universität innsbruck

EduMFA Multifactor-Authentifizierung für Microsoft Entra ID

Gegründet im Jahr 1669, ist die Universität Innsbruck heute mit mehr als 28.000 Studierenden und über 5.000 Mitarbeitenden die größte und wichtigste Forschungs- und Bildungseinrichtung in Westösterreich.

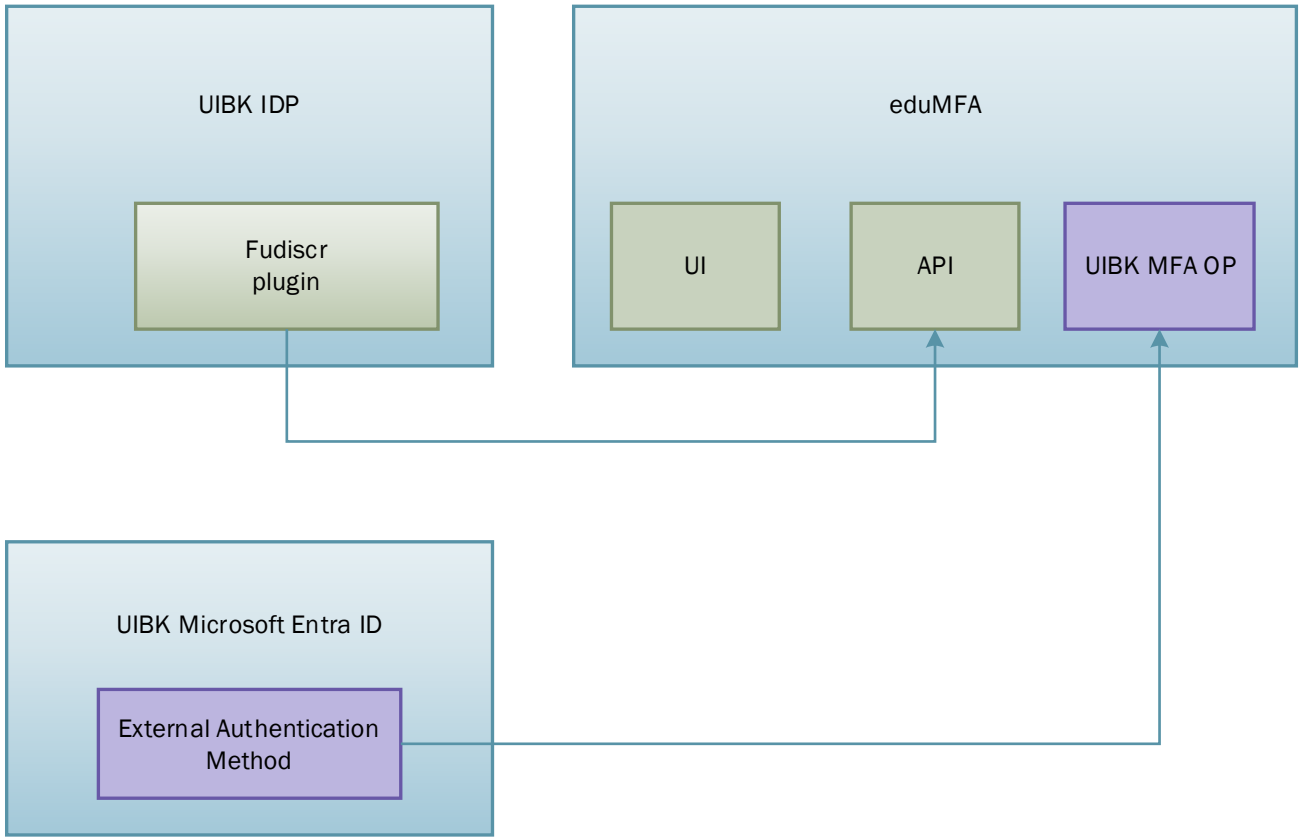
universität innsbruck

EduMFA Multifactor-Authentifizierung für Microsoft Entra ID

Martin Krenn – Zentraler Informatik Dienst
März 2026

This is an independent presentation and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

