nextAuth

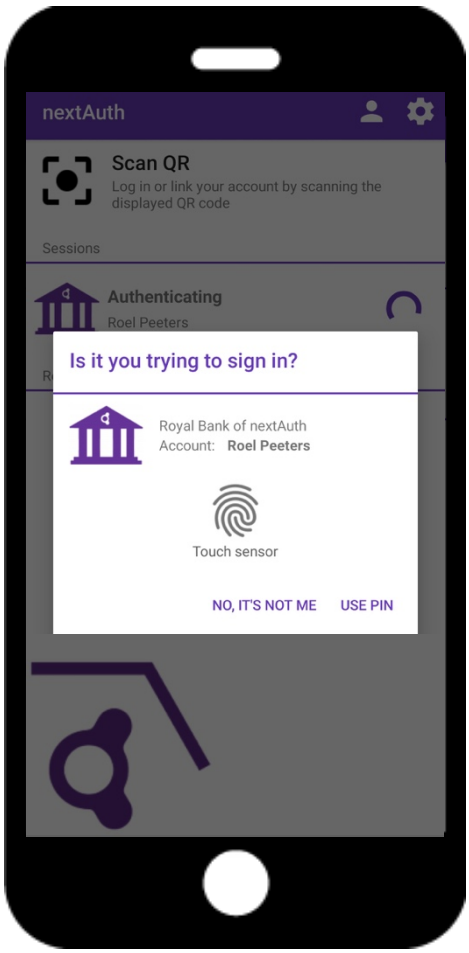
convenient, secure user authentication

In the rapid digitisation of society, a crucial step is the authentication of a person towards an online service, an IoT device, industrial equipment …

Nowadays users expect seamless authentication with high security, without requiring effort. Passwords are thus seen as a nuisance: “yet another password to remember”. Logging in with username/password on mobile is a major source of annoyance, leading up to 70% of users abandoning an app before even using it. Over time, when users forget their password, most of them will not bother to reset it.

At the same time users and companies are becoming more and more security aware. In 2017, 81% of security breaches leveraged weak, default or stolen passwords. Security breaches come with an average direct cost of 3.2 million euro and indirect losses through decline in share value and loss of customers.

nextAuth gives users a seamless experience while providing cutting-edge security, both for authentication across devices and in-app authentication.



Contact

Jens Hermans
CEO
jens.hermans@nextauth.com

Roel Peeters
CTO
roel.peeters@nextauth.com

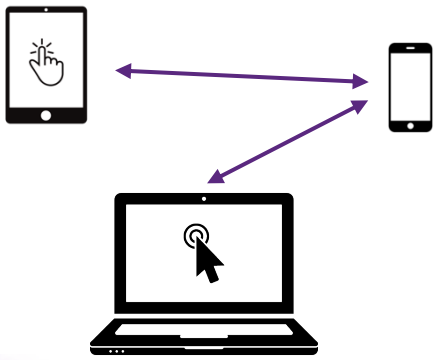
https://www.nextauth.com

Unique user experience

Seamless authentication

The best authentication from a user perspective is invisible authentication. In its basic form, this is exactly what nextAuth does.

nextAuth allows your developers to focus on creating functionality instead of worrying about authentication. Your app will seamlessly login to the backend whenever the user launches it. For more security, you can add a second authentication factor to your app, like for instance a PIN code or fingerprint.



Authentication transfer

Users don't restrict themselves to one device and authentication should neither. Instead of sharing credentials across devices, their mobiles can become the central credential. Imagine you want to show an application on your own or even a colleague's tablet without trusting it with your password.

nextAuth allows users to temporarily transfer their authentication to other devices, without revealing their credentials. With the snap of a QR-code or a simple tap a session will open on the target device. With a swipe on their nextAuth device, the session will be closed again. No need to worry anymore about entering your password on an untrusted device.

Dynamic authentication

nextAuth is extremely flexible and can dynamically authenticate users with different security levels. For simple actions, a seamless authentication can be sufficient, for higher security, a dynamic request for entering the second factor can pop up while providing the necessary context to the user.

A single account for multiple applications, multiple accounts for a single application, transaction approval, subaccounts for fine grained dynamic authentication or maybe just an instant notification of sensitive actions? You imagine it, nextAuth can provide it.

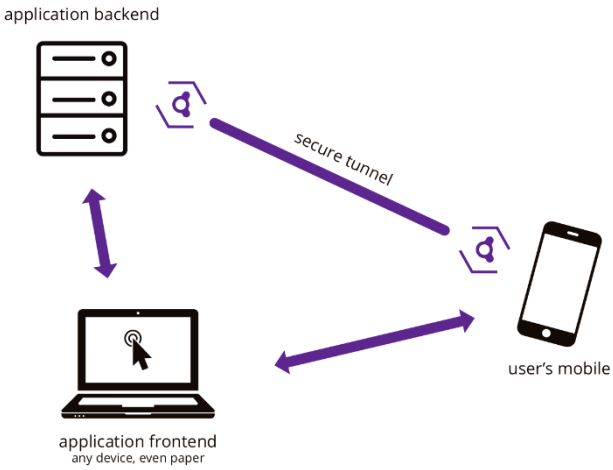
Architecture

nextAuth integrates with the application backend to authenticate both direct connections from nextAuth enabled apps and transferred authentications from other devices.

nextAuth can provide authentication for a wide variety of applications due to its flexible API and simple integration libraries.

nextAuth has been designed to run on premise, next to the application backend, keeping you in full control of this critical part of your IT infrastructure.

We respect the privacy of your users. nextAuth is dedicated to use as little data as possible from users for authentication.



Security

nextAuth brings together multiple state-of-the art security techniques, directly from the research of KU Leuven – COSIC:

- Going far beyond the security offered by commodity technology such as TLS, nextAuth makes use of a mathematically proven authentication protocol.
- No need to worry about your credential database leaking: our public key cryptography combined with patent-pending two-factor authentication technology renders your user credential database useless for attackers.
- Keeping users in control of their active sessions through continuous authentication (logout from app).
- Dynamic authentication: flexibility to match any use case.
- In-depth secured implementation, built by experts in security and cryptography.
- Optional: post-quantum secure cryptography

KU LEUVEN

COSIC