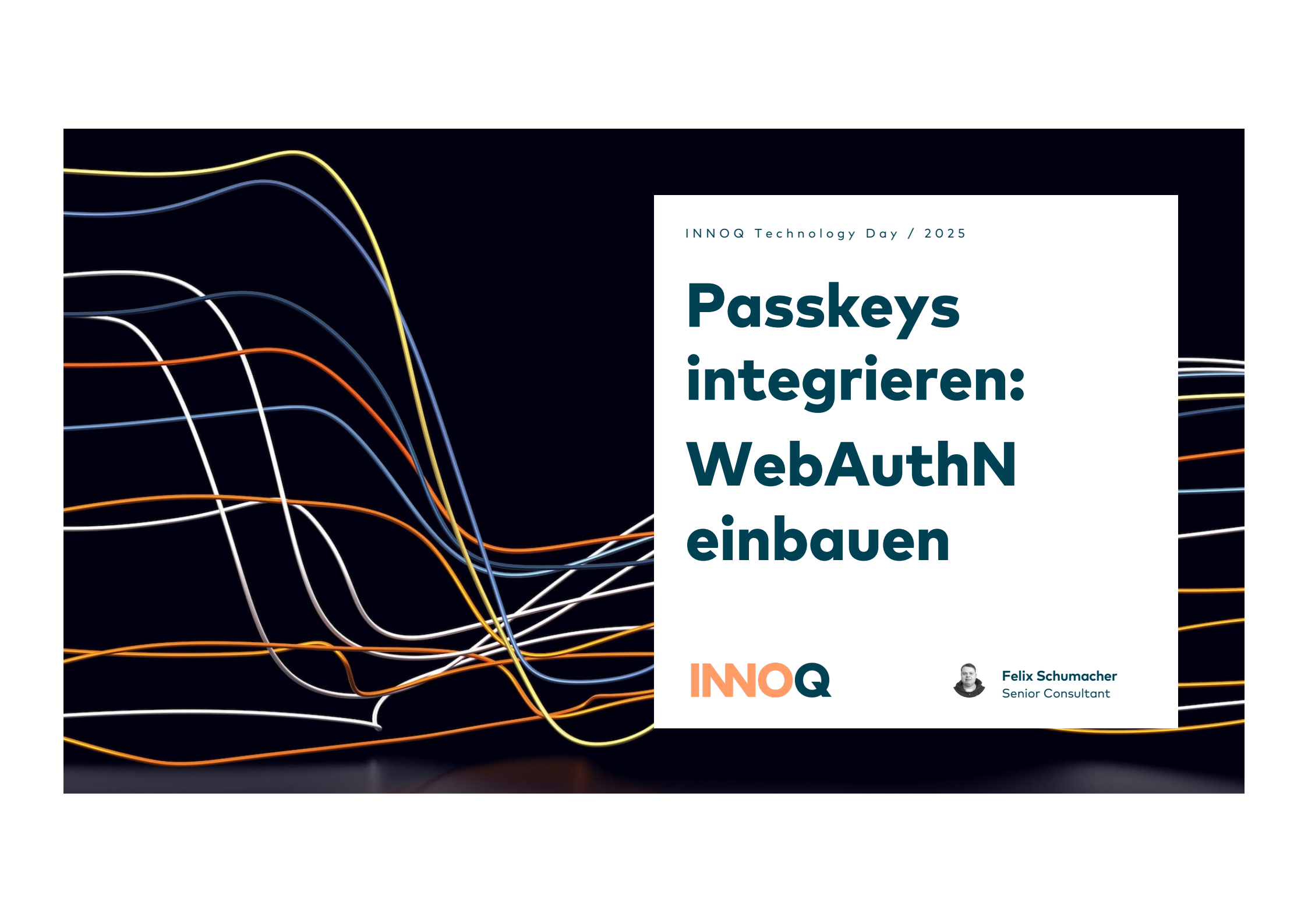




INNOQ Technology Day / 2025

Passkeys integrieren: WebAuthN einbauen

INNOQ



Felix Schumacher
Senior Consultant

Die Gegenwart...

Login mit Username und Passwort

Login

E-Mail

Passwort

[Einloggen](#)

Noch kein Konto? [Jetzt registrieren](#)

[← Zurück zum Shop](#)

Problem Phishing...

```
set>sudo setoolkit
[---] The Social-Engine Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLIX) [---]
      Version: 8.0.3
      Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engine Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engine Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Can't pickle local object <function show_banner.<locals>.pull_version at 0x103b5a610>
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engine Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engine Toolkit

set>
```

Was sind Passkeys?

In a nutshell...

- WebAuthN (W3C API
<https://www.w3.org/groups/wg/webauthn/>)
- Public-Key Verfahren zur Authentifizierung
- Rechner erzeugt Schlüsselpaar, Public-Key geht an Website statt Passwort
- Domain ist Teil des Schlüssels (verhindert Phishing unter Domain mit "0 statt o" etc.)

Also los...

Passkeys...

- <https://passkeys.dev/docs/tools-libraries/libraries/>
- SimpleWebAuthn (<https://simplewebauthn.dev/docs/>) – JS
- <https://github.com/Yubico/java-webauthn-server> (Java)
- Auch libraries für .NET, go, python, ruby...
- Awesome-Page: <https://github.com/yackermann/awesome-webauthn>



Passkeys...

- Java, Spring Boot, Passkeys – Suche
- <https://docs.spring.io/spring-security/reference/servlet/authentication/passkeys.html>
- <https://www.baeldung.com/spring-security-integrate-passkeys>
- Es gibt also schon was...

Die KI losschicken...

- Codex ein Repo gegeben
- Eine Beispiel App mit Password-Auth und DB
- Erster Versuch – will <https://github.com/Yubico/java-webauthn-server> nutzen, compiled aber nach viel hin und her nicht...
- Zweiter Versuch – mit Bitte, Spring-Mittel zu nutzen – hat versucht die Spec komplett ohne lib zu implementieren, compiled, funktioniert aber nicht...

Selber loslegen

 **spring** initializr

Project
☐ Gradle - Groovy ☐ Gradle - Kotlin ☒ **Java** ☐ Kotlin ☐ Groovy
☒ **Maven**

Language
☒ **Java** ☐ Kotlin ☐ Groovy

Spring Boot
☒ **4.0.0 (SNAPSHOT)** ☐ 4.0.0 (RC2) ☐ 3.5.8 (SNAPSHOT) ☐ 3.5.7
☐ 3.4.12 (SNAPSHOT) ☐ 3.4.11

Project Metadata

Group

com.example

Artifact

demo

Name

demo

Description

Demo project for Spring Boot

Package name

com.example.demo

Packaging

☒ **Jar** ☐ War

Configuration

☒ **Properties** ☐ YAML

Java

☐ 25 ☐ 21 ☒ **17**

Dependencies ADD DEPENDENCIES... % + B

Spring Web **WEB**
Build web, including RESTful, applications using Spring MVC. Uses Apache Tomcat as the default embedded container.

