

Automatic authentication keys

Problem: Every website needs you to create an account. This is a pain to manage, and a barrier. This is especially problematic for self-hosted things like Forgejo, because it gives centralized platforms an advantage (everyone already has an account there). It should be trivial to immediately start using a site without going through a registration process.

Other solutions: OIDC, OpenID and such all require you to have an account with a provider. You fully trust this provider with your access, or you need to self-host it which is extra work. Passkeys are extremely Google-shaped and dubiously designed and documented. Federation is a massively complex solution to design for, and really an unnecessary complexity expense for the vast majority of self-hosted cases.

Proposed solution: Authentication directly integrated into browser through a browser extension. It uses request interception APIs and such to detect "is supported" headers from websites, and inject authentication headers into requests upon confirmation from the user that they wish to authenticate (it should not disclose its existence before that point). Authentication is done through keys managed locally by the browser and optionally stored encrypted on a third-party server.

Unsolved issues: Key management and backup, making it robust. Offer to backup to a USB key? How to deal with Manifest v3 in Chrome?

Revision #2

Created 11 December 2024 00:06:54 by joepie91

Updated 11 December 2024 15:56:33 by joepie91