Web Authentication Working Group Charter

The mission of the [Web Authentication Working Group](https://www.w3.org/Webauthn/), in the Security Activity is to define a client-side API providing strong authentication functionality to Web Applications.

[Join the Web Authentication Working Group.](https://www.w3.org/2004/01/pp-impl/87227/join)

|  |  |
| --- | --- |
| **Start date** | 4/15/2021 |
| **End date** | 31 December 2022 |
| **Confidentiality** | Proceedings are [public](https://www.w3.org/2015/Process-20150901/#confidentiality-levels) |
| **Charter extension** | See [Change History](https://www.w3.org/2019/10/webauthn-wg-charter.html#history). |
| **Chairs** | John Fontana, YubicoAnthony Nadalin, W3C Invited Expert |
| **Team Contacts** | Wendy Seltzer (0.05 FTE) |
| **Meeting Schedule** | **Teleconferences:** 1-hour calls will be held weekly.**Face-to-face:** We will meet during the W3C's annual Technical Plenary week; additional face-to-face meetings may be scheduled by consent of the participants, no more than 3 per year. |

Goals

The Web Authentication Working Group will develop recommendation-track specifications defining an API, as well as signature and attestation formats which provide an asymmetric and symmetric cryptography-based foundation for authentication of users to Web Applications.

Overall goals include obviating the use of shared secrets, i.e. passwords, as authentication credentials, facilitating multi-factor authentication support as well as hardware-based key storage while respecting the Same Origin Policy (SOP) by default and allowing for explicit, constrained SOP relaxation.

Scope

The Working Group will determine use cases that the API needs to support and use these to derive requirements. Success will be determined by the implementation of API features as defined in this section of the charter.

API Features in scope are: (1) Requesting generation of multiple asymmetric key pair within a specific scope (e.g., an origin) with crypto agility and crypto parameter selection; (2) Proving that the browser has possession of a specific private key, where the proof can only be done within the scope of the key pair. In other words, authentication should obey the same origin policy; (3) Remote desktop (lights out operations) ability; (4) Ability to allow a modal UI; (5) Binding of ambient credentials; (6) Re-authentication from the discretion of the replying party; (6) Dynamic Linking of authentication credentials.

Dependencies may exist on the [Credential Management API](http://www.w3.org/TR/credential-management-1/) in the [W3C Web Application Security Working Group](https://www.w3.org/2011/webappsec/) along with the [Client To Authenticator Protocol specification](https://fidoalliance.org/specs/fido-v2.0-rd-20161004/fido-client-to-authenticator-protocol-v2.0-rd-20161004.html) in FIDO.

Note that the details of any user experience (such as prompts) will not be normatively specified, although they may be informatively specified for certain function calls.

The Web Authentication Working Group should aim to produce specifications that have wide deployment and should adopt, refine and when needed, extend, existing practices and community-driven draft specifications when possible. The APIs should integrate well with Web Applications and so should be developed in concert with Web Application developers and reviewed by the [Web Application Security](https://www.w3.org/2011/webappsec/) and [Web Applications](https://www.w3.org/WebPlatform/WG/) Working Groups.

Comprehensive test suites should be developed for the specification to ensure interoperability. User-centric privacy considerations of device management and credentials should be taken into account. The Working Group may produce protocol standards as needed by the API.

Out of Scope

Out of scope: federated identity, multi-origin credentials, low-level access to cryptographic operations or key material.

Success Criteria

In order to advance to [Proposed Recommendation](https://www.w3.org/Consortium/Process/#rec-pr), each specification is expected to have at least two independent implementations of each feature defined in the specification. The extensions listed in the specification are tested at extension framework level for correctness, the functionality of each extension is tested independently.

Deliverables

Normative Specifications

The working group will deliver at least the following:

Web Authentication API Level

This specification makes secure authentication available to Web application developers via a standardized API. This new version will incorporate errata of Level 1 Specification and any additional authenticator selection criteria use cases.

**[Web Authentication:An API for accessing Public Key Credentials Level 3](https://www.w3.org/TR/webauthn-2/)
Latest publication:**

Draft State: Working Draft TBD

Expected Completion: 2Q 2022

Adopted Draft: TBD [First Public Working Draft](https://www.w3.org/TR/2019/WD-webauthn-2-20190604/)

Reference Draft: TBD [First Public Working Draft](https://www.w3.org/TR/2019/WD-webauthn-2-20190604/)

The specifications must contain sections detailing any known security and privacy implications for implementers, Web authors, and end users. The Web Authentication WG will actively seek open security and privacy reviews.

The specifications should take advantage of existing platform and operating-system authentication libraries as appropriate.

More detailed milestones and updated publication schedules will be available on the [group publication status page](https://www.w3.org/Webauthn/pubstatus.html).

Other Deliverables

The working group will produce a test suite and implementation report for its specification(s).

Other non-normative documents may be created such as:

* Use case and requirement documents, including use cases as needed to inform user requirements across horizontal areas,
* Primer or Best Practice documents to support web developers, and
* Protocol design overview documents or flow diagrams.

Coordination

For all specifications, this Working Group will seek [horizontal review](https://www.w3.org/Guide/Charter.html#horizontal-review) for accessibility, internationalization, performance, privacy, and security with the relevant Working or Interest Groups, and with the [TAG](https://www.w3.org/2001/tag/). Invitation for review will be issued during each major standards-track document transition, including [FPWD](https://www.w3.org/Consortium/Process/#first-wd) and [CR](https://www.w3.org/Consortium/Process/#last-call), and should be issued when major changes occur in a specification.