Spring Security **SECURITY**
Highly customizable authentication and access-control framework for Spring applications.

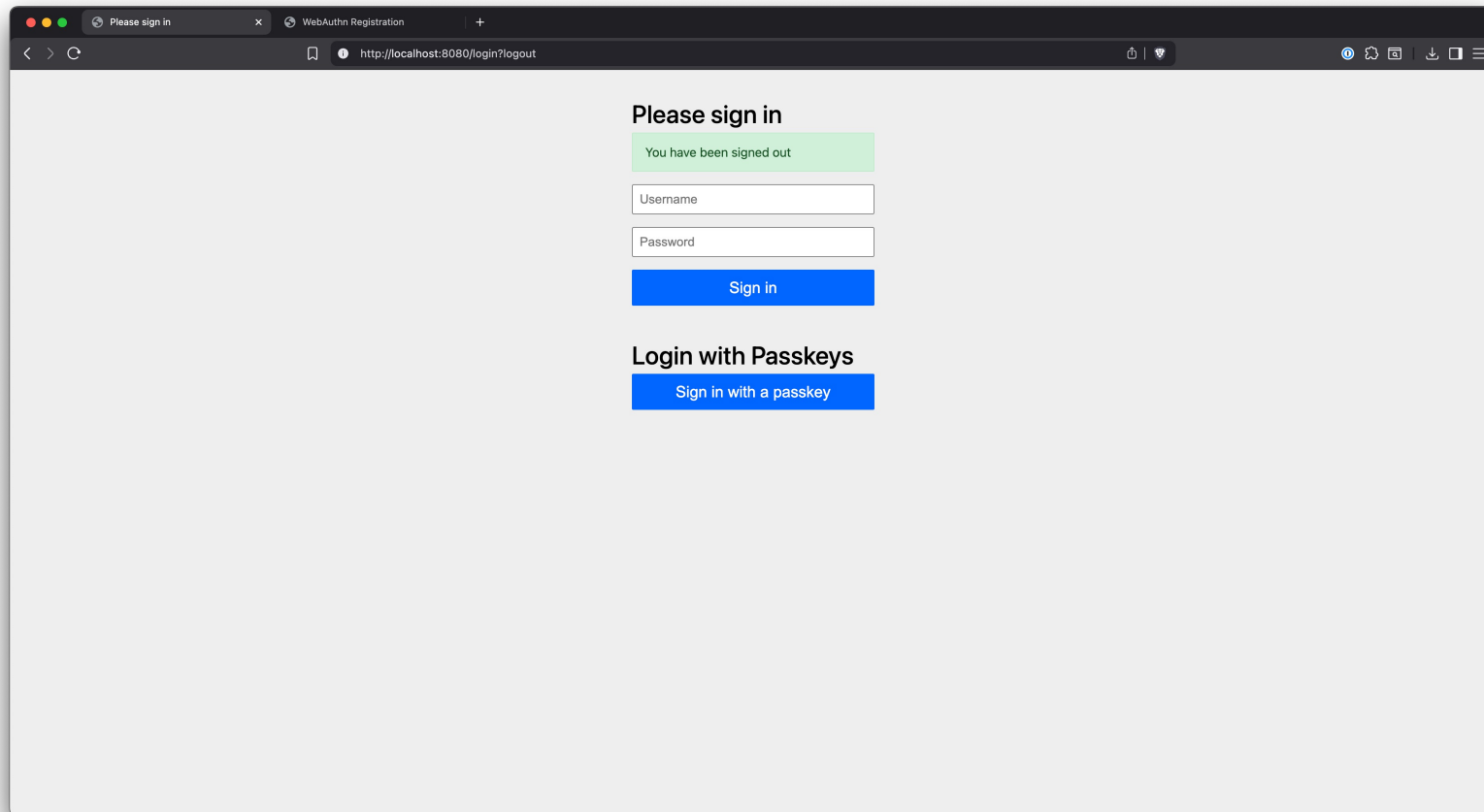
WebAuthn for Spring Security **SECURITY**
Support for WebAuthn in Spring Security.

Beispielapp

@Bean

```
public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {  
    return http.authorizeHttpRequests( ht -> ht.anyRequest().authenticated())  
        .formLogin(withDefaults())  
        .webAuthn(webauth ->  
            webauth.allowedOrigins("http://localhost:8080")  
            .rpId("localhost")  
            .rpName("webshopname")  
        )  
        .build();  
}
```

Beispielapp



The screenshot shows a web browser window with two tabs: 'Please sign in' and 'WebAuthn Registration'. The address bar displays 'http://localhost:8080/login?logout'. The page content includes a heading 'Please sign in', a green message box stating 'You have been signed out', a username input field, a password input field, a blue 'Sign in' button, a heading 'Login with Passkeys', and a blue button labeled 'Sign in with a passkey'.

