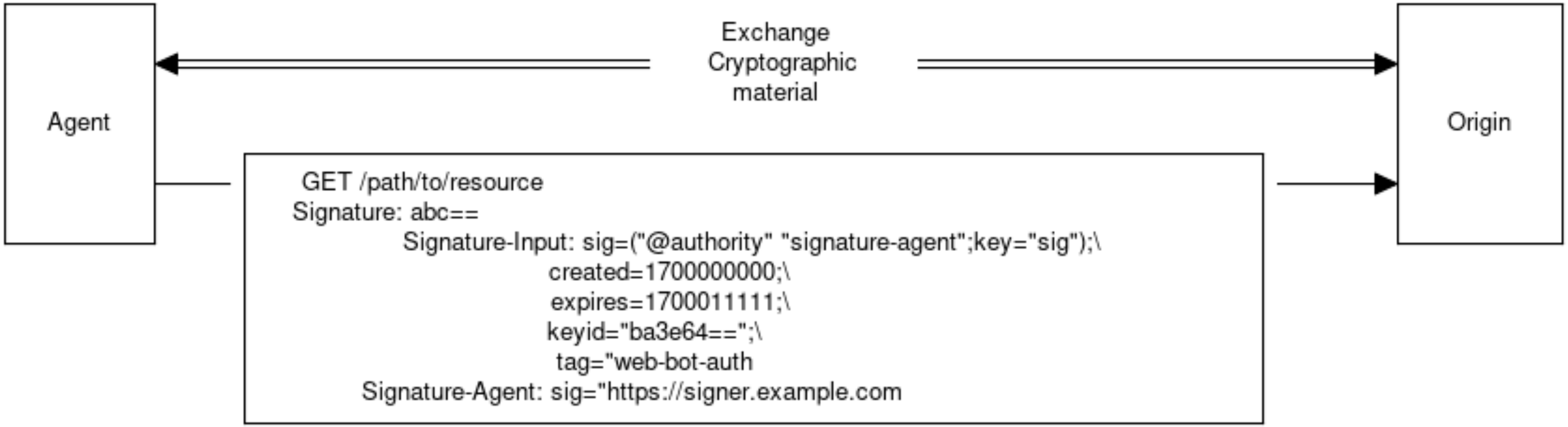
HTTP Message Signatures for automated traffic

`draft-meunier-web-bot-auth-architecture-04`

Sandor Major (Google) - Thibault Meunier (Cloudflare)

IETF 124, November 2025, Montreal

High level

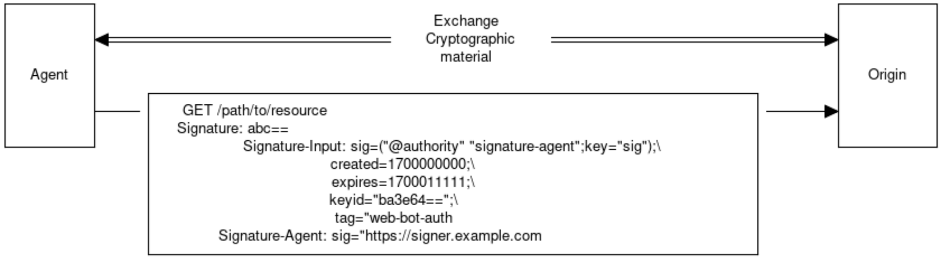


draft-meunier-web-bot-auth-architecture-04

Description

Using HTTP Message Signatures as defined in RFC 9421 for authenticating non-browser clients to Web sites intended for browsers

Uses Signature-Agent for discovery
Accept-Signature to request more parameters
Nonce for anti-replay

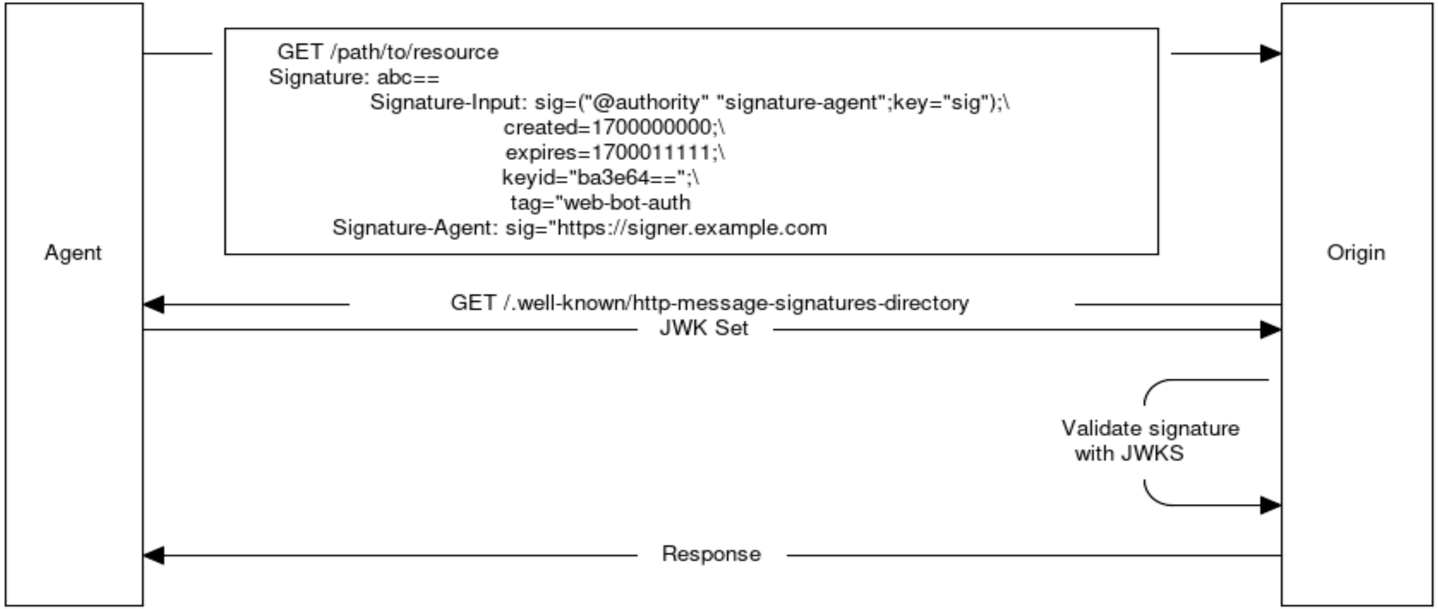


draft-meunier-web-bot-auth-architecture-04

Specification overview

draft-meunier-web-bot-auth-architecture-04

On-path discovery



draft-meunier-web-bot-auth-architecture-04

Implementations

Multiple public implementations

1. Go
2. TypeScript
3. Rust
4. Python
5. Ruby

Interop

Basic test vectors so far

1. Do we need more?
2. Greasing

draft-meunier-web-bot-auth-architecture-04

Open questions

22 open issues on GitHub (possibly to be moved)

1. Optimisation: how much is needed
   a. Performance numbers
   b. Replay
   c. On-demand signing
2. Session binding (TLS, cookies, others)
3. kid and keyid
4. Best practice document

Should the working group adopt the document?

draft-meunier-web-bot-auth-architecture-04