

# Verifiable Claims Data Model 1.0

Expressing verifiable information on the Web



[W3C Editor's Draft 29 August 2017](#)

**This version:**

<https://w3c.github.io/vc-data-model/>

**Latest published version:**

<https://www.w3.org/TR/verifiable-claims-data-model/>

**Latest editor's draft:**

<https://w3c.github.io/vc-data-model/>

**Editors:**

Daniel C. Burnett, [Standards Play](#)

Manu Sporny, [Digital Bazaar](#)

Dave Longley, [Digital Bazaar](#)

Gregg Kellogg, [Spec-Ops](#)

**Authors:**

Manu Sporny, [Digital Bazaar](#)

Dave Longley, [Digital Bazaar](#)

**Participate:**

[GitHub w3c/vc-data-model](#)

[File a bug](#)

[Commit history](#)

Copyright © 2017 [W3C](#)<sup>®</sup> ([MIT](#), [ERCIM](#), [Keio](#), [Beihang](#)). [W3C liability, trademark and permissive document license rules apply.](#)

---

## Abstract

Driver's licenses are used to claim that we are capable of operating a motor vehicle, university degrees can be used to claim our education status, and government-issued passports enable holders to travel between countries. This specification provides a standard way to express these sorts of claims on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.

## Status of This Document

*This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current [W3C publications](#) and the latest revision of this technical report can be found in the [W3C technical reports index](https://www.w3.org/TR/) at <https://www.w3.org/TR/>.*

Comments regarding this document are welcome. Please file issues directly on [GitHub](#), or send them to [public-vc-comments@w3.org](mailto:public-vc-comments@w3.org) ([subscribe](#), [archives](#)).

This document was published by the [Verifiable Claims Working Group](#) as an Editor's Draft. Comments regarding this document are welcome. Please send them to [public-vc-comments@w3.org](mailto:public-vc-comments@w3.org) ([subscribe](#), [archives](#)).

Publication as an Editor's Draft does not imply endorsement by the [W3C Membership](#). This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work in progress.

This document was produced by a group operating under the [5 February 2004 W3C Patent Policy](#). [W3C](#) maintains a [public list of any patent disclosures](#) made in connection with the deliverables of the group; that page also includes instructions for disclosing a patent. An individual who has actual knowledge of a patent which the individual believes contains [Essential Claim\(s\)](#) must disclose the information in accordance with [section 6 of the W3C Patent Policy](#).

This document is governed by the [1 March 2017 W3C Process Document](#).

## Table of Contents

- 1. Introduction**
  - 1.1 What is a Verifiable Claim?
  - 1.2 Ecosystem Overview
  - 1.3 Use Cases and Requirements
- 2. Terminology**
- 3. Core Data Model**
  - 3.1 Claims
  - 3.2 Credentials
  - 3.3 Profiles
- 4. Basic Concepts**
  - 4.1 Issuer
  - 4.2 Signature

- 4.3 Expiration
- 4.4 Revocation
- 5. Advanced Concepts**
- 5.1 Evidence
- 6. Verification**
- 6.1 Syntax
- 6.2 Credential
- 6.3 Issuer
- 6.4 Subject
- 6.5 Signature
- 6.6 Expiration
- 6.7 Revocation
- 6.8 Fitness for Purpose
- 7. Syntaxes**
- 7.1 JSON
  - 7.1.1 Verifiable Credential
  - 7.1.2 Verifiable Profile
- 7.2 JSON-LD
  - 7.2.1 Verifiable Credential
  - 7.2.2 Verifiable Profile
- 8. Privacy Considerations**
- 8.1 Spectrum of Privacy
- 8.2 Personally Identifiable Information
- 8.3 Identifier-based Correlation
- 8.4 Signature-based Correlation
- 8.5 Device Fingerprinting
- 8.6 Favor Abstract Claims
- 8.7 The Principle of Minimum Disclosure
- 8.8 Bearer Claims
- 8.9 Validity Checks
- 8.10 Storage Providers and Data Mining
- 8.11 Aggregation of Claims
- 8.12 Usage Patterns
- 8.13 Sharing Information with the Wrong Party
- 8.14 Frequency of Claim Issuance
- 8.15 Prefer Single Use Claims

## 9. Security Considerations


- 9.1 Unsigned Claims
- 9.2 Bundling Dependent Claims
- 9.3 Highly Dynamic Information


## A. References


- A.1 Normative references
- A.2 Informative references

# 1. Introduction

Granting a benefit requires proof and verification. Some benefits demand a formal process that includes three parties. In this process, the **holder** asks for the benefit and the **inspector-verifier** grants or denies the benefit based on verification of the holder's qualification from a trusted **issuer**.

For example, we use  driver's licenses to prove that we are ~~capable of operating~~ a motor vehicle, a university degree to prove our education status, and government-issued passports to grant travel between countries. This specification provides a standard way to express these claims on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.

For those that are unfamiliar with the concepts related to verifiable claims,  the following sections provide an overview of:

1. what a verifiable claim  contains,
2. an ecosystem where verifiable claims are expected to be useful, and
3. the use cases and requirements that informed this specification

## 1.1 What is a Verifiable Claim?

### ISSUE

Expand on introductory verifiable claims section that doesn't dive too deeply into the details but rather provides an overview of what we're trying to achieve.

## 1.2 Ecosystem Overview

This section outlines a basic set of roles and an ecosystem where verifiable claims are expected to be useful. In this section, we distinguish the essential roles of core actors and the relationships be-

tween them; how do they interact? A role is an abstraction that might be implemented in many different ways. The separation of roles suggests likely interfaces and/or protocols for standardization. The following roles are introduced in this specification:

## ISSUE

The VCWG is actively discussing the number of roles and terminology used in this specification. The group expects terminology and role identification to be an ongoing discussion and will be influenced by public feedback on the specification. At present, the following incomplete list of roles and terminology have been considered: Subject, Issuer, Authority, Author, Signatory, Holder, Presenter, Asserter, Claimant, Sharer, Subject's Agent, Prover, Mediator, Inspector, Evaluator, Verifier, Consumer, and Relying Party. Some of these are aliases for the same concept, others are possibly new roles in the ecosystem. Reviewers should be aware that the terminology used in this document is not necessarily final and the group is actively soliciting feedback on the roles and terminology used in this specification.