Please sign in

You have been signed out

Username

Password

Sign in

Login with Passkeys

Sign in with a passkey

Beispielapp

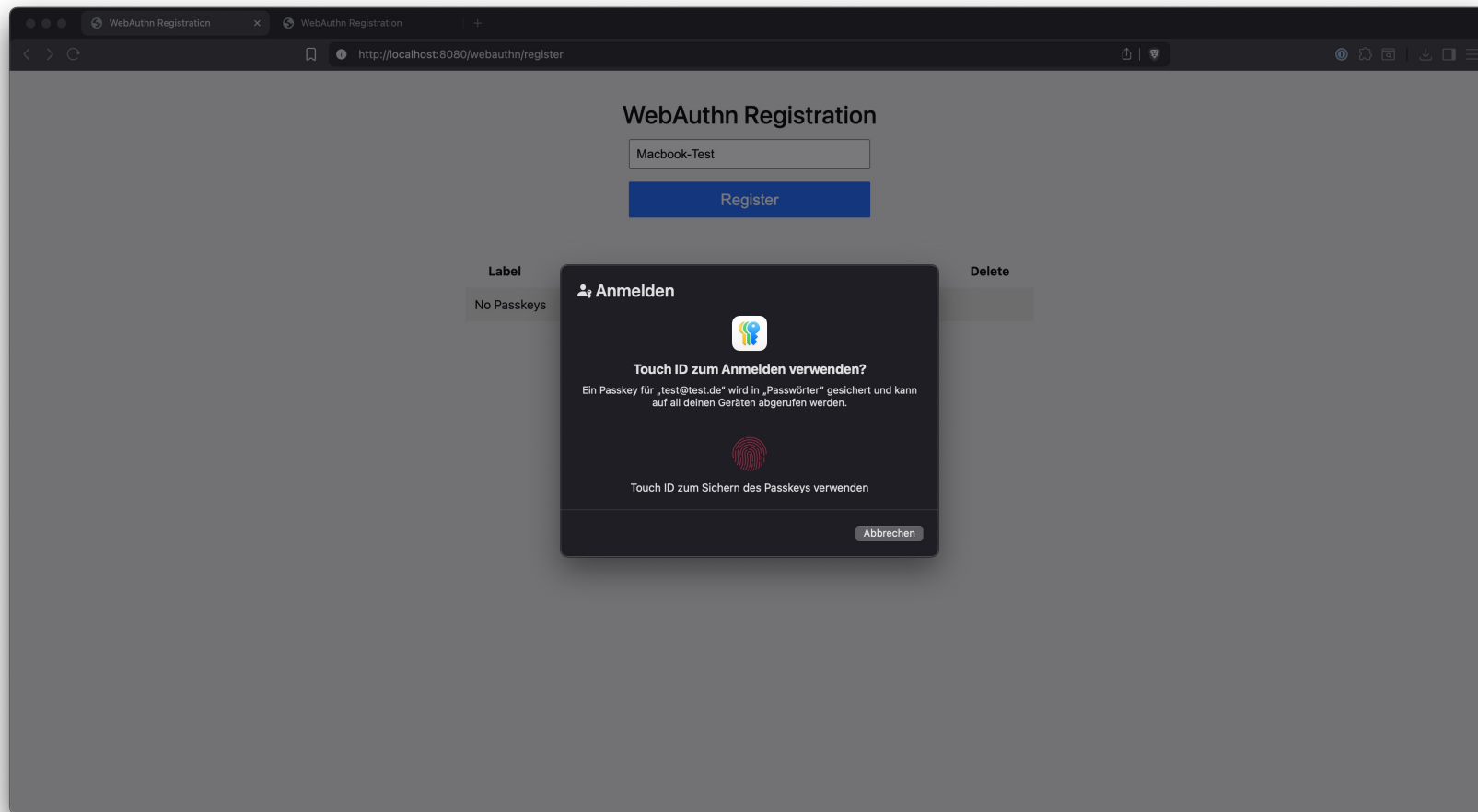
WebAuthn Registration

Passkey Label

Register

Label	Created	Last Used	Signature Count	Delete
No Passkeys				

Beispielapp



Beispielapp

WebAuthn Registration

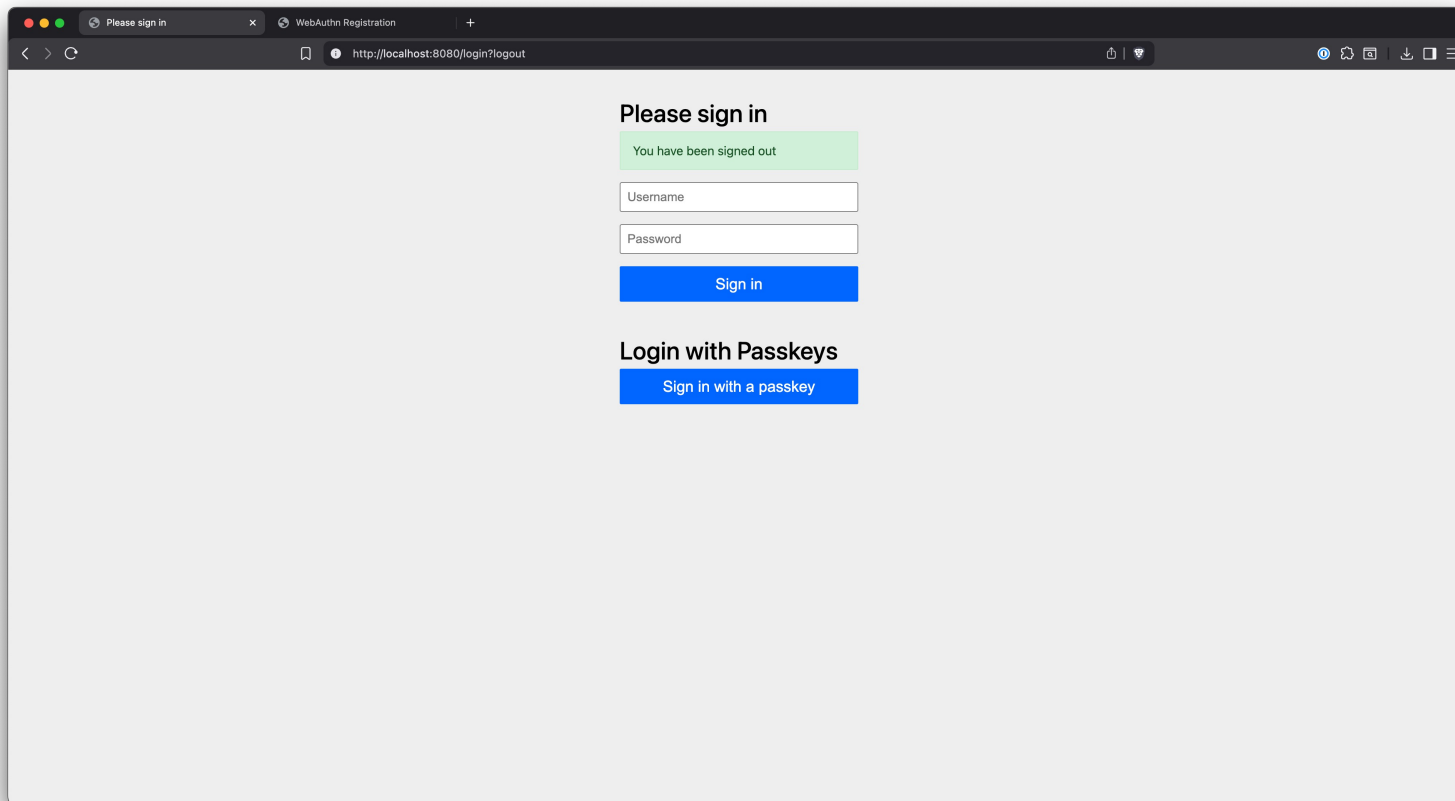
Success!