Unser Setup IDP, Microsoft 365, MFA

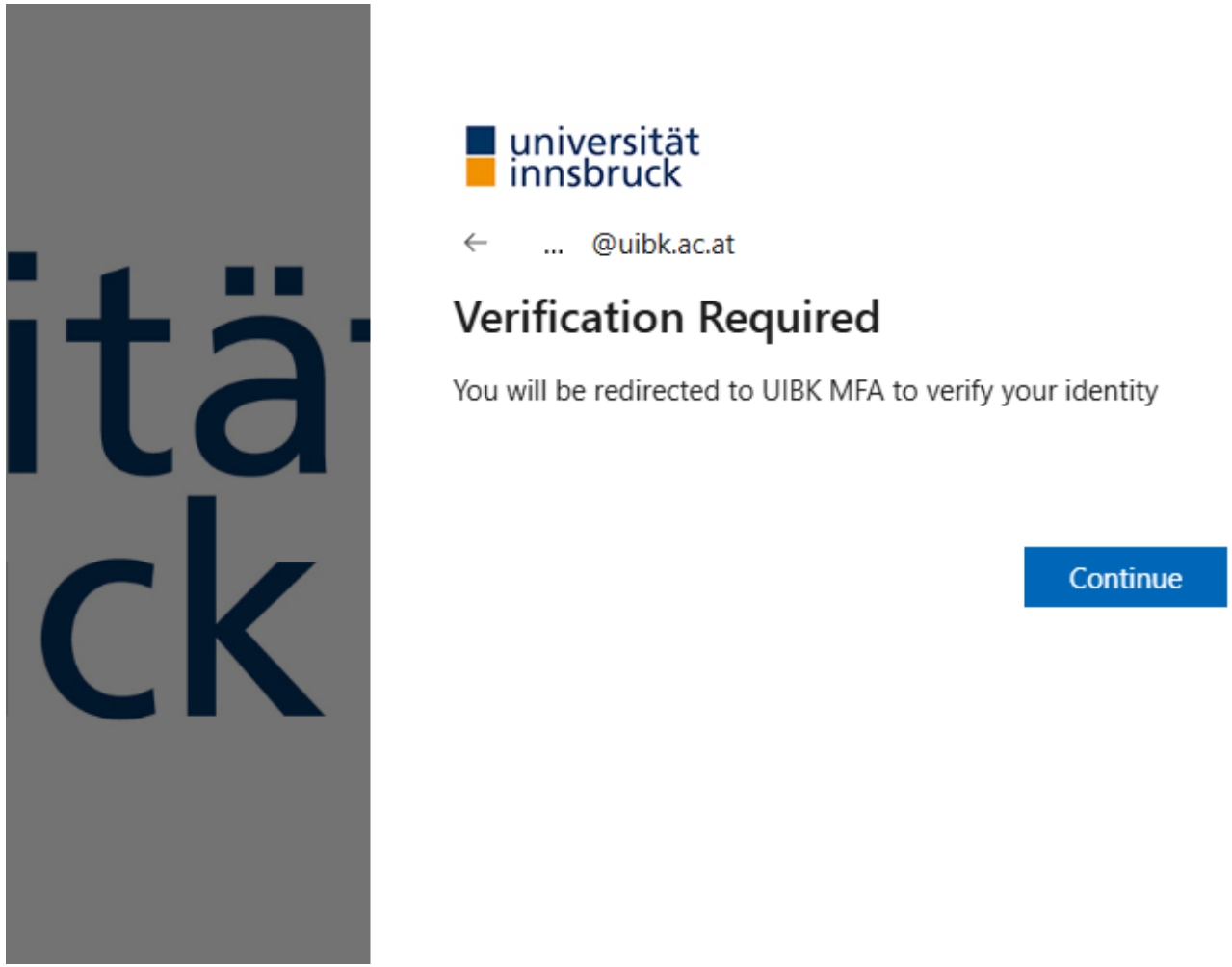


Demo

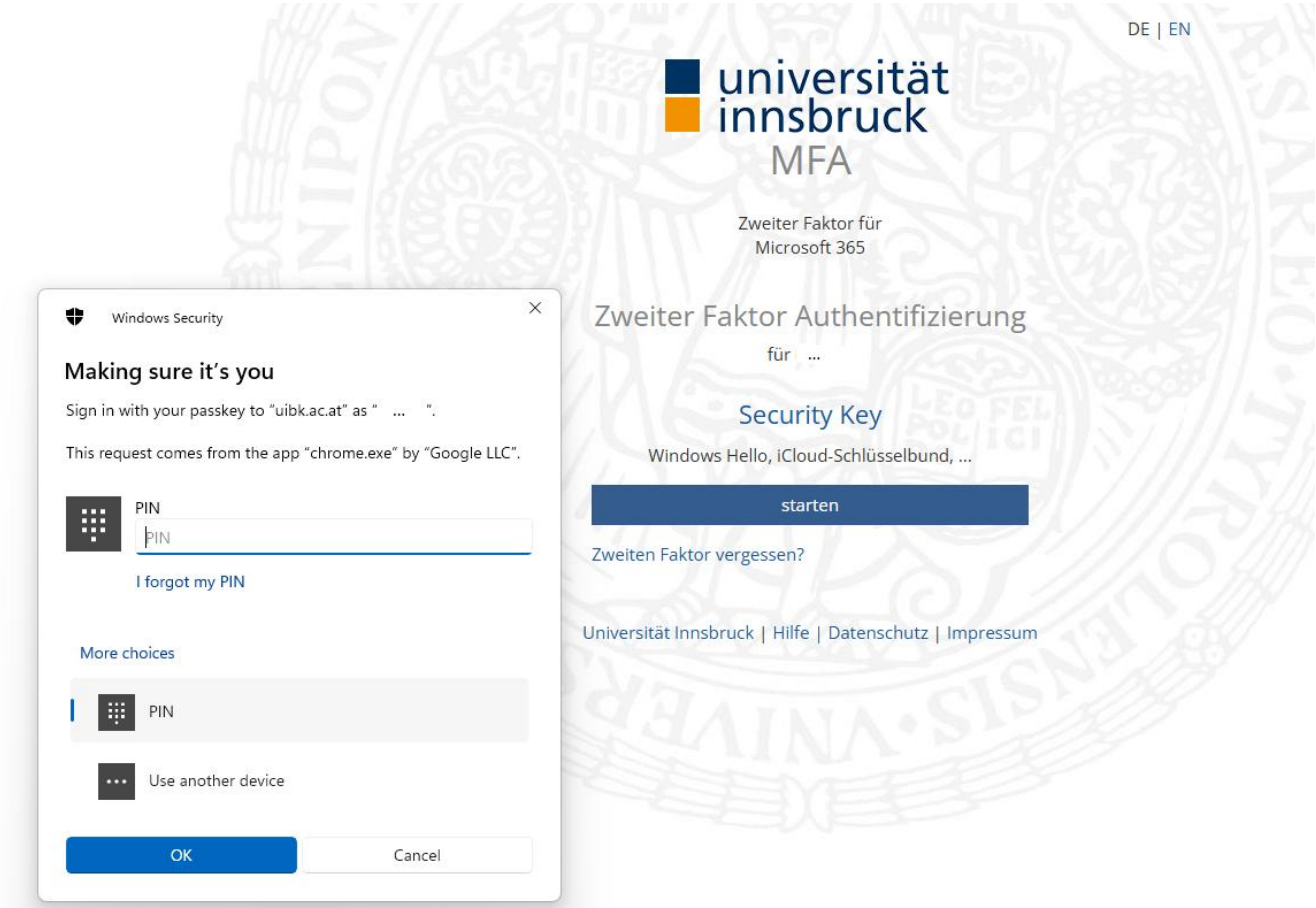

ersitä
bruck


universität
innsbruck
...
@uibk.ac.at
Enter password
Password
Sign in

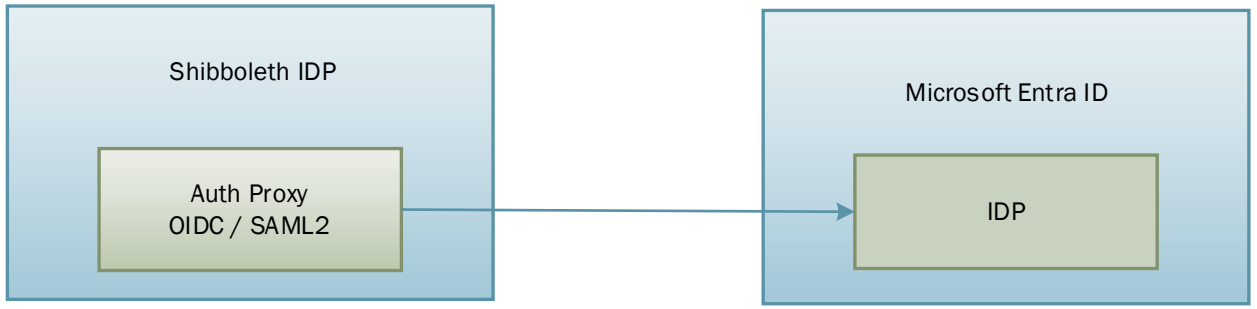
Demo


universität
innsbruck
... @uibk.ac.at
Verification Required
You will be redirected to UIBK MFA to verify your identity
Continue

Demo


DE | EN
universität innsbruck
MFA
Zweiter Faktor für Microsoft 365
Zweiter Faktor Authentifizierung
für ...
Security Key
Windows Hello, iCloud-Schlüsselbund, ...
starten
Zweiten Faktor vergessen?
Universität Innsbruck | Hilfe | Datenschutz | Impressum
Windows Security
Making sure it's you
Sign in with your passkey to "uibk.ac.at" as " ... ".
This request comes from the app "chrome.exe" by "Google LLC".
PIN
PIN
I forgot my PIN
More choices
PIN
Use another device
OK
Cancel

