Web Authorization Protocol
Internet-Draft
Intended status: Informational
Expires: 26 July 2021

V. Bertocci
auth0.com
G. Fletcher
Verizon Media

22 January 2021

Identity Use Cases in Browser Catalog
draft-bertocci-identity-in-browser-00

Abstract

This informational document aims to gather in a single place all the most important scenarios in which identity protocols in current use leverage web browser features to achieve their goals and deliver their intended user experience. The purpose of compiling this scenario collection is to make it easier for the identity community to engage with the browser vendors, and in particular to preserve (or enhance) user experience and expressive power of the identity protocols in mainstream use as browsers introduce new privacy preserving restrictions and new identity tailored features. By providing a single artifact, listing scenarios in a consistent format, we hope to anchor the conversation on concrete outcomes and impact of changes on end users, developers, providers and in general everyone contributing to identity in the industry.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 July 2021.

Table of Contents

1. Overview

As attempts to profile and track user activities on the web intensify, leading to increasingly egregious privacy violations, browser vendors introduce new constraints meant to thwart known tracking techniques. As they do so, however, they often end up

breaking legitimate use cases as well- with identity protocols features such as single sign on, token renewals and the like being disptoportionally affected. Conscious of those effects and committed to preserve user experience, browser vendors are working on dedicated identity API that aim at preserving and enhancing the user experience

in identity transactions, without relying on the general purpose artifacts on which current identity protocols depend on. One key challenge that is emerging in the process is that browser vendors tend to design around a limited set of well-known, consumer-only use cases, classifying most other cases as enterprise use cases hence solvable by exceptions and local business policies, whereas that is often not the case (e.g., single sign on is a common requirements across web properties even for consumer services, such as online managines form the same publisher) or the expected solutions (e.g. companies deploying MDM and managing policies on their employees and contributors machines) are not always viable. Discussions between browser vendors and identity experts are not always easy, and are frequently repeated whenever the individuals and initiatives involved change. This makes progress difficult. This infomational document is a collection of use cases in which identity protocols depend on web browser features to perform their intended function. By gathering the main use cases in a single, shared artifact, and by describing every use case thru a fixed schema designed to surface the most salient characteristics germane to the identity-browser features discussion, we aim to provide a tool to facilitate conversations between browser vendors and identity experts. This is meant to be a living document, constantly gathering and discussing scenarios contribuitions (via dedicated GitHub repository and OAuth working group mailing list) and periodically incorporating new entries in the main document. The contribution process is described in Section 3.

1.1. Scope

This document considers in scope scenarios and use cases for which all the following requirements apply: - must be in common use, represent a common practice, a behavior of products in widespread adoption, etc. - can be from any mainstream identity and authorization protocol specification, regardless of standard bodies affiliation: e.g. OAuth, OpenID Connect, SAML, etc. - must require use of browser features (e.g. cookies, redirects, decorated links, HTTP headers, local storage etc) for at least part of its sequence of

messages. - can involve, but isn't limited to: establishing a user session, obtaining credentials and intermediate artifacts (e.g. OAuth2 authorization codes).

The following is considered out of scope: - any scenario or protocol not currently in mainstream use, regardless of standardization status. - any scenario not using a web broweser in any capacity. - proposing new browser behaviors or API, or identity scenarios using hypothetical new browser capabilities. The goal of this project is to document what's already in place, to inform discussions about what's next taking place in forums shared with the browser vendors.

2. Conventions and Definitions

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] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Contribution Process

Before submitting feedback and contributions, please familiarize yourself with our current issues list and review the working group home page (https://datatracker.ietf.org/wg/oauth/documents/). If you're new to this, you may also want to read the Tao of the IETF (https://www.ietf.org/tao.html).

Be aware that all contributions to the specification fall under the "NOTE WELL" terms outlined here (https://www.ietf.org/about/note-well/).