## holder

An entity that is in control of one or more verifiable claims. Examples of holders include students, employees, and customers.

## issuer

An entity that creates a verifiable claim, associates it with a particular subject, and transmits it to a holder. Examples of issuers include corporations, governments, and individuals.

## inspector-verifier

An entity that receives one or more verifiable claims for processing. Examples of inspector-verifiers include employers, security personnel, and websites.

## identifier registry

Mediates the creation and verification of subject identifiers. Examples of identifier registries include corporate employee databases, government ID databases, and distributed ledgers.

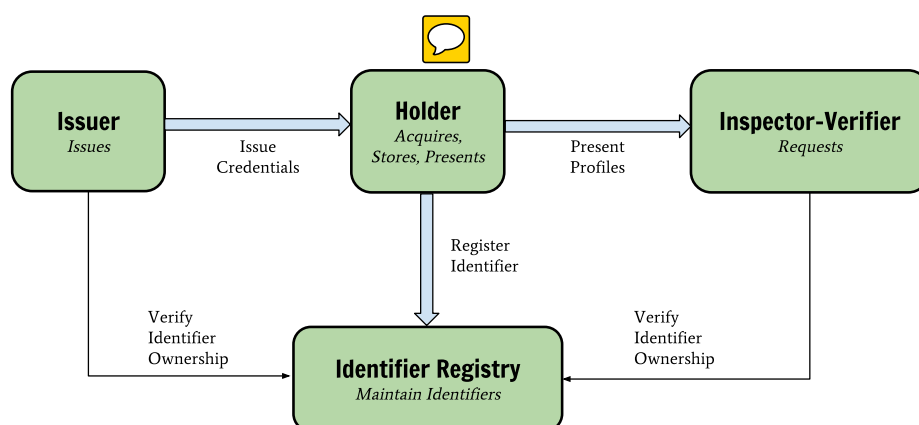


Figure 1 The roles and information flows that form the basis for this specification.

## NOTE






The ecosystem above is provided as an example to the reader in order to ground the rest of the concepts in this specification. Other ecosystems exist, such as protected environments or proprietary systems, where verifiable claims also provide benefit.

## 1.3 Use Cases and Requirements

The Verifiable Claims Use Cases[[VC-USECASES](#)] document outlines a number of key topics that readers may find useful, including:

- a more thorough explanation of the [roles](#) introduced above,
- the [needs](#) identified in market verticals like education, finance, healthcare, retail, professional licensing, and government,
- common [tasks and requirement](#) performed by the roles in the ecosystem, and
- common [sequences and flows](#) identified by the Working Group.

As a result of documenting and analyzing the use cases document, a number of desirable capabilities have been identified as requirements for this specification, specifically:

- **credential**  **credential**
- **Holders must** receive and store [verifiable claims](#) from [issuers](#) through an agent that the issuer does not need to trust. 
- **Holders should** be positioned between [issuers](#) and [inspector-verifiers](#) and mediate the transmission of [verifiable claims](#). 
- **Holders must** provide [verifiable claims](#) to [inspector-verifiers](#) through an agent that inspector-verifiers needn't trust; they only need to trust [issuers](#). 
- [Verifiable claims](#) **must** be associated with [subjects](#), not particular services; [holders](#) **should** decide how to aggregate and manage [verifiable claims](#). 
- **Holders should** be able to easily control and own their own identifiers.
- **Holders must** control which [verifiable claims](#) to use and when.
- **Holders must** be able to freely choose and change the agents they employ to help them manage and share their [verifiable claims](#).
- **Holders** that share [verifiable claims](#) **must not** be required to reveal the identity of the [inspector-verifier](#) to [issuers](#).
- A [verifiable claim](#) **must** be expressed in one or more standard, machine-readable data formats for expressing [verifiable claims](#) which can also be extended with minimal coordination.

- Verifiable claims **must** be able to be independently issued, stored, and verified.
- Verifiable Claims **must** be able to be revoked by the issuer.

## ISSUE

There are other requirements listed in the Verifiable Claims Use Cases document that may or may not be aligned with the requirements listed above. The VCWG will be ensuring alignment of the list of requirements from both documents over time and will most likely move the list of requirements to a single document.

## 2. Terminology

This document attempts to communicate the concepts outlined in the Verifiable Claims space by using specific terms to discuss particular concepts. This terminology is included below and linked to throughout the document to aid the reader:

### *claim*

A statement made about a subject. A **verifiable claim** is a claim that is tamper-resistant and whose authorship can be cryptographically verified.

### *entity*

A thing with distinct and independent existence such as a person, organization, concept, or device.

### *credential*

A set of one or more claims made by the same entity about a subject. A **verifiable credential** is a credential that is tamper-resistant and whose authorship can be cryptographically verified.

### *holder*

An entity that is in control of one or more verifiable claims. A holder is typically also the primary subject of the verifiable claims that they are holding.

### *profile*

A set of one or more credentials typically related to the same subject. An entity may have multiple profiles and each profile may contain verifiable credentials issued by multiple issuers. A **verifiable profile** is a profile that is tamper-resistant and whose contents are typically counter-signed by the holder or subject.

### *identifier registry*

Registries typically mediate the creation and verification of subject identifiers. Some registries, such as ones for UUIDs and public keys, act merely as namespaces for identifiers.

### *issuer*

An entity that creates a verifiable claim, associates it with a particular subject, and transmits it to a holder.

**subject**

An entity which may have multiple verifiable profiles and about which claims may be made.

