code, or any other content that may be interpreted or executed by a VC consumer, e.g. to provide a proof-of-concept, the issuing party SHALL use Markdown's fenced code blocks or inline code option.
- Deeply nested markup can cause a stack overflow in the Markdown processor [GFMENG]. To reduce this risk, VC consumers SHALL use a Markdown processor that is hardened against such attacks. Note: One example is the GitHub fork of the "`cmark`" Markdown processor [GFMCMARK].

  To reduce the risk posed by possibly malicious VC files that do contain arbitrary HTML (including, for example, "`data:image/svg+xml`"), VC consumers SHALL either disable HTML processing (for example, by using the "`--safe`" option in the "`cmark`" Markdown processor) or run the resulting HTML through an HTML sanitizer.

  To reduce the risk posed by possibly malicious links within a VC document (including, for example, "`javascript:`" links), VC consumers SHALL either remove all actions from links (for example, by displaying them as standard text) or render only those actionable that are known to be safe (for example, determining that via the media type). VC consumers that are not prepared to deal with the security implications of formatted messages SHALL NOT attempt to render them and SHALL instead fall back to the corresponding plain text messages. As also any other programming code can be contained within a VC document, VC consumers SHALL ensure that none of the values of a VC document is run as code. Moreover, it SHALL be treated as unsafe (user) input.

Additional, supporting mitigation measures like retrieving only VC documents from trusted sources and check their integrity and signature before parsing the document SHOULD be in place to reduce the risk further.

Any safety, security, and data protection requirements of the context in which VCs are used, have to be translated to and upheld by VC implementation and processes.

Appendix C. Acknowledgments

C.1 Special Thanks

Substantial assistance from the following individuals during the preparation of this document is gratefully acknowledged:

Don Sheppard, Individual Member

Stefan Hagen, Individual Member

C.2 Participants

The following individuals were members of this Technical Committee during the creation of this document and their contributions are gratefully acknowledged:

Members

Abbie Barbir	CVS Health	Secretary
Alan Bachmann	Aetna	Co-chair
Charles Hart	Hitachi	
Chris Dotson	IBM	
Jan Herrmann	Siemens AG	
Jane Ginn	Individual Member	
John Sabo	Individual Member	
Mercedes Anders	HYPR	
Michael Streuling	Aetna	
Paul Ivanivsky	Aetna	
Scott Dowsett	Anomoli	
Vasileios Mavroeidis	University of Oslo	

Past Members and Advisors

Adar Weidman	JFrog
Hiroshi Takechi	NEC Corporation
Kim Hamilton Duffy	Advisor
Kiran Addepalli	Advisor
Louie Gasparini	Advisor
Ryan Rowcliffe	HYPR
Spencer Yezo	HYPR

Appendix D. Revision History

Revisions made since the initial stage of this numbered Version of this document are tracked here.

Revision	Date	Editor	Changes Made
[Rev number]	[Rev Date]	[Modified By]	[Summary of Changes]

Appendix E. Registered VC Claims

E.1 IANA Registered VC Claims

This specification makes use of claim elements that have been registered by IANA [JSON Web Token Claims, IANA, https://www.iana.org/assignments/jwt/jwt.xhtml] as of the date of publication of this document.

This specification is not submitting any new claim elements for registration by IANA.

Appendix F. Sample VC Schemas

This section is informative.

F.1 Sample VC Schema for Template 1 – Basic Personal Identity Schema

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schemaT1",
  "title": "Basic Personal Identity Credential",
  “description”: “Example of Template 1”
  "type": "object",
  "properties": {
    "subject": {
      "type": "string",
      "description": "Unique identifier for the customer"
    },
    "given_name": {
      "type": "string",
      "description": "Customer's given (first) name"
    },
    "family_name": {
      "type": "string",
      "description": "Customer's family (last) name"
    },
    "phone_number": {
      "type": "string",
      "description": "Customer's phone number"
    },
    "email": {
      "type": "string",
      "format": "email",
      "description": "Customer's email address"
    },
    "address": {
      "type": "object",
      "description": "Customer's physical address"
    },
    "assurance_level": {
      "type": "string",
      "description": "Level of assurance of the credential",
      "enum": ["VC-AL1", "VC-AL2", "VC-AL3"]
    },
    "updated_at": {
      "type": "string",
      "format": "date-time",
      "description": "Timestamp of the last update to the credential"
    }
  },
```

```
  "required": ["subject", "given_name", "family_name", “phone_number”,
"email", "assurance_level", "updated_at"]
}
```

Note: The sample VC Schema for Template 5 (Expanded Personal ID Schema) is the same as above with the additional claims inserted.

F.2 Sample VC Schema for Template 2 – Basic Age Disclosure Schema

```
{
  "$id": "https://example.com/credential-schema.json",
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Basic Age Disclosure Schema",
  "description": "Example of Template 2",
  "type": "object",
  "properties": {
    "given_name": {
      "type": "string",
      "description": "Given name of the individual"
    },
    "family_name": {
      "type": "string",
      "description": "Family name of the individual"
    },
    "picture": {
      "type": "string",
      "format": "uri",
      "description": "URL to the individual's picture"
    },
    "gender": {
      "type": "string",
      "description": "Gender of the individual"
    },
    "birthdate": {
      "type": "string",
      "format": "date",
      "description": "Birthdate of the individual"
    },
    "is_over_18": {
```

