

Shibboleth WebAuthnAuthentication plugin

Paul Scott

SWAMID operations

Sunetdagarna våren 2025

Shibboleth WebAuthnAuthentication plugin

- Ny plugin som stödjer Web Authentication API (WebAuthn) som en del av FIDO2-standarden, vilket möjliggör FIDO2-autentisering
- Detta möjliggör stark autentisering av användarna med hjälp av offentliga nycklar
 - med andra ord – passkeys!
- Första version (1.0.0) släpptes i december 2024
- Version 1.1.0 släpptes i mars 2025 efter testning och feedback från SWAMID operations
- Senaste version är 1.2.0.

Autentisering på flera sätt

- som en singelfaktor inom en bredare MFA-lösning
- som en ensam-faktor där användarnamnet anges av användaren (passwordless)
- som en ensam-faktor där användarnamnet inte anges av användaren men istället identifieras implicit från den valda FIDO2 credential (usernameless)

Features

- Administration flöde för användarna
 - så att en användare kan skapa och hantera sina egna credentials
- Management flöde för administratörer
 - så att en administratör kan hantera andras credentials
- Metadata
 - systemet stödjer läsning av metadata för authenticators från bl.a. FIDO alliance metadata service
- Credential registration policies
 - tillåter styrning av vilka typer av authenticators man vill tillåta (t.ex. endast hårdvara säkerhetsnycklar)

SWAMID testning

- Ett MFA authn flöde i second factor mode med lösenord först och sedan en FIDO2 credential (passkey på en Yubikey)
- Tillåter självregistrering av en credential med endast lösenord
- Kräver MFA (lösenord + credential) för att hantera registrerade credentials
- Kan fungera som en multifaktor på AL2-nivå

Video – WebAuthn demo (2 min)

- 00:00 - Användaren testemp1 skapar sin första credential (på en Yubikey) efter inloggning med sitt lösenord.
- 00:28 - Användaren testemp1 testar MFA-inloggning på release-check. Loggar in med lösenord + Yubikey.
- 01:10 - Användaren testemp1 hanterar sina credentials. Observera att användaren måste göra en MFA-inloggning eftersom en credential är redan registrerad.
- 01:27 – Admin-användare testemp3 (som redan har sin egen credential) loggar in i management-gränssnittet och tar bort den credential för användaren testemp1.



Please enter your username below.

KauID

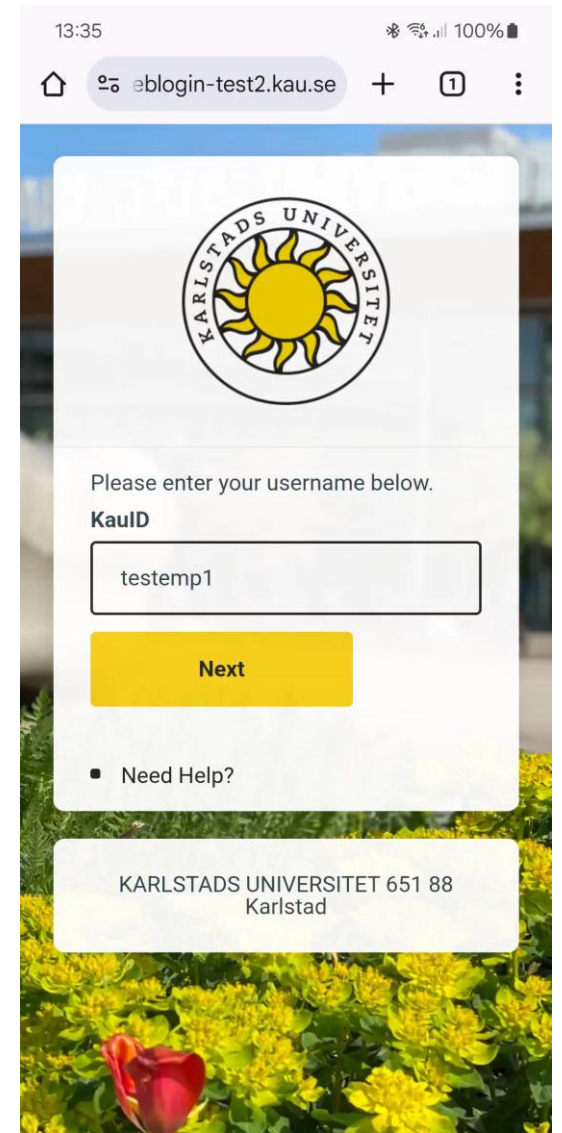
Next

▪ [Need Help?](#)