This informational draft is meant to be a living document, where new scenarios and refinement of the current ones will keep being added as needed. This work originated in the IETF working group for OAuth (https://datatracker.ietf.org/wg/oauth/documents/), however we hope to gather contributions from the entire identity community, regardless of affiliation. Most of the work will happen on https://github.com/IDBrowserUseCases/docs (https://github.com/IDBrowserUseCases/docs), a GitHub repository meant to facilitate contributions from the community as summarized

below.

3.1. Contributing Scenarios

Each scenario is captured in a document following the template described in Section 4. You can find all contributed scenarios in docs/src/scenarios (https://github.com/IDBrowserUseCases/docs/tree/main/src/). If you want to contribute a new scenario: 1. Please read the preamble in this section and ensure that you meet all requirements 2. Verify that your scenario isn't already captured in any of the documents in docs/src/scenarios (https://github.com/IDBrowserUseCases/docs/tree/main/src/scenarios). If it a variant of an already captured scenario, or if you want to contribute to an existing scenario doc, please consider chiming in on the OAuth mailing list (https://www.ietf.org/mailman/listinfo/oauth). 3. If your scenario is new, please fork the repo and create a local copy of SCENARIOTEMPLATE.md, renaming your file to match the format protocolname_protocolscenario.md 4. Edit your local copy by filing

the appropriate sections of the template, see Section 4 for details. 5. Once you are ready, please submit a PR to add the new doc/reflect doc updates to the scenarios folder 6. Monitor the mailing list (https://www.ietf.org/mailman/listinfo/oauth) for discussions and requests for clarification

3.2. Discussing Scenarios Details and Inclusion

All submissions will be discussed on the mailing list (https://www.ietf.org/mailman/listinfo/oauth), possibly undergoing revisions according to the feedback. Once rough consensus is reached, the scenario will be included in this informational document.

4. The Use Case Template

We capture all scenarios following a template, with the intent of providing readers with a consistent way of understanding the scenario goals, intended user experience, browser feature dependencies, privacy characteristics and any other consideration that might help assessing impact of browser feature changes on the scenario. Here's a quick description of each template section. For more details,

please refer to the scenarios already captured.

* Scenario Name
  Each scenario document opens with a concise description of the scenario.

* Contributor
  This section captures the individual(s) contributing this scenario document and their affiliation.

* Protocol
  If the scenario is part of a standard (e.g. SAML, OpenID Connect, OAuth2, etc), this section provides details such as what standard document it refers to, and any reference that can be useful to learn more about the scenario. Examples include indicating specific use cases described by the standard (grants, flows, etc), links to articles and presentations describing the scenario in more detail and so on. Please note that scenarios captured here do not necessarily need to be formally described in a standard, as long as they are in common use. A good example would be the use of cookies for preserving the nonce in OpenID Connect, or the use of cookies for representing a web app session after a federated sign in flow (regardless of the specific protocol) took place.

* Browser Features Required
  This section provides a quick reference of the browser features that play a role in the correct execution of the scenario. Examples include 1st and 3rd party cookies, redirects with link decoration, form posts, access to local storage, iFrames, JavaScript, and so on.

* Intended User Experience
  Description of the intended user experience, with particular attention on the desired outcomes (eg no visible prompt in SSO scenarios)

* Description Of The Flow
  Description of the flow, including entities coming into play, begin state, end state, and sequence diagram when possible.

* Privacy Considerations
  Description of privacy characteristics of the scenario, with particular attention to aspects affecting the browser (eg presence of browser-readable artifacts carrying user info, use of global|pairwise|no identifiers, etc).

* Target Audience
  This section is meant to indicate whether the scenario is used prevalently for a particular audience (eg B2C,B2E, B2B, G2C) or if it can be expected to be relevant for more than one category.

* Adoption
  If known or easy to assess, this session enumerates notable products, industries, vendors that rely on the scenario as described.

* Miscellaneous
  Anything not fitting any of the sections above that is relevant for understanding how the scenario might be affected by browser changes.

5. Scenarios

5.1. OpenID Connect Redirect Based Sign in via Form POST

Web application RP1 offers sign in/sign up functionality for users of identity provider IP1, using OpenID Connect implicit flow and form_post. Ignoring how IP1 auths the user, apart from the fact that successful auth results in a cookie in IP1 domain..