**inspector-verifier**

An entity that receives one or more profiles for processing.

**ISSUE 55: Multiple subjects in a single credential**

It is currently possible to include multiple subjects in a credential. The terminology above glosses over that fact. The group is debating if the terminology should be modified to include this nuance, or if the nuance would make grasping the basic concepts more difficult.



### 3. Core Data Model

The following sections outline core data model concepts, such as claims, credentials, and profiles, that form the foundation of this specification.

#### 3.1 Claims

A claim is statement about a subject. A subject is an entity about which claims may be made. Claims are expressed using *subject-property-value* relationships.

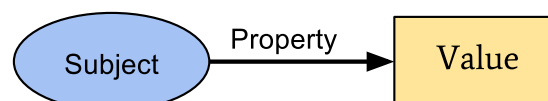


Figure 2 The basic structure of a claim.

The data model for claims described above is powerful and can be used to express a large variety of statements. For example, whether or not someone is over the age of 21 may be expressed as follows:

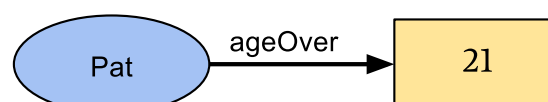



Figure 3 An example of a basic claim that expresses that Pat is over the age of 21.



These claims may be merged together to express a graph of information about a particular subject. The example below extends the data model above by adding claims that state that Pat knows Sam and that Sam is a student. 

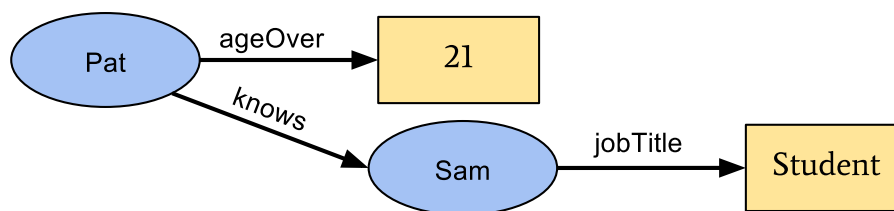



Figure 4 Multiple claims may be combined to express a more complex graph.

At this point, the concept of a claim has been introduced. To make the claim verifiable, more information must be added to the graph of information.

### 3.2 Credentials

A credential is set of one or more claims about a subject. It typically includes an identifier to uniquely identify the credential. Credential metadata may also be included to express concepts such as when the credential expires. A digital signature is **most always**  provided by the issuer of the credential to enable verifiability of the credential. Therefore, a **verifiable credential** is a set of claims that are tamper-resistant and whose authorship can be cryptographically verified.

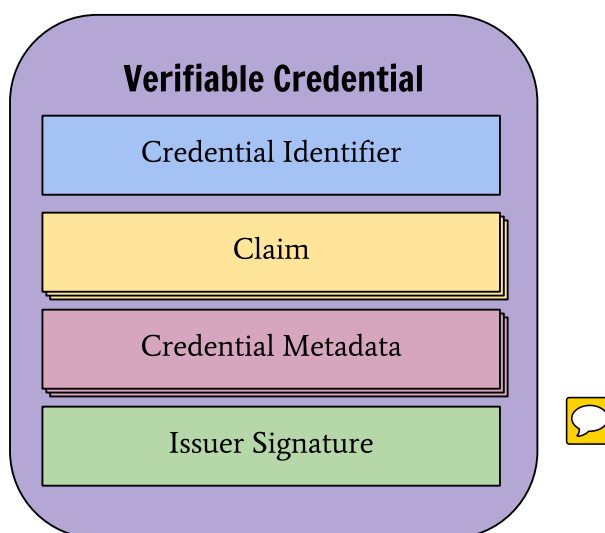





Figure 5 The basic components of a verifiable credential.

Examples of verifiable credentials include digital employee identification cards, digital proofs of age, and digital educational certificates.

## 3.3 Profiles

As this specification takes a privacy-first approach, it is important that the entities that use this technology are able to express only the portions of their persona that are appropriate for the situation. **The expression of a subset of one's persona is called a verifiable profile.** 

A **verifiable profile** is a collection of one or more **verifiable credentials** **typically about the same subject** that have been issued by multiple **issuers**. The aggregation of this information typically expresses an aspect of a **person, organization, or entity.**   


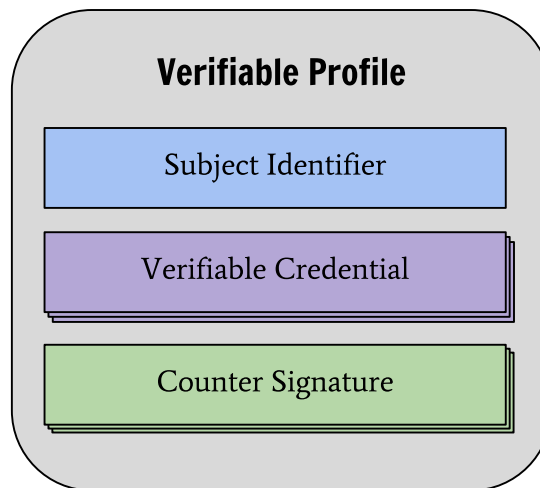


Figure 6 The basic components of a verifiable profile.

Examples of different profiles include a person's professional persona, online gaming persona, or home life persona.

## 4. Basic Concepts

### 4.1 Issuer

Issuer information may be expressed via the following properties:

#### *issuer*

The value of this property **must** be a URI. It is **recommended** that dereferencing the URI results in a document containing machine-readable information about the issuer that may be used to verify the information expressed in the credential.

#### *issued*

The value of this property **must** be a string value of an [ISO8601] combined date and time string and represents the date and time the credential was issued. Note that this date represents the earliest date when the information associated with the *claim* property became valid.

