Accessible Authentication

What is it for?

When people can't use a login page, the harm can be serious. It can take away their right to privacy, security, and independence.

Logins should not rely on hard memory tests or puzzles, as these block users with cognitive needs. Forcing people to pass these checks often locks them out of vital services.

Logins designed with accessibility in mind are safer and easier to use for everyone.

How to support it

To make login pages accessible, developers should follow these steps:

- Don't rely solely on puzzles or memory tests. Always provide an alternative method.
- Support password managers and allow users to paste text. This improves both accessibility and security.
- Never disable autofill by setting autocomplete to 'off'. Forcing people to type complex details causes unnecessary difficulty.
- Offer flexible alternatives like biometrics, one-time codes, and magic links.

Useful links

- Understanding SC 3.3.8: Accessible Authentication (Minimum), from the World Wide Web Consortium (W3C)
- Accessibility in Cybersecurity: A Practical Guide
- The autocomplete attribute and web security (Mozilla Developer Network)