NoPass

PASSWORDLESS REGISTRATION AND AUTHENTICATION

Contact us
sales@identite.us
www.identite.us

Burden of Passwords

Passwords are the most used form of website authentication. Password authentication requires users to create a key that only they (and the website) know as a way to access their online accounts.

Password-based security has become less secure in recent times due to more sophisticated phishing attacks and challenges faced by users to create and manage numerous passwords. Also, the centralized storage of millions of user credentials (including passwords) in a cloud or a website server can provide a single point of a target for hackers, which can greatly increase the cost of a single security breach. Online attacks like Man-in-the-Middle (MitM) and Man-in-the-Browser (MitB) can pose a substantial threat to online authentication by secretly modifying the communication between user and server.

NoPass™ Passwordless Authentication

NoPass™ is a passwordless registration and authentication tool to authenticate users coming into a customer or constituent portal. With minimal typing or actions by a user, they can quickly register and authenticate with 3 factors – something you know, something you have and something you are.

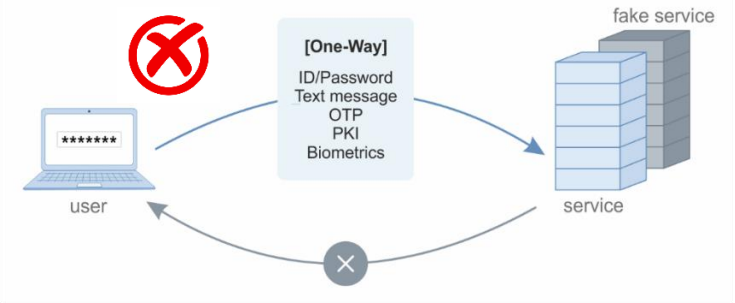
Simple and Secure

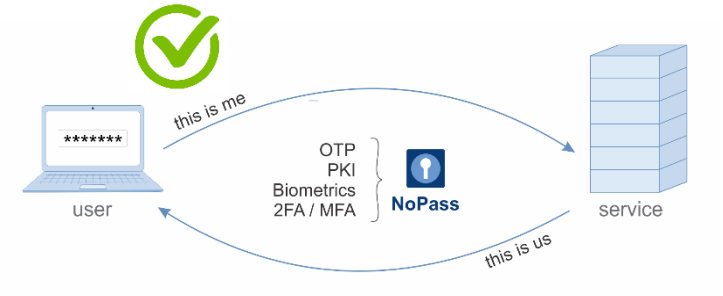
NoPass™ is a secure authentication app that brings you the two things you need most: the highest level of authentication security and the simplest user experience. Now you can have the confidence of never worrying about a compromise of your online credentials.

Along with very strong security, the user does not need to enter a password. The NoPass™ server and application in the phone takes care of all of the bi-directional handshaking, requiring only that the user compare two images (a picture and a 3-digit number), then swipe or touch the approve button, and they are connected. This method provides a million encrypted combinations, and is virtually un-hackable since the metadata is valid for only a few seconds and is useless after that. Even if the user mistakenly approves the transaction, we are able to detect the intrusion and block the entry into the server.

FULL DUPLEX AUTHENTICATION™ Technology

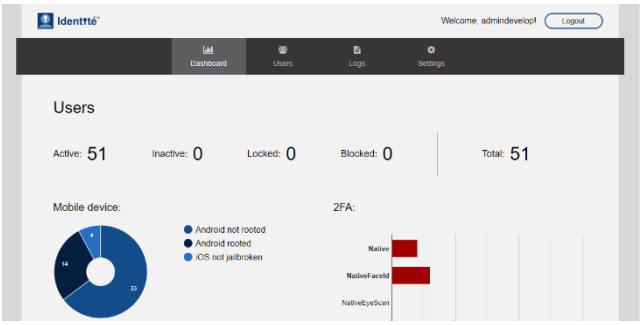
The NoPass™, Full Duplex Authentication™ process follows a decentralized authentication model. This lets us work together with any kind of traditional user authentication technology, such as PIN, OTP, PKI, and Biometrics. NoPass™ has a flexible architecture to easily integrate with any User Authentication solution.





NoPass™ Admin Panel

Gain complete Administration Overview - Using the NoPass™ Admin Panel. Device Trust Ensure all devices meet security standards. Adaptive Access Policies Set policies to grant or block access attempts. Remote Access Secure access to all applications and servers.



Every aspect of your NoPass™ authentication system can be managed from the NoPass™ Admin Panel. This includes creating and managing applications, enrolling and activating users, managing mobile devices, fine-tuning the user experience of your NoPass™ installation, and more.

Infrastructure Requirements

On-premise

- Highly available deployment
- Docker & Kubernetes support
- Reverse proxy
- Clustering and HA

Cloud

- Private cloud deployable (ie. AWS, Azure, IBM)Highly available deployment
- High scalability
- Deploy in almost every country
- Support for self-sign up for trials and production

Product Features

- Simple & Clear User Experience for Registration, Authentication, and Restoration
- Innovative picture and code OTP, user convenient and much higher brute force security
- Progressive registration with minimal typing or actions by a user
- Easy to use Admin Panel to set policies and restrictions
- Controlling device hygiene and checking for rooted or jailbroken devices that may compromise security
- Flexible Integration with any existing User Authentication
- Android and iOS supported
- Encrypted secure cloud account backups accessible for both iOS and Android

Benefits of NoPass™

Increased Revenue
The improved user experience will help acquire new customers and retain the old ones.

Security
Login credentials are unique across every website, never leave the user's device and are never stored on a server. Prevent Identity theft by eliminating insider attacks from compromised employee credentials.

Convenience
Users unlock login credentials with simple built-in methods such as fingerprint readers or face scans.

Scalability
The wide use of smartphones and our cloud deployment make it super easy to scale any existing authentication.

Privacy
Protect your users from credential leaks and password phishing.