**EXAMPLE 1: Usage of issuer properties**

```
{
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issued": "2010-01-01T19:73:24Z",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": { ... }
}
```

## 4.2 Signature

A [credential](#) may be made verifiable by adding the following [property](#):

### *signature*

The method used for a signature will vary by representation language. However, this property is expected to have a value that is a set of name-value pairs including at least a signature, a reference to the signing entity, and a representation of the signing date.

**EXAMPLE 2: Usage of signature property**

```
{
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": {
    "type": "LinkedDataSignature2017",
    "created": "2017-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
    "signatureValue": "BavE1l0/I1zpYw8XNi1bgVg/sCne04Jugez8RwDg/+
MCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR9Cky6Ed
+W3JT24="
  }
}
```

### 4.3 Expiration

Expiration information for the [credential](#) **may** be provided by adding the following [property](#):

***expires***

The value of this property **must** be a string value of an [\[ISO8601\]](#) combined date and time string and represents the date and time the [credential](#) will cease to be valid.

**EXAMPLE 3: Usage of expires property**

```
{
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issued": "2010-01-01T19:73:24Z",
  "expires": "2020-01-01T19:73:24Z",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": { ... }
}
```


## 4.4 Revocation

Revocation information for the claims in the Verifiable Claims Model may be provided by adding the following [property](#):

***revocation***

The value of this property **must** be a revocation scheme that provides enough information to determine whether or not the credential has been revoked. The revocation scheme will vary depending on a variety of factors, such as whether it is simple to implement or privacy-enhancing.

**ISSUE 35: Define ONE concrete format for the revocation parameter**

The group is currently determining whether or not they should publish a very simple scheme for revocation as a part of this specification. 

#### EXAMPLE 4: Usage of revocation property

```
{
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issued": "2010-01-01T19:73:24Z",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "revocation": {
    "id": "https://dmv.example.gov/revocation/24",
    "type": "RevocationList2017"
  },
  "signature": { ... }
}
```



## 5. Advanced Concepts

### 5.1 Evidence

Evidence information for the claims in the Verifiable Claims Model may be provided by adding the following [property](#):

#### *evidence*

The value of this property **must** be one or more evidence schemes that provides enough information to a [inspector-verifier](#) to determine whether or not the evidence gathered meets their requirements.

#### ISSUE

The group is currently determining whether or not they should publish a very simple scheme for evidence as a part of this specification.

**EXAMPLE 5: Usage of evidence property**

```
{
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issued": "2010-01-01T19:73:24Z",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "evidence": {
    "id": "https://dmv.example.gov/evidence/f2aee97-fc0d-42bf-8ca7-054",
    "type": "DocumentVerification",
    "verifier": "https://dmv.example.gov/issuers/14",
    "evidenceDocument": "DriversLicense",
    "subjectPresence": "Physical",
    "documentPresence": "Physical"
  },
  "signature": { ... }
}
```

## 6. Verification

This section describes a number of checks required to verify a claim. Some checks are essential for all verifiable claims, while some are applicable to only some claims.

### 6.1 Syntax

- Document is syntactically valid (e.g. JSON, JSON-LD).

### 6.2 Credential


- Required properties are present. For example, for a Credential, **type** and **claim** are required.
- Property values match expectations described in the specification. For example, the document type for a verifiable claim must contain the class "Credential".

### 6.3 Issuer

- The **issuer** id must match expectations. Likely, that means it is the id of a known and trusted verifiable profile.
- Recent metadata about the **issuer** which was published by the issuer **must** be available.

## 6.4 Subject



- The claim subject identifier must match expectations. Likely, that means it is the id of a known and trusted verifiable profile for the subject of the claim. If the entity that is subject of a claim has transmitted it to the inspector-verifier, the subject may be able to prove ownership of key identifying properties such as email address(es) and public key(s). 

## 6.5 Signature

- The document signature is available in the form of a known signature suite.
- Required signature properties are present. For example, for a Linked Data Signature, **type**, **created**, **creator**>, and **signatureValue** are present.
- The public key associated with the signature is available and a trustworthy link between this signing key and the issuer's verifiable profile may be established. The key must not be revoked or expired.
- The cryptographic signature is valid.

## 6.6 Expiration

- The **issued** date must be in the expected range. For example, an inspector-verifier may wish to ensure that the recorded issued date of valid claims is not in the future.

and that the expires date is not in the past

## 6.7 Revocation

- If revocation instructions are present, the claim must not have been revoked.

## 6.8 Fitness for Purpose

- The custom properties in the claim should be appropriate for the inspector-verifier's purpose. For example if an inspector-verifier needs to determine that a subject is older than 21 years of age, they may accept claims of specific birthdate or abstract properties such as **ageOver**.
- The issuer is trusted by the inspector-verifier to make the claims at hand. For example, Fast



Food Resturant A will not be trusted to make a claim that an individual may enjoy a lifetime 10% discount to its competitor Fast Food Restaurant B.

- If the issuer has placed any policy information about the use of the credential, e.g. intended inspector-verifiers, expiration date, etc., that this policy is adhered to.
- If the holder has placed any policy information about the use of the credential, e.g. intended inspector-verifiers, restricted usage rights, etc., that this policy is adhered to.

#### 6.9. Holder

The inspector-verifier should check that the holder is authorised to posses the credential.

## 7. Syntaxes

This section defines how the data model described in Section is realized in each of 3 different languages: JSON, JSON-LD, and WebIDL. Although syntactic mappings are only provided for these three different languages, applications and services may also use any other data representation language (XML, for example) that can support the data model.

### 7.1 JSON

#### 7.1.1 Verifiable Credential

In JSON, an instance of the Verifiable Credential is expressed as a single JSON object whose properties are the verifiable credential's properties, with the following value type assignments:

- Any number value **must** be represented as a Number type.
- Any boolean value **must** be represented as a Boolean type.
- Any sequence value **must** be represented as an Array type.
- Any unordered set of values **must** be represented as an Array type.
- Any set of properties **must** be represented as an Object type.
- Any empty value **must** be represented as a null value.
- Any other value **must** be represented as a String type.

