Consent Extension Elements 1.0

Proposal 2022-08-22

Latest editor's draft:

<https://xxx>

Editors:

tbd

Authors:

### Thomas C. Jones, Salvatore D’Agostino

Version Control:

tbd

[Copyright](https://www.w3.org/Consortium/Legal/ipr-notice#Copyright) © 2022 by the Contributors to the Consent Extension Elements

Abstract

There are many standards, like OAUTH 2.0 that have been repurposed by other standards, like OpenID Connect, into providing functions to be used by ordinary people employing ubiquitous browser User Experiences. What they were not designed to enable is user privacy and control. Security and some privacy measures are typically addressed in existing standards. However, these standards do not adequately address people’s concerns as evidenced by the current state of user privacy and control. This document defines data elements that are specific to people’s privacy and control when added into existing flows, like OAUTH 2.0. The document focuses on a presentation to people that allows informed consent decisions.

Status of This Document

This specification is proposed to the W3C Consent Community WG for adoption as a work item.

If you wish to make comments regarding this document, please send them to tbd

# 1. Introduction

We typically are asked to provide data about ourselves to authenticate and ultimately gain access to various resources in both the real word and the digital domains. For example, we use some unique identification such as email addresses to identify ourselves to online services, driver's licenses to prove that the subject is permitted to operate a motor vehicle, university degrees to prove the subject is well-trained and knowledgeable, and government-issued passports to travel between countries or to access financial services. When the credentials are presented, some proof of presence, like a picture or a secret password is used to provet that we are the subject identified in that credential. It is the goal of this specification to provide an easy, standard way to express a request for data and the user’s consent to that request. Unlike other specifications on consent, this specification does not define a protocol for exchanging collections of data elements between parties as perfectly good protocols already exist for that purpose. This specification does not assume that the user will be protected by the traditional browser, but rather assumes that the user agent will be operating in the best interests of the user. If the browser will not respect the user’s intent, then it is assumed that the browser will no longer be permitted to present any user data to the Relying Party. There are a number of desirable capabilities for these kinds of data elements, referred to in this specification as Privacy Controls, that have been identified as requirements for this specification.

Privacy Controls refer to an architecture where:

Privacy Controls bind both users[[1]](#footnote-1) and verifiers to a negotiated set of conditions.

Privacy Controls must be able to be simplify the request into a Consent Dialog[[2]](#footnote-2) that a holder can comprehend, hiding all the inessential details.

Privacy Controls operating through an agent must have a secure place to store private information (often PII)

Privacy Controls record local policies on how private information is released to others.

Privacy Controls operate through an agent that can also supply proof of presence of the holder to the verifier.

Privacy Controls agents will be able to display any purpose requested in a form and with language that allow a holder to make an informed consent decision.

Privacy Controls only supply information that is required to complete the business at hand. Any other data requested must be designated as OPT-IN. by the user agent.

Privacy Controls require that any request for their information must be understood sufficiently to make an informed decision about whether to proceed with the current transaction.

A standard, machine-readable data format for expressing Privacy Controls that can be extended with minimal coordination.

An independent issuance, storage, and cryptographic verification of any Privacy Controls and the related Notice or Consent.

A standard mechanism for requesting private data.

A standard mechanism for expressing Agreement (Consent, Grant?) for terms of use for that user private data.

The ability to manage Privacy Controls and Consent dynamically and over time including where applicable, revocation, suspension, updating and re-issuing.al

This specification is based upon work presented in … TBD

Instructions on how to express specific instances of the data elements in two different syntactic formulations: JSON, and JSON-LD.

# 2. Terminology

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

*Entity*

A named object with distinct and independent existence such as a person, organization, data base, or device.

*Holder*

An entity that controls the data for the user. It may refer to the user or to a guardian or delegate.

*User*

A named human that is the subject of the user private data. In order to be precise this document will typically use terms subject or holder rather than user.

*Verifier*

An entity or collection of entities that requires user personal data, (provide a notice about the nature of its need/purpose) and makes a request specifying the purpose for which the data is requested and verifies the Consent element presented returned by the user agent.

*Relying Party*

An entity the relies on data supplied by the user. The verifier of the data may be a role within the Relying Party, or a in a separate entity. The relying party will be either a data controller or a data processor as defined in the GDPR.