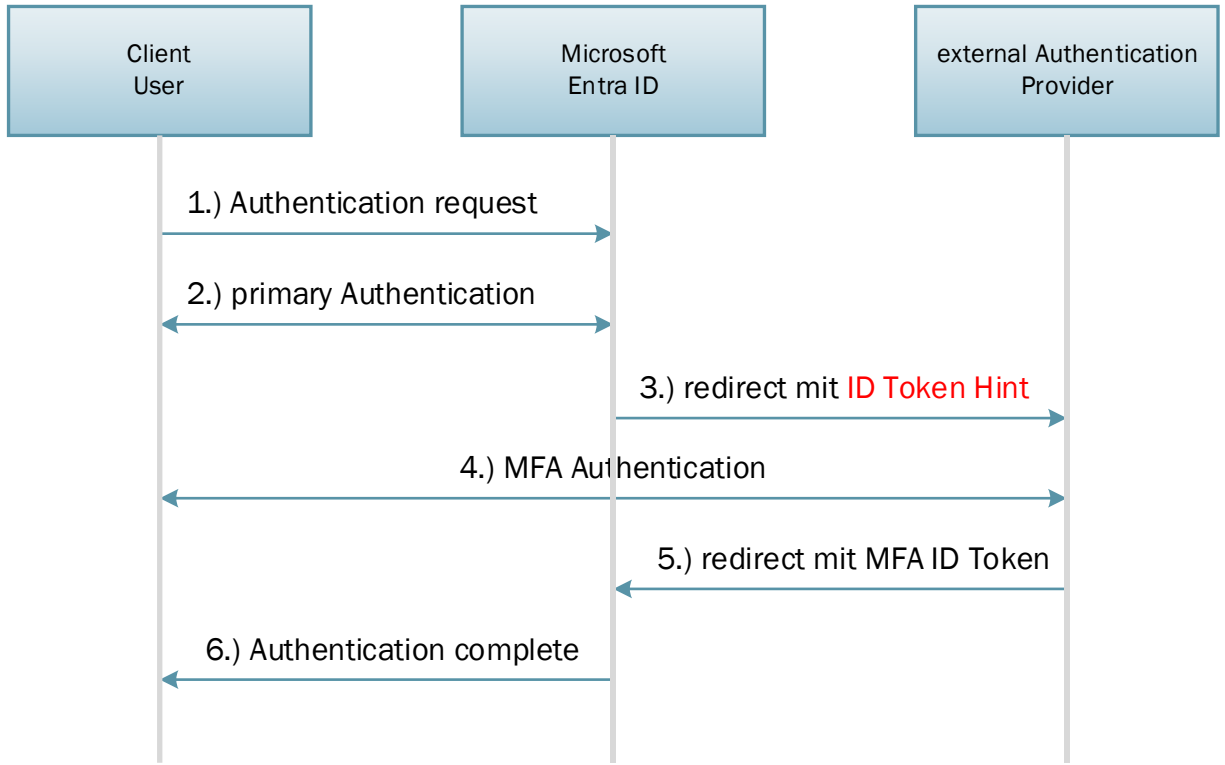
Die andere / übliche Lösung



Wie kamen wir zu unserer Lösung

- unseren Shibboleth IDP betreiben wir schon lange
- Minimales Microsoft 365 (Authentifizierung delegiert mit SAML2 über unseren IDP)
- Einführung MFA für unseren IDP (Frühjahr 2024)
- Start größerer Rolle für Microsoft 365 (Sommer 2025)
  - Problemstellung MFA
  - Microsoft ADFS als Lösung ausgeschlossen
  - Investigation External Authentication Method
  - Implementierung unserer Lösung
- Einführung Microsoft 365 (Herbst 2025)

Microsoft Entra ID – External Authentication Method (OpenID Connect implicit flow)



id_token_hint


```
{
  "aud": "f4592ed6-3930-4d64-...",
  "iss": "https://login.microsoftonline.com/5783bdad-f801-.../v2.0",
  "iat": 1773687840,
  "nbf": 1773687840,
  "exp": 1773688740,
  "name": "Krenn, Martin",
  "oid": "e7f07b71-9255-4185-.....",
  "preferred_username": "....@uibk.ac.at",
  "sub": "qNNT4FdnQpcNM4ud….",
  "tid": "5783bdad-f801-…",
  "upn": "...@uibk.ac.at",
  "uti": "-fy5ZlG_2E6idIjDSaB4AA",
  "ver": "2.0"
}
```

Shibboleth als Microsoft Entra ID external MFA provider

- Shibboleth IDP ist mit Hilfe von offiziellen Plugins OpenID Provider.
- id_token_hint: gibt es im OpenID Connect Standard. Wird allerdings anders verwendet.
- Der id_token_hint enthält einen ID Token, der vom Entra ID OP des Tenants augestellt ist. Als Audience ist eine „Proxy RP“ hinterlegt.
- Wir benötigen einen Authenticator für den ID Token im id_token_hint Parameter.