The following example demonstrates how to express an verifiable credential containing a simple (unverifiable) claim about a particular subject. In this case, the claim is that the subject with the Verifiable Profile id of `did:ebfeb1f712ebc6f1c276e12ec21` is 21 years of age or older. While a human reading the property `age0ver` may be able to guess its meaning by its name, no machine-readable semantics for the name are provided. There is information about the claim itself, such as an identifier for the entity that issued it and a date for when it was issued.

**EXAMPLE 6: A simple claim**

```
{
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21", // subject identifier
  "ageOver": 21 // property-value pair
}
```

The following example demonstrates how to express the same [claim](#) about the same [subject](#), but in a verifiable form. As such, it contains a [signature](#) that can be used to verify its entire contents, including the claim.

**EXAMPLE 7: A simple verifiable credential**

```
{
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "revocation": {
    "id": "http://example.gov/revocations/738",
    "type": "SimpleRevocationList2017"
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavE1l0/I1zpYw8XNi1bgVg/sCne04Jugez8RwDg/+
MCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
PRdW+gGsutPTLzvueMwmFhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR9Cky6Ed
+W3JT24="
  }
}
```

The following example demonstrates how one could express the same [claim](#) about the same [subject](#) using a JSON Web Token.



```
// JWT Header
{
  "alg": "RS256",
  "typ": "JWT"
}
// JWT Payload
{
  "iss": "https://dmv.example.gov",
  "iat": 1262304000,
  "exp": 1483228800,
  "aud": "www.example.com",
  "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "entityCredential": {
    "@context": "https://w3id.org/security/v1",
    "id": "http://example.gov/credentials/3732",
    "type": ["Credential", "ProofOfAgeCredential"],
    "issuer": "https://dmv.example.gov",
    "issued": "2010-01-01",
    "claim": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "ageOver": 21
    }
  }
}
```

The following example demonstrates how to express a more complex set of verifiable claims about a particular [subject](#).

**EXAMPLE 9: A more complex verifiable claim**

```
{
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "PassportCredential"],
  "name": "Passport",
  "issuer": "https://example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "Alice Bobman",
    "birthDate": "1985-12-14",
    "gender": "female",
    "nationality": {
      "name": "United States"
    },
    "address": {
      "type": "PostalAddress",
      "addressStreet": "372 Sumter Lane",
      "addressLocality": "Blackrock",
      "addressRegion": "Nevada",
      "postalCode": "23784",
      "addressCountry": "US"
    },
    "passport": {
      "type": "Passport",
      "name": "United States Passport",
      "documentId": "123-45-6789",
      "issuer": "https://example.gov",
      "issued": "2010-01-07T01:02:03Z",
      "expires": "2020-01-07T01:02:03Z"
    }
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-21T03:40:19Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "783b4dfa",
    "signatureValue": "Rxj7Kb/tDbGHFAs6ddHjVLSHDiNyYzxs2MPmNG8G47oS06NE"
  }
}
```

**7.1.2 Verifiable Profile**

In JSON [[JSON](#)], an instance of the Verifiable Profile is expressed as a single JSON object whose properties are the verifiable profile's [properties](#), with the following value type assignments:

- Any number value **must** be represented as a Number type.
- Any boolean value **must** be represented as a Boolean type.
- Any sequence value **must** be represented as an Array type.
- Any unordered set of values **must** be represented as an Array type.
- Any set of [properties](#) **must** be represented as an Object type.
- Any empty value **must** be represented as a null value.
- Any other value **must** be represented as a String type.

The following example demonstrates how to express a simple [verifiable profile](#).

**EXAMPLE 10: A simple verifiable profile**

```

{
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "credential": [{
    "id": "http://dmv.example.gov/credentials/3732",
    "type": ["Credential", "ProofOfAgeCredential"],
    "issuer": "https://dmv.example.gov/issuers/14",
    "issued": "2010-01-01T19:73:24Z",
    "claim": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "ageOver": 21
    },
    "signature": {
      "type": "LinkedDataSignature2017",
      "created": "2017-06-17T10:03:48Z",
      "creator": "https://dmv.example.gov/issuers/14/keys/234",
      "nonce": "d61c4599-0cc2-4479-9efc-c63add3a43b2",
      "signatureValue": "pYw8XNi1bgVg/sCne04BavEll0/I1zJugez8RwDg/+
ibcC1wpsMCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuF
zvueMwmFPRdW+gGsutPTLhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR+W3JT24
9Cky6Ed="
    },
  ]},
  "signature": [{
    "type": "LinkedDataSignature2017",
    "created": "2017-06-18T21:19:10Z",
    "creator": "did:example:ebfeb1f712ebc6f1c276e12ec21/keys/2",
    "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCne04Jugez8RwDg/+
MCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
PRdW+gGsutPTLzvueMwmFhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR9Cky6Ed
+W3JT24="
  }]
}

```

## 7.2 JSON-LD

JSON-LD [[JSON-LD](#)] is a data storage and expression approach called [Linked Data](#). It is a way of expressing information on the Web that is both simple and extensible.

### 7.2.1 Verifiable Credential

Instances of the [Verifiable Credential](#) are expressed in JSON-LD in the same way they are expressed in JSON (Section ), except that there is an additional [property @context](#). Each property of the [verifiable credential](#) expression, along with each sub-property within the [claim](#) property (such as the generic [issuer](#) property or the app-specific [age0ver](#)), is given context via the [@context](#) value. Other contexts can be used or combined to express any arbitrary information about claims in idiomatic JSON.