Passkey Label

Register

Label	Created	Last Used	Signature Count	Delete
Macbook-Test	2025-11-19T17:36:04Z	2025-11-19T17:36:04Z	0	Delete

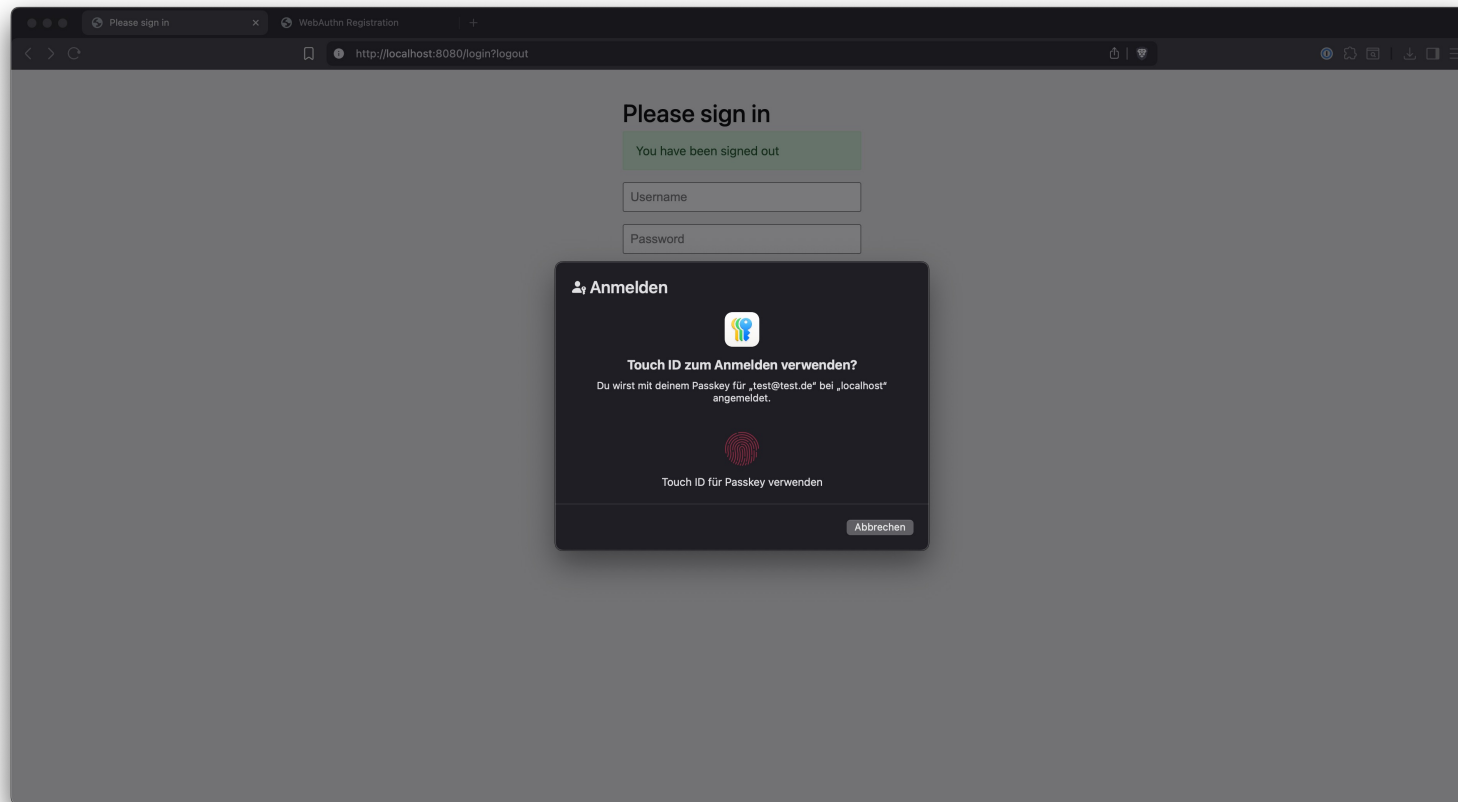
Beispielapp



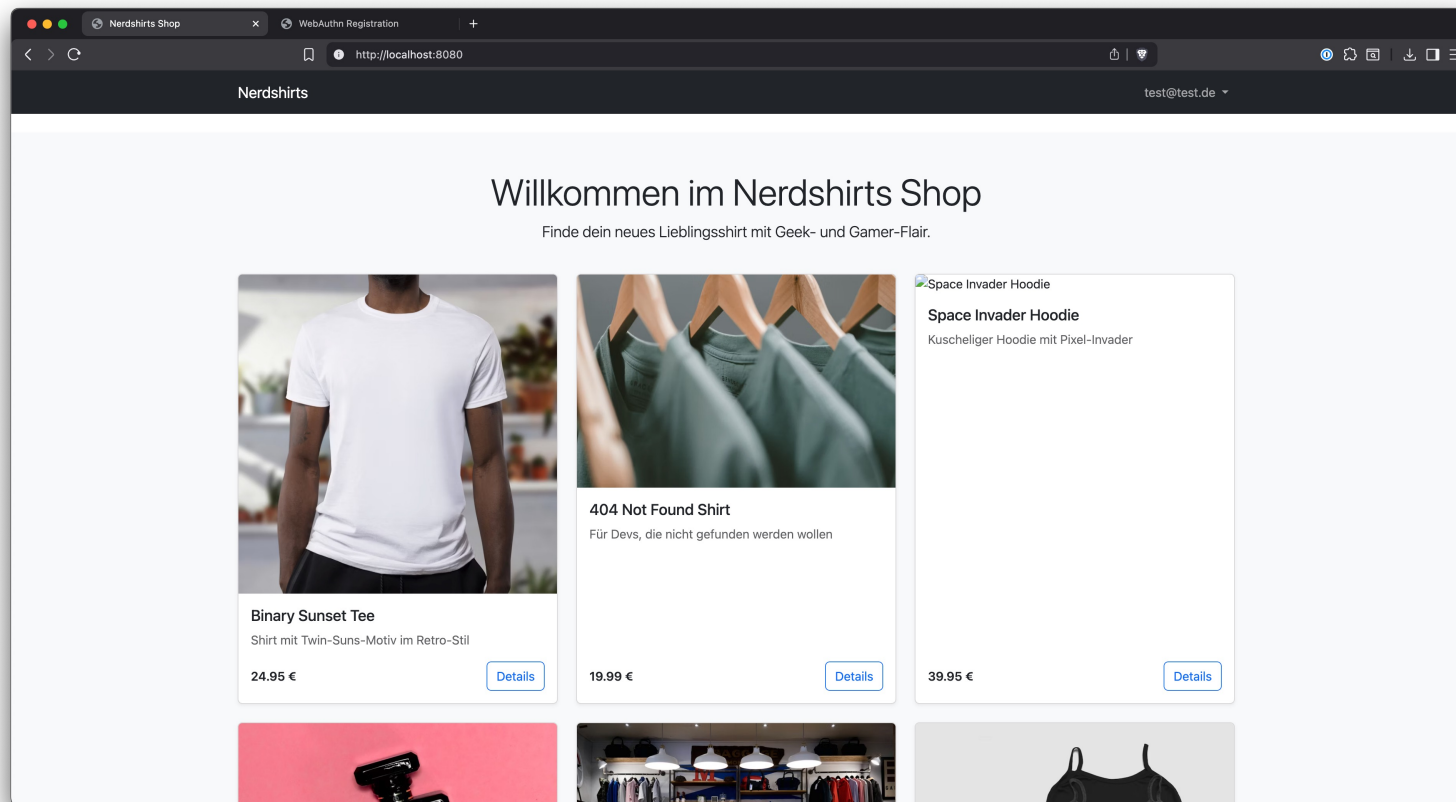
The screenshot shows a web browser window with two tabs: 'Please sign in' (active) and 'WebAuthn Registration'. The address bar displays 'http://localhost:8080/login?logout'. The page content is centered and includes the following elements:

- Please sign in**: A heading in bold black text.
- You have been signed out**: A message in a light green rectangular box.
- Username**: A text input field.
- Password**: A text input field.
- Sign in**: A blue button with white text.
- Login with Passkeys**: A heading in bold black text.
- Sign in with a passkey**: A blue button with white text.

Beispielapp



Beispielapp



Spring-Magie



Alternative (Passkeys as a Service)

The logo for Corbado, featuring a stylized 'C' icon followed by the word 'Corbado' in a sans-serif font, all in white on a dark blue background.

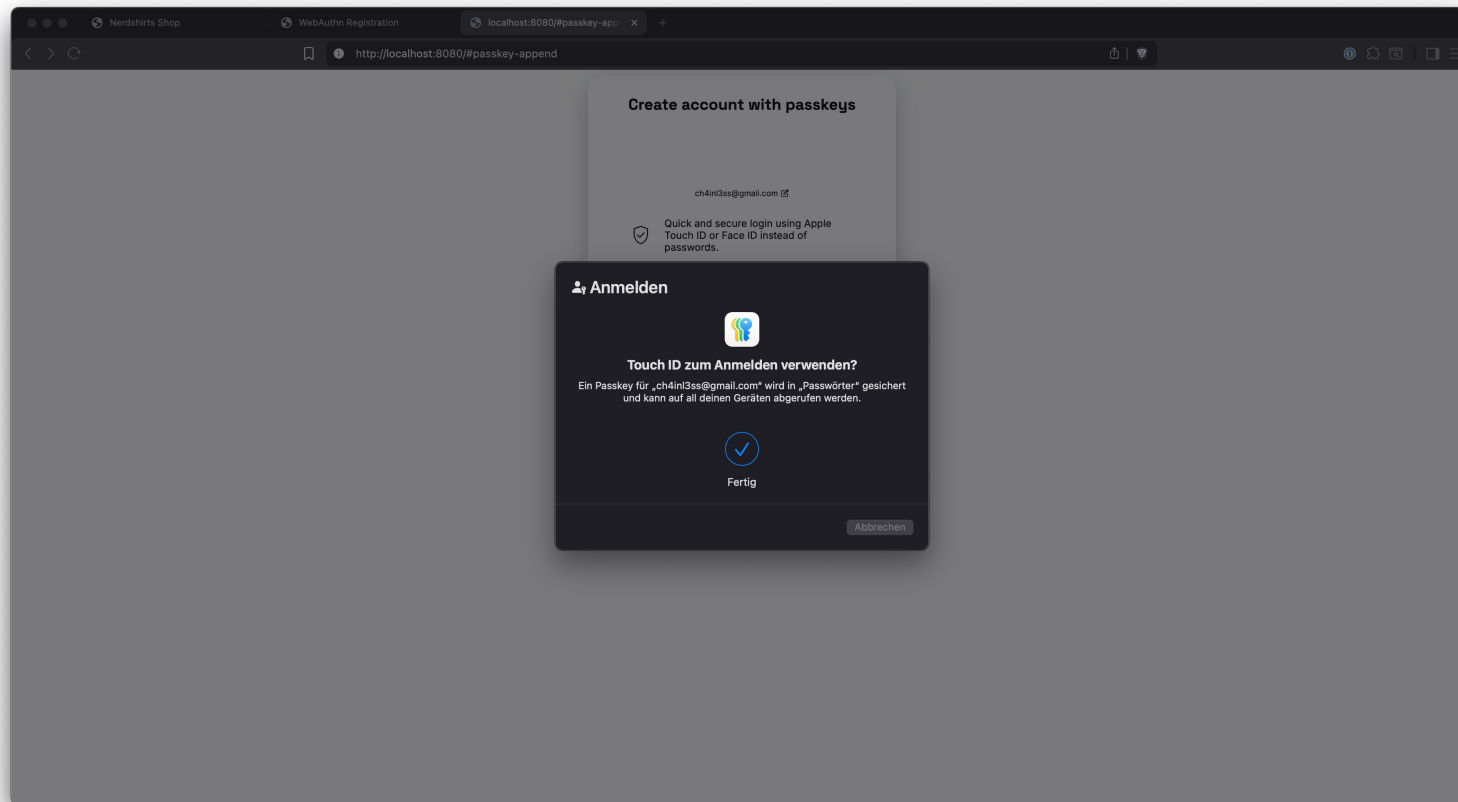
© Corbado

Corbado

The screenshot shows a web browser window with the following details:

- Browser Tabs:** "Nerdshirts Shop", "WebAuthn Registration", and "localhost:8080/#signup-init".
- Address Bar:** "http://localhost:8080/#signup-init".
- Form Title:** "Create your account to access webshop".
- Input Field:** "Email address" with a text input box.
- Buttons:** A blue "Continue" button.
- Separator:** A horizontal line with the word "or" in the center.
- Icons:** Three icons for social login: Google, Microsoft, and Apple.
- Text:** "You already have an account? [Log in](#)".
- Footer:** A blue button labeled "Secured by Corbado".