- Wir müssen aus dem ID Token einen Benutzer auflösen, der bei EduMFA verwendet werden kann.
- Ein paar Besonderheiten. (x5 jwk parameter, amr claims)
- Shibboleth IDP ≠ Shibboleth MFA OP

IdTokenHint Authentication Plugin

https://idp2.uibk.ac.at/shibplugin/authn/idtokenhint/

Mögliche Probleme und Besonderheiten

- Interne Browser von Microsoft Applikationen können sehr sensibel bei Javascript sein.
  Debug Möglichkeiten sind oft sehr eingeschränkt (keine Development Tools, Alert geht nicht,..).
- HTTP Sicherheitsfeatures mittels Content-Security-Policy zur sichereren Verwendung von Javascript können Probleme machen.
- White Screens / kein Javascript bei z.B. Webauthn Authentifizierung
- Webauthn Parameter client hints können die Funktionalität in Microsoft Apps brechen
  (Danke Florian Ritterhoff)

Ausblick

- Microsoft Entra ID – external authentication method ist nun ein offizielles feature und kein preview feature mehr (seit Feb. 2026)
- Plugin Ausblick:
  - Update in den nächsten Wochen
  - Shibboleth 5.2 Kompatibilität
  - Graph API Lookup zum Erhalt eines Benutzers, der von eduMFA verwendet werden kann. (OnPremisesSamaccountName,…)
  - Interessierte Parteien / early adopters

Weitere Informationen

- Manage an external multifactor authentication method in Microsoft Entra ID
- Use Microsoft Entra MFA with an external MFA provider

- https://edumfa.io/
- IdP-Authn-Plugin fudiscr
- IdTokenHint Authn plugin

- Shibboleth OIDC OP plugin

Danke!

Martin Krenn – martin.krenn@uibk.ac.at