The following example demonstrates how to express a simple (unverifiable) [claim](#) about a particular [subject](#). In this case, the claim is that the [subject](#) with the [Entity Profile id](#) of [did:ebfeb1f712ebc6f1c276e12ec21](#) is 21 years of age or older. While a human reading the property [age0ver](#) may be able to guess its meaning by its name, the context maps it to a global identifier (URL) where a document could be retrieved that provides its semantics in a machine-readable data format. There is also information about the [claim](#) itself, such as an identifier for the [entity](#) that issued it and a date for when it was issued.

#### EXAMPLE 11: A simple claim

```
{
  "@context": "https://w3id.org/identity/v1",
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "age0ver": 21
}
```

The following example demonstrates how to express the same [claim](#) about the same [subject](#), but in a verifiable form. As such, it contains a [signature](#) that can be used to verify its entire contents, including the claim.



**EXAMPLE 12: A simple verifiable credential**

```
{
  "@context": [
    "https://w3id.org/identity/v1",
    "https://w3id.org/security/v1"
  ],
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:10:38Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "6165d7e8",
    "signatureValue": "g4j9UrpHM4/uu32NlTw0HDSaYF2sykskfuByD7UbuqEcJI"
  }
}
```

The following example demonstrates how to express a more complex set of verifiable claims about a particular [subject](#).

EXAMPLE 13: A more complex verifiable credential

```
{
  "@context": [
    "https://w3id.org/identity/v1",
    "https://w3id.org/security/v1"
  ],
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "PassportCredential"],
  "name": "Passport",
  "issuer": "https://example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "Alice Bobman",
    "birthDate": "1985-12-14",
    "gender": "female",
    "nationality": {
      "name": "United States"
    },
    "address": {
      "type": "PostalAddress",
      "addressStreet": "372 Sumter Lane",
      "addressLocality": "Blackrock",
      "addressRegion": "Nevada",
      "postalCode": "23784",
      "addressCountry": "US"
    },
    "passport": {
      "type": "Passport",
      "name": "United States Passport",
      "documentId": "123-45-6789",
      "issuer": "https://example.gov",
      "issued": "2010-01-07T01:02:03Z",
      "expires": "2020-01-07T01:02:03Z"
    }
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-21T03:43:29Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "c168dfab",
    "signatureValue": "jz4bEW2FBMDkANYEjiPnrIctucHQCIwxrtzBXt+rVGmYMEf"
  }
}
```

## 7.2.2 Verifiable Profile

Instances of the [Verifiable Profile](#) are expressed in JSON-LD in the same way they are expressed in JSON (Section ), except that there is an additional property `@context`. Each property of the verifiable profile, such as `name` or `email`, is given context via the `@context` value. Other contexts can be used or combined to express any arbitrary information about an [verifiable profile](#) in idiomatic JSON.

The following example demonstrates how to express a simple [verifiable profile](#).

**EXAMPLE 14: A simple verifiable profile**

```

{
  "@context": [
    "https://w3id.org/identity/v1",
    "https://w3id.org/security/v1"
  ],
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "credential": [{
    "id": "http://dmv.example.gov/credentials/3732",
    "type": ["Credential", "ProofOfAgeCredential"],
    "issuer": "https://dmv.example.gov/issuers/14",
    "issued": "2010-01-01T19:73:24Z",
    "claim": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "ageOver": 21
    },
    "signature": {
      "type": "LinkedDataSignature2017",
      "created": "2017-06-17T10:03:48Z",
      "creator": "https://dmv.example.gov/issuers/14/keys/234",
      "nonce": "d61c4599-0cc2-4479-9efc-c63add3a43b2",
      "signatureValue": "pYw8XNi1bgVg/sCne04BavEll0/I1zJugez8RwDg/+
      ibcC1wpsMCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuF
      zvueMwMfPRdW+gGsutPTLhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR+W3JT24
      9Cky6Ed="
    }
  ]},
  "signature": [{
    "type": "LinkedDataSignature2017",
    "created": "2017-06-18T21:19:10Z",
    "creator": "did:example:ebfeb1f712ebc6f1c276e12ec21/keys/2",
    "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCne04Jugez8RwDg/+
    MCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
    PRdW+gGsutPTLzvueMwMfhwYmfIFpbBu95t501+rSLHIEuuJM/+PXR9Cky6Ed
    +W3JT24="
  }]
}

```

**ISSUE 54: Should spec include WebIDL and XML expressions**

The group is currently considering which expressions of the data model should be listed in the spec. WebIDL and XML are two of the expressions that are being considered.

## 8. Privacy Considerations

This section details the general privacy considerations and specific privacy implications of deploying the verifiable claims data model into production environments.

### 8.1 Spectrum of Privacy

It is important to recognize that there is a spectrum of privacy that ranges from pseudo-anonymous to strongly identified. Depending on the use case, people have different appetites when it comes to what information they are willing to provide and what information may be derived from what is provided.

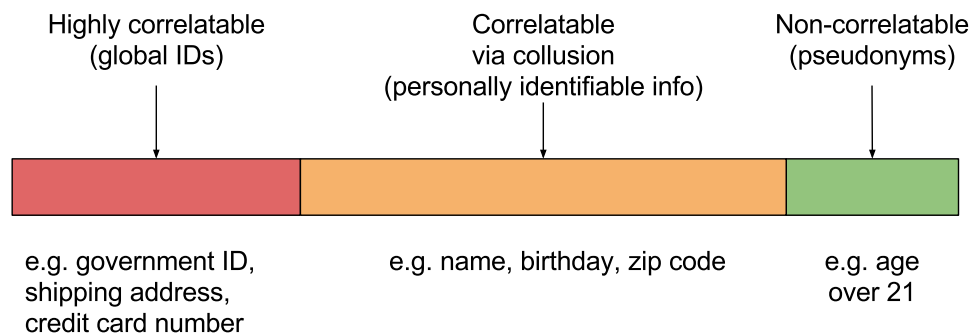


Figure 7 - Privacy is a spectrum that ranges from pseudo-anonymous to fully identified.

