DRAFT Charter:
WebBotAuthN Working Group

Non-browser clients (colloquially, 'bots') are increasingly used on the Web. These clients need to reliably authenticate themselves to origins (Web servers) for several reasons:

1. Regulatory compliance may require transparency of automated systems
2. Origins wish to manage their resources and access control
3. Both bots and origins seek protection against impersonation and reputation management
4. Origins may wish to differentiate service levels between automated and non-automated traffic

Current solutions (such as IP allowlisting, User-Agent strings, and shared API keys) have significant limitations regarding security, scalability, and manageability.

The Web Bot Authentication (webbotauthn) Working Group will standardise methods for cryptographically authenticating non-browser clients and providing additional information about their operators to Web sites. Its products are intended for use by sites that primarily serve browsers.

Scope

In-scope use cases include cryptographically authenticating access to Web sites for:

- Crawlers for search indices
- Web archivers
- Tools such as link checkers and validators
- Crawlers for AI training
- AI agents retrieving or interacting with content on behalf of end users, without addressing identification of a specific end user

The following use cases are out of scope for this work:

- Authenticating access to content not intended for browser clients (e.g., HTTP APIs, agent-to-agent interfaces)
- Authenticating the end user of a non-browser client or agent
- Authentication for application protocols other than HTTP
- Non-cryptographic authentication
- Defining a vocabulary for the intents of bots
- Sharing or otherwise conveying reputation of bots or other information between servers or with third parties
- Techniques for distinguishing bot from non-bot clients

In particular, there is significant activity around so-called agentic use cases where a non-browser client might make requests on the end users' behalf. This effort will focus initially on authentication of the agent. Authentication of the end user is out-of-scope for now.

Deliverables

The Working Group will deliver:

- Standards track document(s) describing technique(s) for authenticating non-browser clients to Web sites intended for browsers.
- A way for web servers to learn more information about the bot, including an association with an existing widely-used identifier (such as a domain name, hostname, or URL). This might include a small set of initial terms.
- Best current practice and/or Informational document(s) describing operational considerations such as lifecycle management, key management, deployment considerations, etc. It will also address impacts on the openness of the web.

Particular attention should be paid to barriers to new bot clients and sites that might be created by this work. The architecture created should not introduce any new 'choke points' around the identity of non-browser clients.

Input documents that the Working Group might consider for adoption include:

- draft-meunier-web-bot-auth-architecture
- draft-meunier-http-message-signatures-directory

Liaison

The Working Group is expected to liaise with the AIPREF, HTTPBIS, OAUTH, TLS, and WIMSE Working Groups as appropriate on any relevant documents.

Milestones

- April 2026 - Standards track specification(s) describing authentication technique(s) and a means for conveying additional information about bots sent to the IESG
- August 2026 - Best Current Practice specification sent to the IESG