This API should work with a wide variety of authenticators and should not require non-standardized vendor-specific infrastructure. We will establish liaisons with the other standards bodies working on particular authenticators as needed.

Additional technical coordination with the following Working Groups will be made, per the [W3C Process Document](https://www.w3.org/Consortium/Process/#WGCharter):

W3C Groups

[Web Application Security Working Group](https://www.w3.org/2011/webappsec/)

Coordination with Credential Management API and application security.

[Web Applications Working Group](https://www.w3.org/2019/webapps/)

Coordination on API design.

[Web Payments Working Group](https://www.w3.org/Payments/WG/)

To liaison over issues related to strong authentication for payments and tokenization.

[Web Payments Security Interest Group](https://www.w3.org/securepay/)

To liaison over issues related to strong authentication for payments and tokenization with FIDO, W3C and EMVCo.

[Privacy Interest Group](https://www.w3.org/Privacy/)

Coordination on privacy implications.

[Accessible Platform Architectures (APA) Working Group](https://www.w3.org/WAI/APA/)

Coordination to review accessibility requirements for APIs and for any direct user interfaces that may be specified.

[Decentralized Identifier Working Group](https://www.w3.org/2019/did-wg/)

To liaison over issues related to strong authentication and proof of ownership of decentralized identifiers.

External Organizations

[IETF Security Area Directorate](https://datatracker.ietf.org/group/secdir/about/)

The IETF Security Area Directorate consists of the Working Group Chairs of the Security Area and selected individuals chosen for their technical knowledge in security.

FIDO 2.0 Working Group

Coordination on [Client to Authenticator Protocol](https://fidoalliance.org/specs/fido-v2.0-rd-20161004/fido-client-to-authenticator-protocol-v2.0-rd-20161004.html).

Participation

To be successful, this Working Group is expected to have 6 or more active participants for its duration, including representatives from key implementors of this specification, and active Editors and Test Leads for each specification. The Chairs, specification Editors, and Test Leads are expected to contribute half of a day per week towards the Working Group. There is no minimum requirement for other Participants.

The group encourages questions, comments and issues on its public mailing lists and document repositories, as described in [Communication](https://www.w3.org/2019/10/webauthn-wg-charter.html#communication).

The group also welcomes non-Members to contribute technical submissions for consideration, with the agreement from each participant to Royalty-Free licensing of those submissions under the W3C Patent Policy.

Communication

Technical discussions for this Working Group are conducted in [public](https://www.w3.org/Consortium/Process/#confidentiality-levels). Meeting minutes from teleconference and face-to-face meetings will be archived for public review, and technical discussions and issue tracking will be conducted in a manner that can be both read and written to by the general public. Working Drafts and Editor's Drafts of specifications will be developed on a public repository, and may permit direct public contribution requests.

Information about the group (including details about deliverables, issues, actions, status, participants, and meetings) will be available from the [Web Authentication Working Group home page.](https://www.w3.org/Webauthn)

Most Web Authentication Working Group teleconferences will focus on discussion of particular specifications, and will be conducted on an as-needed basis.

This group primarily conducts its technical work through a [GitHub repository](https://github.com/w3c/webauthn) and on the public mailing list public-webauthn@w3.org ([archive](https://lists.w3.org/Archives/Public/public-webauthn/)). The public is invited to raise issues on GitHub.

The group may use a Member-confidential mailing list for administrative purposes and, at the discretion of the Chairs and members of the group, for member-only discussions in special cases when a participant requests such a discussion.

Decision Policy

This group will seek to make decisions through consensus and due process, per the [W3C Process Document (section 3.3](https://www.w3.org/2015/Process-20150901/#def-Consensus)). Typically, an editor or other participant makes an initial proposal, which is then refined in discussion with members of the group and other reviewers, and consensus emerges with little formal voting being required.

However, if a decision is necessary for timely progress, but consensus is not achieved after careful consideration of the range of views presented, the Chairs may call for a group vote, and record a decision along with any objections.

To afford asynchronous decisions and organizational deliberation, any resolution (including publication decisions) taken in a face-to-face meeting or teleconference will be considered provisional. A call for consensus (CfC) will be issued for all resolutions (for example, via email and/or web-based survey), with a response period from one week to 10 working days, depending on the chair's evaluation of the group consensus on the issue. If no objections are raised on the mailing list by the end of the response period, the resolution will be considered to have consensus as a resolution of the Working Group.

All decisions made by the group should be considered resolved unless and until new information becomes available, or unless reopened at the discretion of the Chairs or the Director.

This charter is written in accordance with the [W3C Process Document (Section 3.4, Votes)](https://www.w3.org/Consortium/Process/#Votes).

Patent Policy

To promote the widest adoption of Web standards, W3C Recommendations have a Royalty-Free IP commitment from Working Group participants under the [W3C Patent Policy](https://www.w3.org/Consortium/Patent-Policy/). The [W3C Patent Policy Implementation](https://www.w3.org/2004/01/pp-impl/) details the disclosure obligations for this group.

Licensing

This Working Group will use the [W3C Document License](https://www.w3.org/Consortium/Legal/copyright-documents) for all its deliverables.

About this Charter

This charter has been created according to [section 5](https://www.w3.org/Consortium/Process/#GAGeneral) of the [Process Document](https://www.w3.org/Consortium/Process). In the event of a conflict between this document or the provisions of any charter and the W3C Process, the W3C Process shall take precedence.

Charter History

The following table lists details of all changes from the initial charter, per the [W3C Process Document (section 5.2.3)](https://www.w3.org/2015/Process-20150901/#CharterReview):