For example, one would most likely desire to remain anonymous when purchasing alcohol because the regulatory check that's required is solely whether or not the person is above a particular age. However, when a doctor is writing a prescription for a patient, the pharmacy fulfilling the prescription is required to more strongly identify the medical professional. Therefore it is important to recognize that there is not one approach to privacy that works for all use cases; privacy solutions tend to be use case specific.

#### ISSUE

Note that even if one may desire to remain anonymous when purchasing alcohol, a photo ID may still be required to provide appropriate assurance to the merchant. The merchant may not need to know your name or other details (other than that you are over a certain age), but in many cases a mere proof of age may still be insufficient to meet regulations.

The Verifiable Claims data model strives to support the full spectrum of privacy and does not take philosophical positions on the right level of anonymity for any particular transaction. The follow-

ing sections provide guidance for implementers that want to avoid specific scenarios that are hostile to privacy.

## 8.2 Personally Identifiable Information

The data associated with verifiable claims stored in the `credential.claim` field are largely susceptible to privacy violations when shared with Inspector-verifiers. Personally identifying data such as a government-issued identifier, shipping address, and full name can be easily used to determine, track, and correlate an entity. Even information that does not seem personally identifiable like the combination of a birth date and zip code have very powerful correlation and de-anonymizing capabilities.

Implementers are strongly advised to warn Holders when they share data with these sorts of characteristics. Issuers are strongly advised to provide privacy-protecting credentials when possible. For example, issuing `ageOver` credentials instead of `birthdate` credentials when the Inspector-verifier desires to determine if an entity is over the age of 18.

## 8.3 Identifier-based Correlation

Subjects of verifiable claims are identified via the `credential.claim.id` field. The identifiers that are used to identify the subject of a claim create a danger of correlation when the identifiers are long-lived or used across more than one web domain.

If strong anti-correlation properties are a requirement in a system using verifiable claims, it is strongly advised that identifiers are bound to a single origin or that identifiers are single-use or not used at all and are replaced by short-lived, single use bearer tokens.

## 8.4 Signature-based Correlation

The contents of verifiable claims are secured via the `credential.signature` field. The `credential.signature.signatureValue` field creates a danger of correlation when it is used across more than one web domain and the value does not change.

If strong anti-correlation properties are desired, it is strongly advised that signature values and metadata are regenerated each time using technologies like group signatures.

## 8.5 Device Fingerprinting

There are mechanisms external to Verifiable Claims that are used to track and correlate individuals

on the Internet and the Web. Some of these mechanisms include Internet Protocol address tracking, Web Browser fingerprinting, Evercookies, Advertising Network trackers, mobile network position information, and in-application Global Positioning System APIs. The use of Verifiable Claims cannot prevent the use of these other tracking technologies. In addition, when these technologies are used in concert with Verifiable Claims, new correlatable information may be discovered. For example, a birthday coupled with a GPS position can be used to strongly correlate an individual across multiple websites.

It is advised that privacy preserving systems prevent the use of these other tracking technologies when verifiable claims are being utilized. In some cases, these tracking technologies may need to be disabled entirely on devices that transmit verifiable claims on behalf of the Holder.

## 8.6 Favor Abstract Claims

In order to enable recipients of verifiable claims to use them in a variety of circumstances without revealing more personally identifiable information than necessary for the transaction, issuers should consider limiting the information published in a claim to a minimal set needed for the expected purposes. One way to avoid placing personally identifiable information in a claim is to use an "abstract" property that meets the needs of inspector-verifiers without providing specific information about the subject.

An example in this document is the use of the `ageOver` property as opposed to a specific birthdate that would constitute much stronger personally identifiable information. If retailers in a market commonly require purchasers to be older than a specific age, an issuer trusted in that market may choose to offer a credential claiming that subjects have met that requirement as opposed to offering claims of their specific birthdates. This enables individual customers to purchase items without revealing specific personally identifiable information.

## 8.7 The Principle of Minimum Disclosure

Privacy violations occur when information divulged in one context leaks into another. Accepted best practice for preventing such violations is to limit the information requested, and received, to the absolute minimum necessary. This minimal disclosure approach is required by regulation in multiple jurisdictions, including HIPAA in the US and GDPR in the EU.

With verifiable claims, minimal disclosure for issuers means limiting the content of a claim to the minimum required by potential inspector-verifiers for expected use. For inspector-verifiers, it means limiting the scope of claims request or required for accessing services.

For example, a driver's license containing a driver's ID number, height, weight, birthday, and home address is an example of a claim set containing more information than is necessary to establish that



the person is above a certain age.

It is considered a best practice for issuers to atomize information or use a signature scheme that allows for selective disclosure. For example, an issuer that issues driver's licenses could issue a claim set containing every attribute that appears on a driver's license in addition to individual claims (a singular claim containing the person's birthday), and individual claims that are more abstract (a singular claim containing an `ageOver` attribute). In addition, the issuer is encouraged to provide secure HTTP endpoints for retrieving single-use bearer claims to promote the pseudonymous usage of claims when it is safe for the issuer to issue such claims.

Similarly, inspector-verifiers are urged to only request information that is absolutely necessary for a particular transaction to occur. This is important for at least two reasons: 1) it reduces the liability on the inspector-verifier for handling highly sensitive information that it does not need, and 2) it enhances the privacy of the individual by only asking for information that is required for the particular transaction.

## 8.8 Bearer Claims

### ISSUE

Bearer claims containing PII or unique identifiers can be correlated. Bearer claims can be tracked based on usage patterns.

## 8.9 Validity Checks

### ISSUE

Inspector-verifier (corporation) is required to check revocation via Issuer (government).

## 8.10 Storage Providers and Data Mining

When a holder receives a claim from an issuer, the claim will need to be stored somewhere (e.g. in a credential repository). Holders are warned that the information in a verifiable claim may be sensitive in nature and highly individualized, making it a high value target for data mining. Therefore, there may be services that store verifiable claims for free and mine personal data and sell it to organizations that desire individualized profiles on people and organizations (i.e. if the service is free, you are the product).