```
    "type": "boolean",
    "description": "Is the individual over 18 years old"
  },
  "is_over_21": {
    "type": "boolean",
    "description": "Is the individual over 21 years old"
  },
  "is_over_65": {
    "type": "boolean",
    "description": "Is the individual over 65 years old"
  },
  "is_over_13_and_less_than_18": {
    "type": "boolean",
    "description": "Is the individual over 13 and less than 18 years old"
  },
  "sub": {
    "type": "string",
    "description": "Subject identifier"
  },
  "issuer": {
    "type": "string",
    "description": "Credential issuer"
  },
  "assurance_type": {
    "type": "string",
    "description": "Type of assurance provided"
  },
  "assurance_level": {
    "type": "string",
    "description": "Level of assurance",
    "enum": ["VC-AL1", "VC-AL2", "VC-AL3"]
  },
  "assurance_evidence": {
    "type": "array",
    "items": {
      "type": "string"
    },
    "description": "Evidence supporting the assurance"
  },
  "updated_at": {
    "type": "string",
```

```
      "format": "date-time",
      "description": "Timestamp of the last update"
    }
  },
  "required": ["given_name", "family_name", "picture", "gender", "birthdate",
"sub", "issuer", "updated_at"]
}
```

F.3 Sample VC Schema for Template 3 – Basic Financial Customer Schema

```
{
  "$id": "https://example.com/credential-schema.json",
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Basic Financial Customer Schema",
  "description": "Example of Template 3",
  "type": "object",
  "properties": {
    "given_name": {
      "type": "string",
      "description": "Given name of the individual"
    },
    "middle_name": {
      "type": "string",
      "description": "Middle name of the individual"
    },
    "family_name": {
      "type": "string",
      "description": "Family name of the individual"
    },
    "phone_number": {
      "type": "string",
      "description": "Phone number of the individual"
    },
    "email": {
      "type": "string",
      "format": "email",
      "description": "Email address of the individual"
    },
```

```
  "address": {
    "type": "object",
    "description": "Physical address of the individual",
    "properties": {
      "unit_number": {
        "type": "string",
        "description": "Unit number of the address"
      },
      "street": {
        "type": "string",
        "description": "Street name and number"
      },
      "city": {
        "type": "string",
        "description": "City of the address"
      },
      "postal_code": {
        "type": "string",
        "description": "Postal code of the address"
      },
      "country": {
        "type": "string",
        "description": "Country of the address"
      }
    },
    "required": ["street", "city", "postal_code", "country"]
  },
  "ID_reference_type": {
    "type": "string",
    "description": "Type of ID reference"
  },
  "ID_reference": {
    "type": "string",
    "description": "ID reference of the individual"
  },
  "sub": {
    "type": "string",
    "description": "Subject identifier"
  },
  "issuer": {
    "type": "string",
```

```
      "description": "Credential issuer"
    },
    "assurance_type": {
      "type": "string",
      "description": "Type of assurance provided"
    },
    "assurance_level": {
      "type": "string",
      "description": "Level of assurance",
      "enum": ["VC-AL1", "VC-AL2", "VC-AL3"]
    },
    "assurance_evidence": {
      "type": "array",
      "items": {
        "type": "string"
      },
      "description": "Evidence supporting the assurance"
    },
    "updated_at": {
      "type": "string",
      "format": "date-time",
      "description": "Timestamp of the last update"
    }
  },
  "required": ["given_name", "family_name", "phone_number", "email",
"address", "sub", "issuer", "updated_at"]
}
```

F.4 Sample VC Schema for Template 4 – Basic Biometric VC Schema

```
{
  "$id": "https://example.com/credential-schema.json",
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Basic Biometric VC Schema",
  "description": "Example of Template 4",
  "type": "object",
  "properties": {
    "given_name": {
      "type": "string",
```

```
    "description": "Given name of the individual"
  },
  "family_name": {
    "type": "string",
    "description": "Family name of the individual"
  },
  "picture": {
    "type": "string",
    "format": "uri",
    "description": "URL to the individual's picture"
  },
  "biometric_method": {
    "type": "string",
    "description": "Biometric method used",
    "enum": ["fingerprint", "facial recognition", "iris scan", "voice recognition"]
  },
  "biometric_template": {
    "type": "string",
    "description": "Template of the biometric data"
  },
  "validity_period": {
    "type": "string",
    "description": "Validity period of the credential",
    "format": "date-time"
  },
  "Biometric_creator": {
    "type": "string",
    "description": "Entity or device that created the biometric data"
  },
  "sub": {
    "type": "string",
    "description": "Subject identifier"
  },
  "issuer": {
    "type": "string",
    "description": "Credential issuer"
  },
  "assurance_type": {
    "type": "string",
    "description": "Type of assurance provided"
  },
```

```
    "assurance_level": {
      "type": "string",
      "description": "Level of assurance",
      "enum": ["VC-AL1", "VC-AL2", "VC-AL3"]
    },
    "assurance_evidence": {
      "type": "array",
      "items": {
        "type": "string"
      },
      "description": "Evidence supporting the assurance"
    },
    "updated_at": {
      "type": "string",
      "format": "date-time",
      "description": "Timestamp of the last update"
    }
  },
  "required": ["given_name", "family_name", "picture", "biometric_method",
"biometric_template", "validity_period", "sub", "issuer", "updated_at"]
}
```

F.5 Sample VC Schema for Template 4 – Basic Biometric VC Schema (CBEFF fields)

```
"@context": [
"https://www.w3.org/2018/credentials/v1",
{
    "cbeff": "https://example.org/cbeff#",
    "biometricIdentifier": "cbeff:biometricIdentifier",
    "biometricFeature": "cbeff:biometricFeature",
    "validityPeriod": "cbeff:validityPeriod",
    "creator": "cbeff:creator",
    "index": "cbeff:index",
    "challengeResponse": "cbeff:challengeResponse",
    "payload": "cbeff:payload"
  }
]
```

Appendix G. Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website: [https://www.oasis-open.org/policies-guidelines/ipr/].

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]

The name "OASIS" is a trademark of OASIS, the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark/ for above guidance.