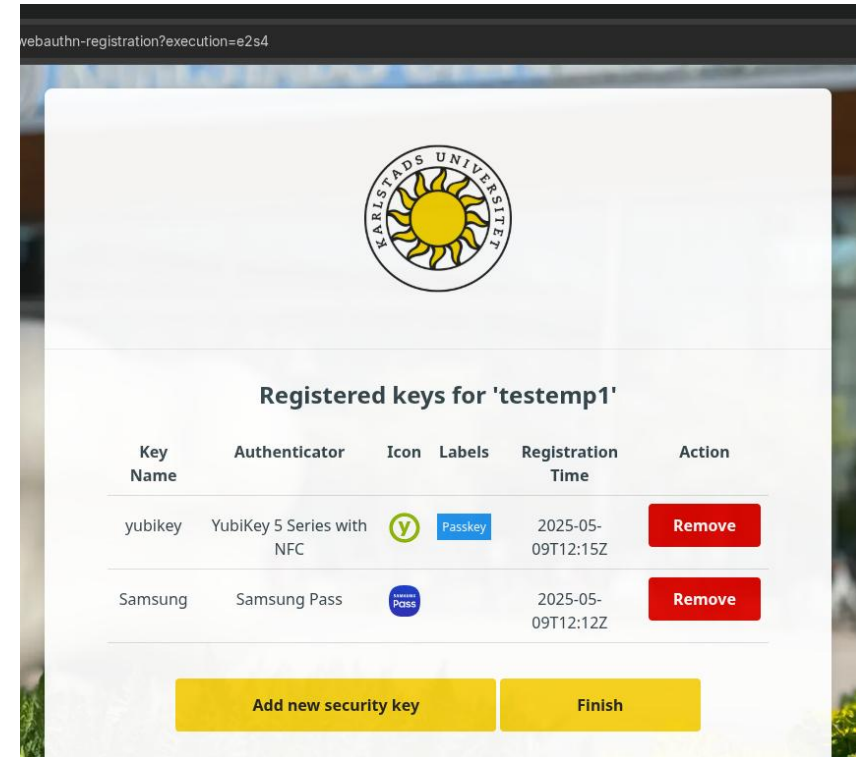
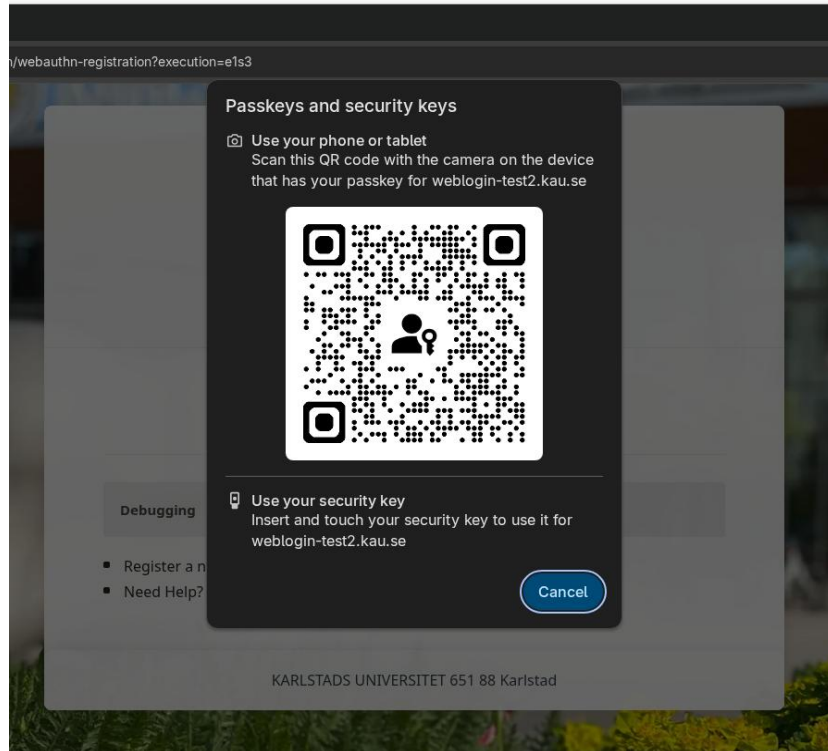
KARLSTADS UNIVERSITET 651 88 Karlstad

Stöd för andra enheter

- Stöd för andra enheter finns i plugin så det blir möjligt och smidigt att logga in oavsett vilken device man använder.
- I videon loggar testanvändaren in i management gränssnittet på sin mobil och använder en passkey som finns i mobilens säkerhetschip.



Stöd för andra enheter



- Rekommendationen är att göra mobilregistrering först, för att möjliggöra registrering på flera enheter senare.

Mer information

- Shibboleth wiki
 - <https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/3395125387/WebAuthn>
- Webinar...?
 - Kommer under hösten 2025