It is suggested that holders be aware of the terms of service for their credential repository, specifically the correlation and data mining protections that are in place for those who store their verifiable claims at the service provider.

There are a number of effective mitigations for data mining and profiling:

- Use service providers that do not sell your information to third parties.
- Use software that encrypts verifiable claims such that a service provider cannot view the contents of the claims.
- Use software that stores verifiable claims locally on a device that you control and that does not upload or analyze your information beyond your expectations.

## 8.11 Aggregation of Claims

### ISSUE

Aggregation of claims can reveal more information than just the attributes being aggregated.

## 8.12 Usage Patterns

Despite the best efforts to assure privacy, the actual use of verifiable claims can potentially lead to de-anonymization and a loss of privacy. This correlation can occur:

1. When the same claim is presented to the same inspector-verifier more than once – that inspector-verifier could infer that the holder is the same individual.
2. When the same claim is presented to different inspector-verifiers, and either those inspector-verifiers collude or a third party has access to transaction records from both inspector-verifiers – the observant party could infer that the individual presenting the claims is the same person at both services, i.e., the accounts are controlled by the same person.
3. When the same subject identifier of a claim refers to the same subject across presentations or inspector-verifiers. Even when different claims are presented, if the subject identifier is the same, inspector-verifiers (and those with access to inspector-verifier logs) could infer that the holder of the claims is the same person.
4. When the underlying information in a claim can be used to identify an individual across services – using information from other sources (including information provided directly by the user), inspector-verifiers can use the information inside the claim to correlate the individual with an existing profile. For example, if a holder presents claims that include zip code, age,

and sex, the inspector-verifier can potentially correlate the subject of that claim with an established profile [see Sweeney 2000 [Simple Demographics Often Identify People Uniquely](#)].

5. When passing the identifier of a claim to a centralized revocation server – the centralized server can correlate the claim usage across interactions. For example, if a verifiable claim is used for proof of age in this manner, the centralized service could know everywhere that claim was presented: all liquor stores, bars, adult stores, lottery purchases, etc.

It's possible to mitigate this in part:

1. Use a globally unique identifier as the subject for any given claim and never re-use that claim.
2. If the claim supports revocation, use a globally distributed service for revocation.
3. Design revocation APIs that do not depend on submitting the ID of the claim, e.g., use a revocation list rather than a query.
4. Avoid associating personally identifiable information with any particular long-lived subject identifier.

It is understood that these mitigation techniques are not always practical or even compatible with necessary usage. Sometimes correlation is the point.

In state prescription monitoring programs, usage monitoring is a requirement: enforcement entities need to be able to confirm that individuals are not cheating the system to get multiple prescriptions for controlled substances. This statutory or regulatory need to correlate usage overrides individual privacy concerns.

Verifiable claims will so be used to intentionally correlate individuals across services, for example, when using a common persona to log in to multiple services, so all activity on each of those services is intentionally linked to the same individual. This is not a privacy issue as long as each of those services uses the correlation in the expected manner.

Privacy risks of claim usage occur when unintended or unexpected correlation arises from the presentation of verifiable claims.

### 8.13 Sharing Information with the Wrong Party

#### ISSUE

Tokenize identifiers (like bank account numbers) when possible. Granting of rights to a service via cryptographic mechanisms.

## 8.14 Frequency of Claim Issuance

### ISSUE

The rate at which an issuer issues claims may be a privacy violation.

## 8.15 Prefer Single Use Claims

### ISSUE

Single-use, origin bound claims are generally safer than long-lived claims.

# 9. Security Considerations

## 9.1 Unsigned Claims

### ISSUE

Claims that are not digitally signed are not verifiable.

## 9.2 Bundling Dependent Claims

It is considered a best practice for issuers to atomize information in a credential, or use a signature scheme that allows for selective disclosure. In the former case, if the atomization is not done securely by the issuer, the holder might bundle together different credentials in a way that was not intended by the issuer.

For example a university might issue two credentials to a person, each containing two properties i.e. "Staff Member" in the "Department of Computing" and "Post Graduate Student" in the "Department of Economics". If these credentials are atomized into separate properties, then the university would issue four credentials to the person, each containing one of the following properties: "Staff Member", "Post Graduate Student", "Department of Computing" and "Department of Economics". The holder could then transfer the "Staff Member" and "Department of Economics" to an inspector-verifier, which together would comprise a false claim.

### ISSUE 17: Dependent claims should be bundled

The group is actively discussing appropriate strategies when bundling dependent claims. When a clear set of suggestions has been identified, they will be placed here.

## 9.3 Highly Dynamic Information

### ISSUE

Time periods should be shorter for highly dynamic information.

## A. References

### A.1 Normative references

#### [ISO8601]

*Representation of dates and times. ISO 8601:2004.*. International Organization for Standardization (ISO). 2004. ISO 8601:2004. URL: [http://www.iso.org/iso/catalogue\\_detail?csnumber=40874](http://www.iso.org/iso/catalogue_detail?csnumber=40874)

#### [JSON]

*The application/json Media Type for JavaScript Object Notation (JSON)*. D. Crockford. IETF. July 2006. Informational. URL: <https://tools.ietf.org/html/rfc4627>

#### [JSON-LD]

*JSON-LD 1.0*. Manu Sporny; Gregg Kellogg; Markus Lanthaler. W3C. 16 January 2014. W3C Recommendation. URL: <https://www.w3.org/TR/json-ld/>

### A.2 Informative references

#### [VC-USECASES]

*Verifiable Claims Use Cases*. Shane McCarron; Daniel Burnett; Gregg Kellogg; Brian Sletten; Manu Sporny. Verifiable Claims Working Group. W3C First Public Working Draft. URL: <https://www.w3.org/TR/verifiable-claims-use-cases/>