*Consent Element*

A statement of the conditions for data transfer acceptable to the user. It may be signed itself or part of a signed message. (Statement of layered notice requirements)

*Purpose Element*

A data element that can be used to create a user experience element that gives the user all of the information that they need to make an informed decision about releasing their private data. (OK so notice is a part of this..) Authority, Purpose, Justification, Notice, Consent

*Presentation*

A collection of data elements created by a user agent in response to a request from a Verifier. Also, the information about the Verifier presented to the user agent.

*Context*

A statement about the scope of applicability of the purpose and consent. It will be expressed as a URL that can point to a structure that can define (e.g.) the terms used for the purpose element. (This can be captured in a receipt that is part of a record that is returned by the Relying Party).

# 3. Purpose

This element is a request, or response to a request, to provide any private data about the subject

EXAMPLE a: A simple purpose request

{

 "@context": "https://w3c.org/xxx ",

 "id": "http://example.gov/credentials/3732",

 "required": ["ageOver:21"],

 “optional”:[“gender”]

}

EXAMPLE b: A simple purpose response

{

 "@context": "https://w3c.org/xxx ",

 "id": "http://example.gov/credentials/3732",

 "type": ["Credential", "DriversLicense"],

 "issuer": "https://dmv.example.gov",

 "issued": "2011-01-01",

 “duration”:”ephemeral”,

 "assertion": {

 "id": "did:ebfeb1f712ebc6f1c276e12ec21",

 "ageOver": 21

 }

}

EXAMPLE c: A rich purpose request

{

 "@context": "https://w3c.org/xxx ",

 "id": "http://example.gov/credentials/3732",

 "optional": ["RewardsProgram",”Name”,”Address”,”mail:to:],

}

EXAMPLE d: A rich purpose response

{

 "@context": "https://w3c.org/xxx ",

 "id": "http://example.gov/credentials/3732",

 "type": ["Credential", "DriversLicense"],

 "issuer": "https://dmv.example.gov",

 "issued": "2011-01-01",

 “duration”:”2022-12-31”,

 "assertion": {

 [

 "name": "Joe Smith",

 "address": [“201 Maple Drive”,”Sunnyvale”,”California”,”90000”],

 "mailto": “joe@smith.com”

 ]

 }

}

# 4. Consent

This element gives the user control over private data. It clearly expresses the user intent to share data with the Relying Party. It is designed with a great deal of flexibility so that it can be included in a wider variety of other structures. For example, the Consent Element could be included with proof of presence in a Presentation to a Relying Party.

EXAMPLE 8: A simple consent (expressed as a part of a JWS),

{

 "@context": [ <https://w3id.org/xxx> ],

 "id": "http://example.gov/credentials/3732",

 "type": ["Credential", "ProofOfAgeCredential"],

 "issuer": "https://dmv.example.gov",

 "issued": "2010-01-01",

 "assertion": {

 "id": "did: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/uu32NlTw0HDaSaYF2sykskfuByD7UbuqEcJIKa+IoLJLrLjqDnMz0adwpBCHWaqqpnd47r0NKZbnJarGYrBFcRTwPQSeqGwac8E2SqjylTBbSGwKZkprEXTywyV7gILlC8a+naA7lBRi4y29FtcUJBTFQq4R5XzI="

}

EXAMPLE 9: A standalone signed consent

TBD

# 5. User Experience

By far the most difficult and most essential part of the consenting process is to extract the essence of the request into a consent dialog that the user can understand in order to make an informed decision.

# 6. Privacy Considerations

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

## 6.1 Personally Identifiable Information

The data associated with assertions stored in the cloud are largely susceptible to privacy violations when shared with Verifiers. Personal 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.

User Agents MUST 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 Verifier desires to determine if an entity is over the age of 18.

## 6.2 Identifier-based Correlation

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

## 6.3 Signature-based Correlation

The contents of consents 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.

## 6.4 Device Fingerprinting

There are mechanisms external to consents 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, cookies, Advertising Network trackers, mobile network position information, and in-application Global Positioning System APIs. The use of consents cannot prevent the use of these other tracking technologies. In addition, when these technologies are used in concert with Consents, 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 consents are being utilized. In some cases, these tracking technologies may need to be disabled entirely on devices that transmit consents on behalf of the Holder.

## 6.5 Validity Checks

ISSUE

Verifier (corporation) is required to check revocation via Issuer (government).

Use software that stores user data locally on a device that you control and that does not upload or analyze your information beyond your expectations.

