



## Carregamento de senhas

As senhas são a forma mais usada de autenticação de sites. A autenticação de senha exige que os usuários criem uma chave que somente eles (e o site) conheçam como uma maneira de acessar suas contas online. A segurança baseada em senha tornou-se menos segura nos últimos anos devido a ataques de phishing cada vez mais sofisticados e aos desafios que os usuários enfrentam na criação e gerenciamento de diversas senhas. Além disso, o armazenamento centralizado de milhões de credenciais de usuário (incluindo senhas) na nuvem ou em um servidor de site pode fornecer um destino único para hackers, o que pode aumentar bastante o custo de uma única violação de segurança. Ataques online como MitM (Man-in-the-Middle) e MitB (Man-in-the-Browser) podem representar uma ameaça substancial à autenticação on-line, modificando secretamente a comunicação entre o usuário e o servidor..



## NoPass™ - Autenticação sem senha

O NoPass™ é uma ferramenta de registro e autenticação sem senha para autenticar usuários que entram em um cliente ou portal constituente. Com pouca digitação ou ações mínimas por um usuário, eles podem se registrar e se autenticar rapidamente com com três fatores: algo que você sabe, algo que você tem e algo que você é.

Algo que usted sabe	Algo que tiene	Algo que usted es
		
Nombre de usuario o la ID que utiliza para iniciar sesión	Smartphone, código de acceso único o tarjeta inteligente	Biometría, como su huella digital, escaneo de retina o reconocimiento de voz

## Simple e seguro

O NoPass™ é um aplicativo de autenticação segura que fornece as duas coisas que você mais precisa: o mais alto nível de segurança de autenticação e a experiência mais simples do usuário. Agora você pode ter certeza de nunca se preocupar em comprometer suas credenciais online. Juntamente com uma segurança muito forte, o usuário não precisa digitar uma senha.

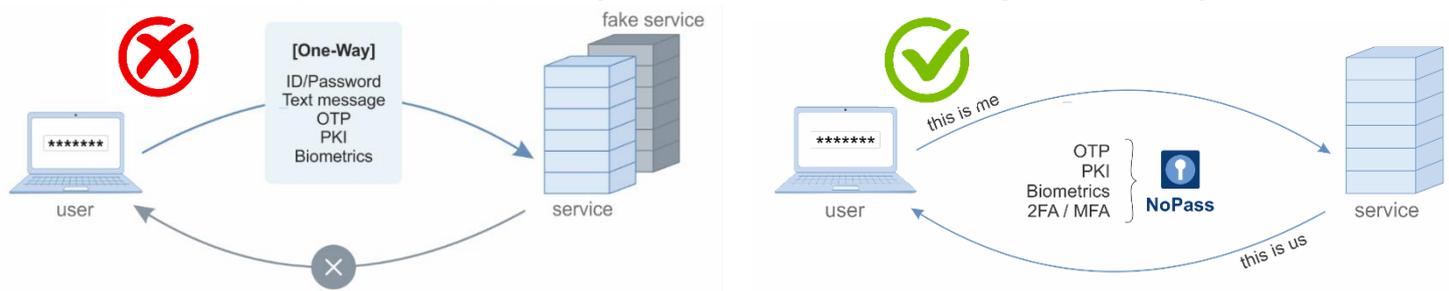
O servidor NoPass™ e o aplicativo para smartphone cuidam de todo o link bidirecional e exigem que o usuário compare duas imagens (uma imagem e um número de 3 dígitos) e, apenas tocando no botão de aprovação, elas estão conectadas.



Esse método fornece um milhão de combinações criptografadas e praticamente não pode ser comprometido por um hacker, pois os metadados são válidos por apenas alguns segundos e depois são inúteis. Mesmo se o usuário aprovar a transação por engano, podemos detectar a intrusão e bloquear a entrada no servidor.

## TECNOLOGIA DE AUTENTICAÇÃO FULL DUPLEX™

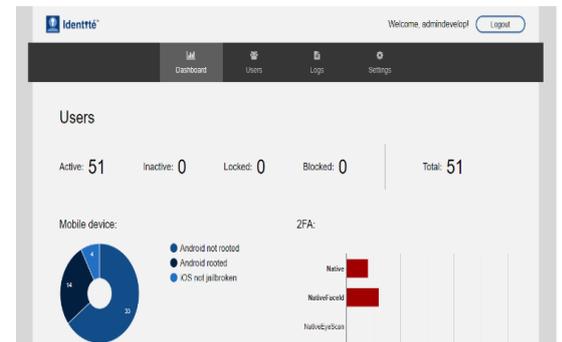
O processo de autenticação NoPass™, Full Duplex™ segue um modelo de autenticação descentralizado. Isso nos permite trabalhar com qualquer tipo de tecnologia tradicional de autenticação de usuário, como PIN, OTP, PKI e biometria. O NoPass™ possui uma arquitetura flexível para integrar-se facilmente a qualquer solução de autenticação de usuário.



### NoPass™ Painel de administração

Obtenha uma visão geral completa da administração: usando o painel de administração do NoPass™. Garantia de confiança do dispositivo - verifique se todos os dispositivos atendem aos padrões de segurança. Políticas de acesso adaptável estabelecem políticas para conceder ou bloquear tentativas de acesso. Acesso remoto, acesso seguro a todos os aplicativos e servidores.

Todos os aspectos do seu sistema de autenticação NoPass™ podem ser gerenciados no painel de administração do NoPass™. Isso inclui criar e gerenciar aplicativos, registrar e ativar usuários, gerenciar dispositivos móveis, ajustar a experiência do usuário da instalação do NoPass™ e muito mais.



### Requisitos de infraestrutura

#### Interno (servidor da empresa)

- Implantação altamente disponível
- Suporte para Docker e Kubernetes
- proxy reverso
- Agrupamento e HA

#### Nuvem

- Implantação em nuvem privada (ou seja, AWS, Azure, IBM) Implantação de alta disponibilidade
- Alta escalabilidade
- Implementar em quase todos os países
- Suporte para auto-registro para teste e produção.

### Características do produto

- Experiência do usuário simples e clara para registro, autenticação e restauração
- Imagem e código OTP inovadores, conveniência do usuário e segurança muito maior da força bruta
- Registro progressivo com digitação ou ações mínimas pelo usuário
- Painel de administração fácil de usar para definir políticas e restrições
- Verifique a higiene do dispositivo e verifique se existem dispositivos raiz ou liberados que possam comprometer a segurança.
- Integração flexível com qualquer autenticação de usuário existente
- Compatível com Android e iOS
- Backups criptografados de contas na nuvem acessíveis para iOS e Android

### Benefícios de NoPass™

#### Aumento de renda

A experiência aprimorada do usuário ajudará a adquirir novos clientes e reter clientes antigos.

#### Segurança

As credenciais de login são exclusivas para todos os sites, nunca saem do dispositivo do usuário e nunca são armazenadas em um servidor. Evite o roubo de identidade, eliminando ataques internos às credenciais comprometidas dos funcionários.

#### Conveniência

Os usuários desbloqueiam credenciais de login com métodos internos simples, como leitores de impressões digitais ou digitalizações faciais.

#### Escalabilidade

O uso extensivo de smartphones e nossa implementação em nuvem facilitam o dimensionamento de qualquer autenticação existente.

#### Privacidade

Proteja seus usuários contra vazamentos de credenciais e phishing de senha.