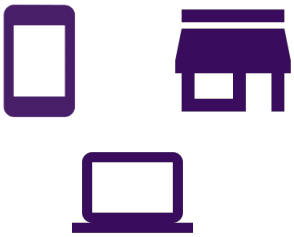
nextAuth

The next generation in user authentication

nextAuth brings highly secure two-factor user authentication to companies, while providing their users with an easy solution that runs on their own mobile devices. We do so by eliminating usernames and passwords, and replacing it with an app in combination with a PIN or biometric.

nextAuth thus drastically improves your security *81% of all data breaches are due to weak/default/stolen passwords* and keeps your help desk focused on helping your users with what matters most: your application *10-30% of all help desk calls are related to password resets*.

The nextAuth approach



Unified authentication experience across all platforms and channels: one or more mobile apps, web applications, retail points…

Your brand first: completely brandable technology and fully embeddable into existing applications.

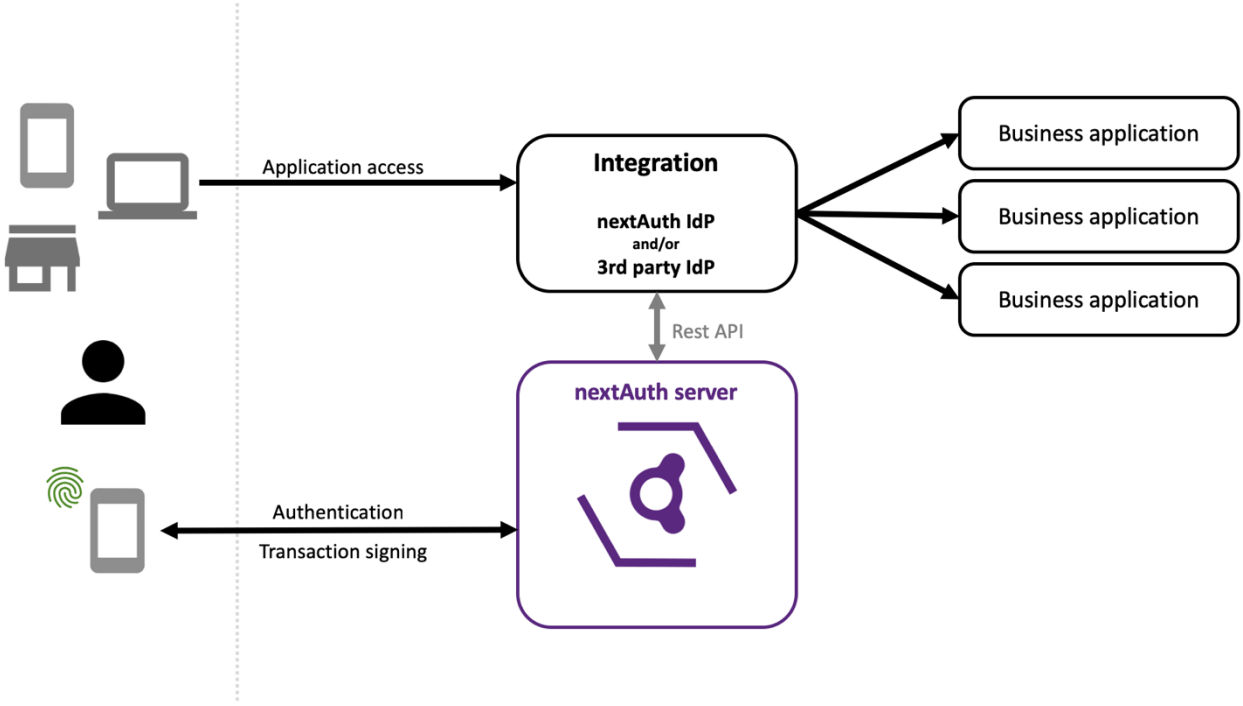
Strong security based on state-of-the-art cryptography. True digital signatures to enable compliance with legal requirements (eIDAS, PSD2...). Transaction signing supported.

Full support of mobile device biometrics, eliminating all user hassle during authentication.

Keep authentication of your users fully under your control, no third party needed.

Product and services overview

nextAuth architecture



Overview of the nextAuth Architecture

Mobile authentication library

The nextAuth mobile authentication library provides strong two-factor (device + pin/fingerprint/ faceID) user authentication from their own mobile devices. The library takes care of all security aspects, among which key management, mutual authentication, back-end communication, implementation security, obfuscation, session management (including app-initiated session termination), inter-app communication and user authentication.

Enrolment of a new user happens by either scanning a QR code (e.g. to associate the new account with existing user data) or through self-registration in the app.

Authentication can be initiated through several means, such as a user action in the app itself, intents from a different app on the same mobile device, a push notification, scanning a QR code... The library will perform authentication, resulting in the authentication of a session (in the app, another app or even an external device).

The library is available for Android and iOS and is provided with code samples to embed it into an existing app or create a new authentication app.

White labelled app

nextAuth provides white labelled apps (both Android and iOS) that incorporate the nextAuth mobile authentication library. These white labelled apps are adjusted to your brand and under your name.

Authentication server

The nextAuth authentication server acts as the endpoint for authentication by the mobile library. It handles all server-side credential management, creation of new device accounts and session management (including push messages). The authentication server offers a privileged REST API for integration with business application back-ends. It can also be integrated through SAML, OAuth2 and OIDC by using the nextAuth IdP. Management of user attributes and identity verification is performed through separate modules and applications.

The authentication server can either be installed on your infrastructure (including cloud) or as a SaaS on nextAuth infrastructure.

Self service module

nextAuth provides modules for self-registration and self-management of devices, allowing users to add and remove devices. This can include the verification/registration of certain user attributes:

- email address (verification email)
- phone number (SMS)

Verification mechanisms typically require integration with the relevant business applications or the identity management platform.

Integration services & security consultancy

In order to facilitate the integration of nextAuth-provided components into existing mobile apps and/or server-side applications, nextAuth provides the necessary integration services. nextAuth also provides advice for the development of the overall security architecture, in particular with aspects related to identification and authentication.

Our security guarantees

- ☑ 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.
- ☑ Users keep control of their active sessions through continuous authentication (logout from app).
- ☑ Dynamic authentication: flexibility to match any use case. 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.
- ☑ In-depth secured implementation, built by experts in security and cryptography.
- ☑ Optional: post-quantum secure cryptography.

Contact

https://www.nextauth.com

Jens Hermans
CEO
jens.hermans@nextauth.com

Roel Peeters
CTO
roel.peeters@nextauth.com