5.1.1. Summary

5.1.1.1. Contributor

* Name: Vittorio Bertocci

* Organization: Auth0 Inc

* Email: vittorio@auth0.com

5.1.1.2. Protocol

* Name: OpenID Connect

* Grant/flow (if applicable): Implicit flow with form post

* Reference: see the (OpenID Connect Implicit flow)[https://openid.net/specs/openid-connect-core-1_0.html#ImplicitFlowAuth (https://openid.net/specs/openid-connect-core-1_0.html#ImplicitFlowAuth)] and (OAuth 2.0 Form Post Response Mode)[https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html (https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html)].

5.1.1.3. Browser Features Required

Per legs of the flow: RP1->IP1
- 1st party cookie (RP1 saves nonce) - Redirect - Decorated links - 1st party cookie (IP1 saves its session cookie upon successful authentication)
IP1->RP1 - Form post - 1st party cookie (nonce carrying cookie) - Javascript (autopost)

5.1.1.3.1. Target Audience

This patters applies to every audience, across the board

5.1.1.4. Adoption

TODO Enumeration of products, industries, vendors that rely on this scenario as described.

5.1.2. Description Of The Flow

TODO long form description of the flow, including start state, end state, and sequence diagram when possible

5.1.3. Intended User Experience

User navigates to RP1 without any pre existing session in place. Once there, either the user clicks on something (protected route, login button) or the app determines an authentication operation is immediately required. This causes the browser to be redirected to IP1, where the user is presented with authentication prompts (details of the authentication factors/mechanics omitted in this particular scenario). Upon successful authentication, the browser is redirected to RP1, and the user is now signed in RP1.

5.1.4. Privacy Considerations

An ID token does transit thru the browser, however 1. It's not meant for the browser. Format might change. It might be encrypted. 2. It might or might not contain profile user attributes

5.1.5. Miscellaneous

TODO anything not fitting any of the sections above that is relevant for understanding how the scenario might be affected by browser changes.

5.2. TODO Scenario Title

TODO Brief description of the scenario. This is the template source.

5.2.1. Summary

5.2.1.1. Contributor

* Name: TODO
* Organization: TODO
* Email: TODO

5.2.1.2. Protocol

* Name: TODO SAML|OIDC|OAUTH2|Other(specify)
* Grant/flow (if applicable): TODO eg. Implicit|Hybrid|AuthCode|SAMLArtifact|etc
* Reference: TODO aa https://linktospecandsection (https://linktospecandsection)

5.2.1.3. Browser Features Required

todo: delete all the ones that don't apply, add anything not listed - 1st party Cookie - 3rd party cookies - Redirect with link decoration - Form post - Local Storage - IFrames - JavaScript

5.2.1.3.1. Target Audience

todo: delete all the ones that don't apply, add anything not listed - B2C - B2E - B2B - G2C

5.2.1.4. Adoption

TODO Enumeration of products, industries, vendors that rely on this scenario as described.

5.2.2. Description Of The Flow

TODO long form description of the flow, including start state, end state, and sequence diagram when possible

5.2.3. Intended User Experience

TODO long form description of the intended user experience, with particular attention on the desired outcomes (eg no visible prompt in SSO scenarios)

5.2.4. Privacy Considerations

TODO long form description of privacy characteristics of the scenario, with particular attention to aspects affecting the browser (eg presence of browser-readable artifacts carrying user info, use of global|pairwise|no identifiers, etc).

5.2.5. Miscellaneous

TODO anything not fitting any of the sections above that is relevant for understanding how the scenario might be affected by browser changes.

6. Acknowledgements

7. IANA Considerations

This draft includes no request to IANA.

8. Security Considerations

This document has no security considerations. Readers should refer to the security considerations of the specifications references by each of the individual use cases.

9. Informative References

[RFC2119] Bradner, S., "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>.

[RFC8174] Leiba, B., "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>.

Authors' Addresses

Vittorio Bertocci
auth0.com

Email: vittorio@auth0.com

George Fletcher
Verizon Media

Email: gffletch@aol.com