Corbado



Corbado

Enter code to create account

ch4inl3ss@gmail.com

One-time passcode
Enter the passcode sent to your email address

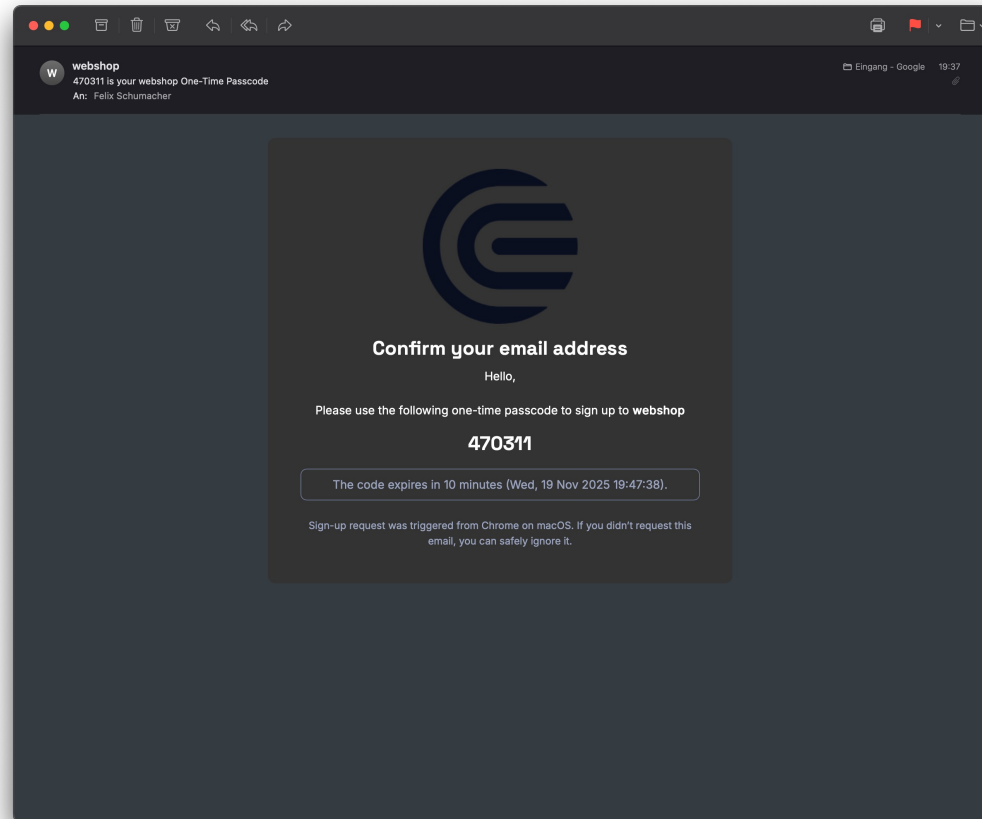
1

[Open in Gmail](#)

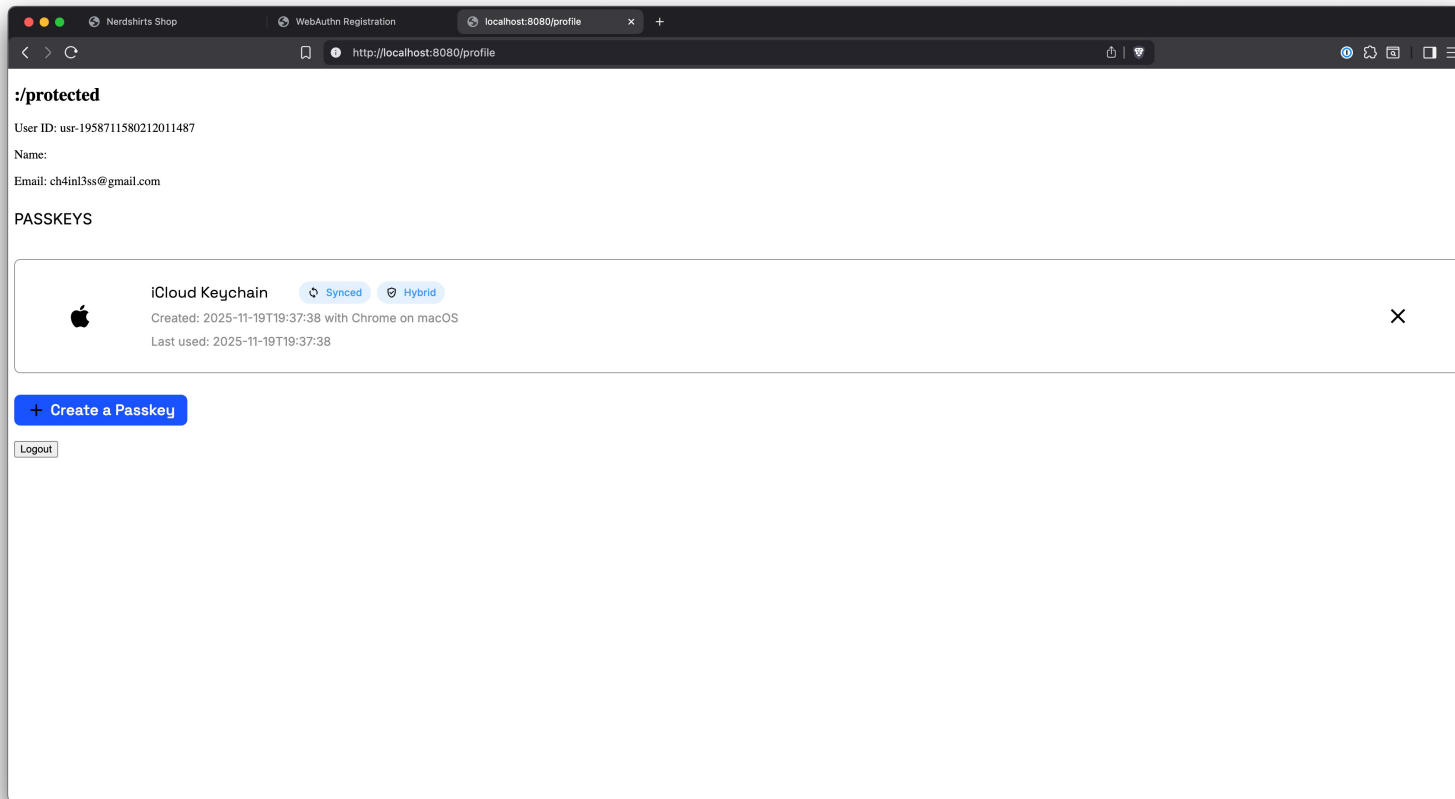
Didn't receive an email?
[Resend code \(18 sec\)](#)