## 6.6 Usage Patterns

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

When the same assertion is presented to the same verifier more than once – that verifier could infer that the holder is the same individual.

When the same assertion is presented to different verifiers, and either those verifiers collude or a third party has access to transaction records from both verifiers – the observant party could infer that the individual presenting the assertions is the same person at both services, i.e., the accounts are controlled by the same person.

When the same subject identifier of a consent refers to the same subject across presentations or verifiers. Even when different assertions are presented, if the subject identifier is the same, verifiers (and those with access to verifier logs) could infer that the holder of the attribute is the same person.

When the underlying information in a consent can be used to identify an individual across services – using information from other sources (including information provided directly by the user), verifiers can use the information inside the consent to correlate the individual with an existing profile. For example, if a holder presents assertions that include zip code, age, and sex, the verifier can potentially correlate the subject of that assertion with an established profile [see Sweeney 2000 [Simple Demographics Often Identify People Uniquely](http://dataprivacylab.org/projects/identifiability/paper1.pdf)].

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

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.

Privacy risks of consent usage occur when unintended or unexpected correlation arises from the presentation of identifiable certificates.

## 6.7 Sharing Information with the Wrong Party

ISSUE

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

# 7. Security Considerations

## 7.1 Unsigned Consents

ISSUE

Consents that are not digitally signed are not verifiable.

## 7.2 Bundling Dependent Consents

ISSUE

Dependent assertions should be bundled together so they're not used for the wrong purposes.

## 7.3 Highly Dynamic Information

ISSUE

Time periods should be shorter for highly dynamic information.

# 8. Verification

This section describes a number of checks required to verify a assertion

## 78.1 Structural Validity

Document is valid JSON-LD.

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 consent must contain the class "Credential".

## 8.2 Entity Validity

A number of checks must be implemented to ensure a set of entities related to a Credential have mutually compatible properties and are trustworthy.

The issuer id must match expectations. Likely, that means it is the id of a known and trusted [identity profile](https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01/#dfn-identity-profile).

The subject identifier must match expectations. Likely, that means it is the id of a known and trusted [identity profile](https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01/#dfn-identity-profile)for the subject of the assertion. If the entity that is subject of a assertion has transmitted it to the verifier, the subject may be able to prove ownership of key identifying properties such as email address(es) and public key(s).

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

The document signature is available in the form of a known signature suite.

The public key associated with the signature is available and a trustworthy link between this signing key and the issuer's [identity profile](https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01/#dfn-identity-profile) may be established.

## 8.3 Fitness for Purpose

The custom properties in the assertion should be appropriate for the verifier's purpose. For example, if an verifier needs to determine that a subject is older than 21 years of age, they may accept assertions of specific birthdate or abstract properties such as ageOver.

# 9. Governance

## 9.1 At the User Agent

The user agent is an entity that is displayed in any message to the Relying Party.

The user experience MUST be designed to work on a smart phone and SHOULD display a single screen on top with a CONSENT icon. The single page may link to more detail as desired.

Required purposes may be assumed to be selected.

Optional purposes MUST be opt-in.

## 9.2 At the Relying Party

The Relying Party is an entity that is identified to the user along with any data request.

# A. References

A.1 Normative references

[JSON-LD]

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

A.2 Informative references

[PURPOSE]

Purpose for Access Request Thomas C. Jones URL: https://tcwiki.azurewebsites.net/index.php?title=Purpose\_for\_Access\_Request

[IDENTITY-CREDENTIALS]

[*Identity Credentials*](http://opencreds.org/specs/source/identity-credentials/). Manu Sporny; Dave Longley. W3C Credentials Community Group. CG-DRAFT. URL: <http://opencreds.org/specs/source/identity-credentials/>

[VERIFICABLE-CREDENTIALS]

Verifiable Claims working group [EDITOR'S DRAFT] Verifiable Claims Working Group Primer URL: [[EDITOR'S DRAFT] Verifiable Claims Working Group Primer (w3c.github.io)](https://w3c.github.io/webpayments-ig/VCTF/primer/)

1. Users can be and are often the Relying Party in OAuth, in that they are users of a person’s data, or require information in order to have resources to manage. [↑](#footnote-ref-1)
2. See DID Document <https://www.w3.org/TR/did-core/#dfn-did-documents> [↑](#footnote-ref-2)