Secured by Corbado

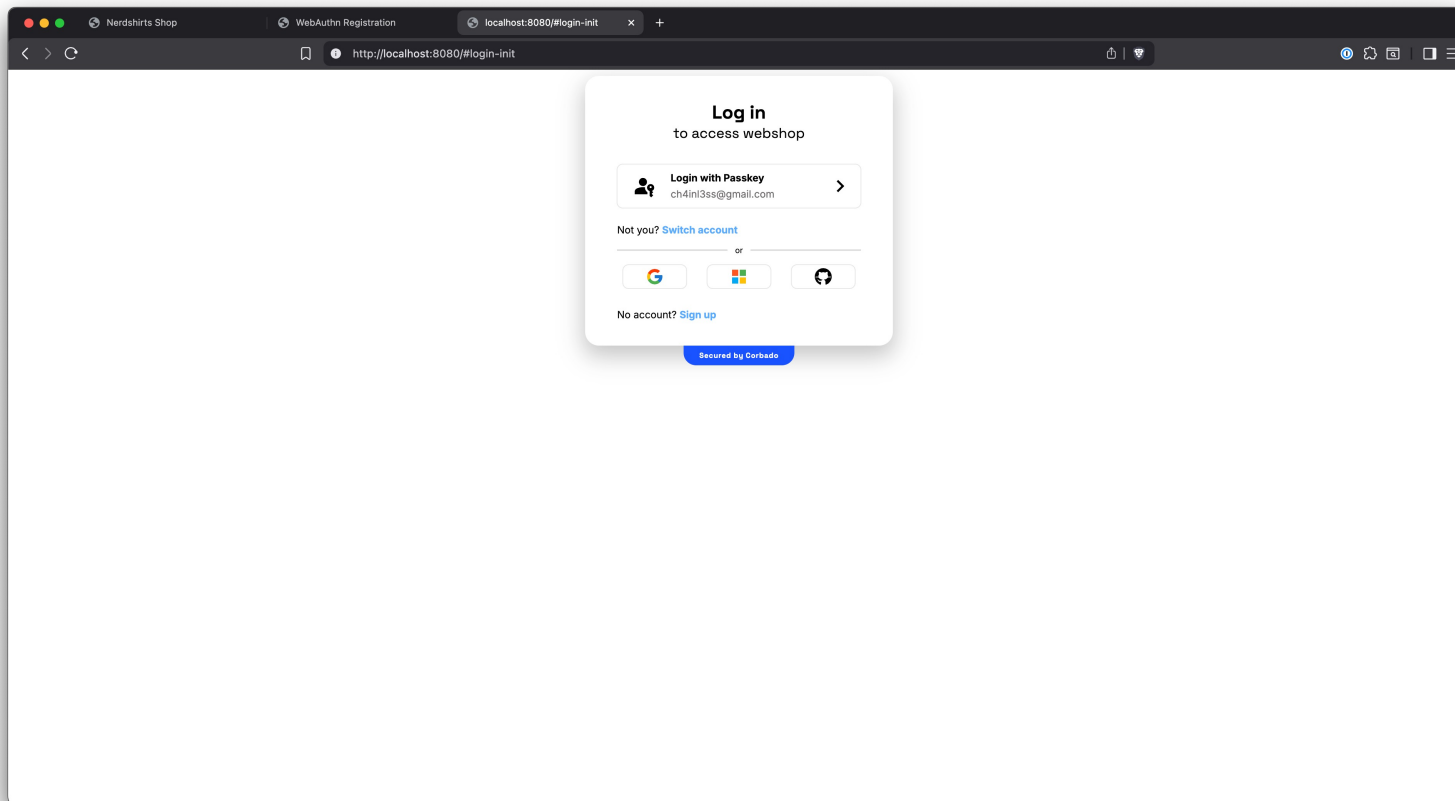
Corbado



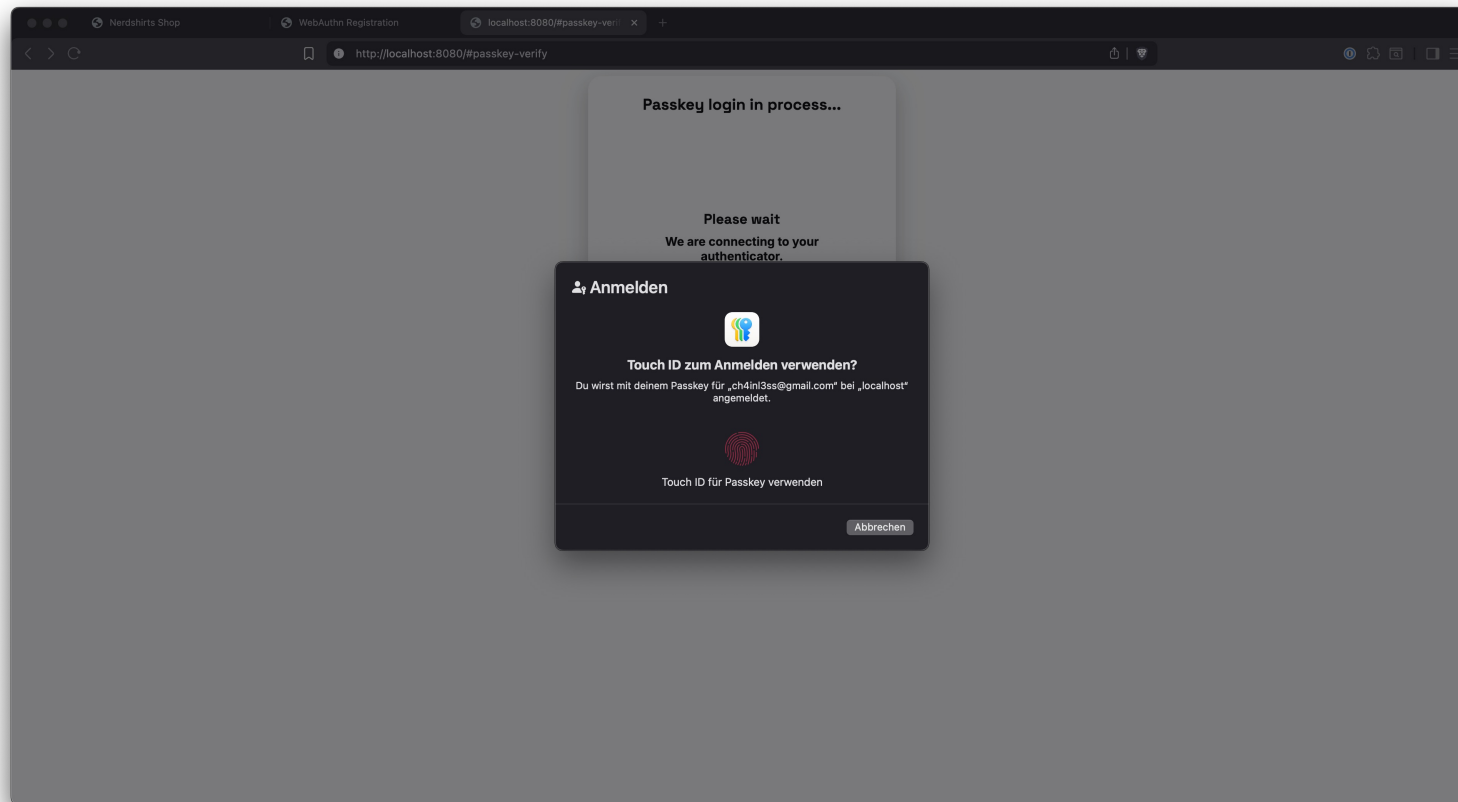
Corbado



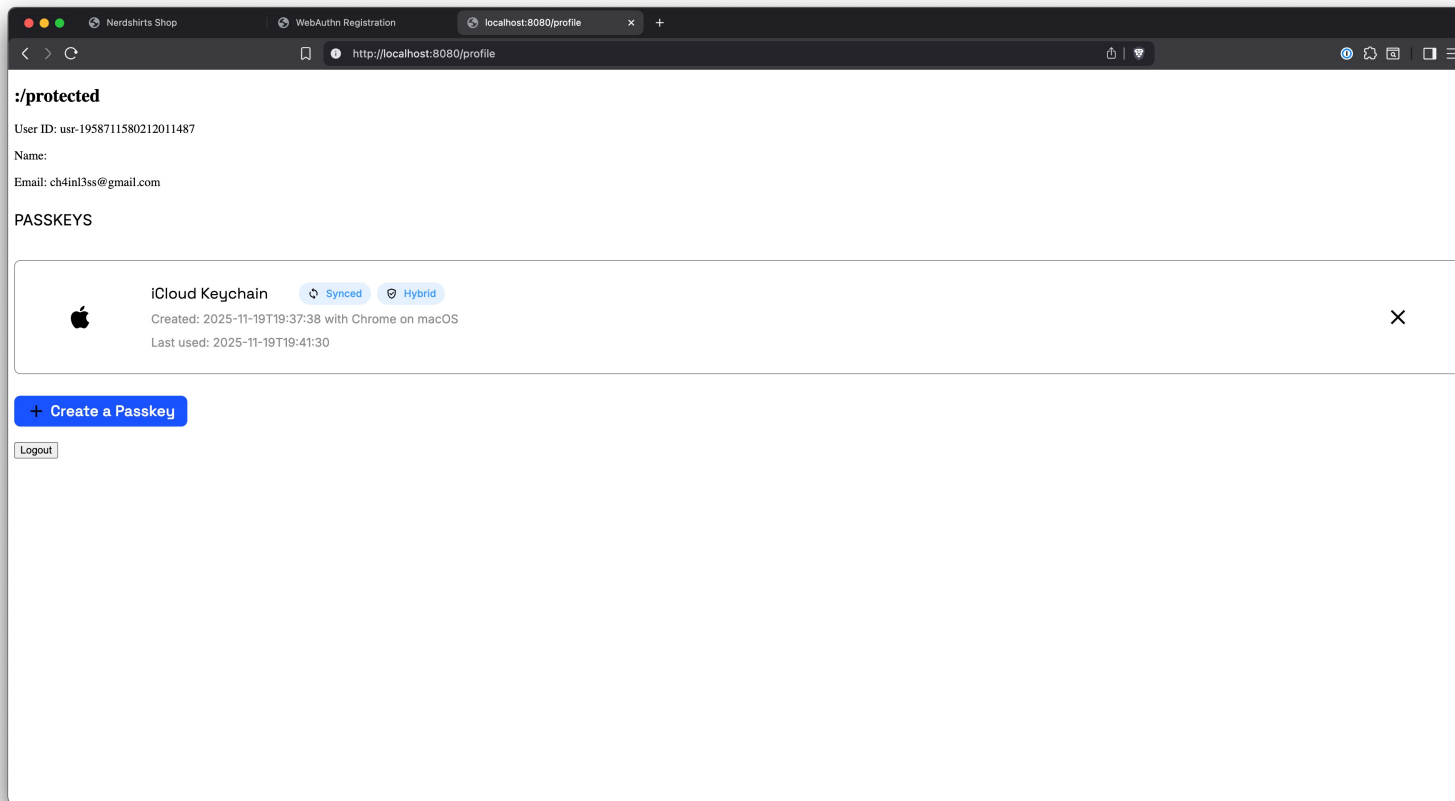
Corbado



Corbado



Corbado



Andere Alternativen:

- Hanko
- FrontEgg
- LoginID
- See <https://www.corbado.com/blog/best-hanko-alternatives>

Probleme mit Passkeys

- 1 Konto pro Gerät? Mehrere Geräte pro Konto?
- Sync über Cloud? (dann wieder MITM?)
- Recovery? (Gerät weg - Konto weg?)
- Transition von Passwörtern zu Passkeys?

Fazit

- Machbar, aber:
 - Libraries sind nicht trivial (yubico)
 - Oder haben super viel Magie... (spring)
 - As a service macht einen vom Provider abhängig
 - Further Research required...
-
- „Vibe-Coding“ führt bei mir zu fragwürdigen Ergebnissen

Danke! Fragen?



Felix Schumacher
felix.schumacher@innoq.com



innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim
+49 2173 3366-0

Ohlauer Str. 43
10999 Berlin

Ludwigstr. 180E
63067 Offenbach

Kreuzstr. 16
80331 München

Wendenstraße 130
20573 Hamburg

Spichernstrasse 44
50672 Köln