IDEE

AuthN by IDEE

Datasheet

AuthN by IDEE

Why is MFA still failing your business?

Password+2FA based Security is a 'Myth'
Passwords, a commonly-used authentication mechanism in most enterprises, constitute one of the biggest threats to security. In 2020, over 80% of breaches (hacking) involved phishing, brute force, or the use of lost or stolen credentials. This is true even in modern enterprises that have implemented Two-Factor Authentication (2FA). Despite its relative superiority over password-only systems, 2FA with a password and OTP cannot protect against phishing. Moreover, 'convenient' and 'robust' Single Sign-On (SSO) have turned out to worsen the problem by creating a single-point-of-failure that leaves multiple systems secured by just one password vulnerable to attack. So, when it comes to enterprise security, passwords – whether with 2FA or as part of SSO – do not prevent phishing nor do they eliminate account takeover.

Security Challenges in Work from Home Models
To ensure business continuity, many organizations have adopted a 'work from home' model. This makes them vulnerable to cyber-attacks. Passwords don't provide adequate protection, and their challenges cannot be mitigated by simply adopting 2FA with weak authentication factors like OTPs. The 'security perimeter' has disappeared, and the only way to ensure security now is through zero trust passwordless systems and strong multi-factor authentication.

Administrative Overhead Costs of Passwords
The financial costs of passwords are not always obvious. One relates to the deployment of a system to create user accounts and manage all passwords. There's also the ongoing cost of administering and managing the system. Lost user productivity caused by authentication problems due to forgotten passwords, and the help-desk resources required to manage password reset requests are also considerable costs. Many organizations think that password security is "free". It's not. It is, in fact, very expensive.

The answer is AuthN.

AuthN is the most secure MFA on the market.
It prevents all phishing and password-based attacks.

Offering 100% passwordless, zero trust, multi-factor authentication as a service, AuthN completely eliminates phishing and password-based attacks, while reducing administrative overhead costs. No passwords, so nothing to phish, intercept or steal! This means fewer breaches and human errors that cause costly security incidents.

Offering built-in interoperability, fast integration, plug-n-play support for existing SSO architectures, and full compliance, AuthN enables enterprises to transition to enterprise-wide multi-factor authentication with ease.

AuthN Top Features

Security
- Adaptive Authentication
- Multi-factor Authentication
- Multi-party Authorization
- Insider Threat Prevention
- User Binding

Management & Compliance
- Auto-enroll Existing Users
- Custom Branding
- Immutable Audit Trail Admin
- Dashboard & APIs

Integration
- FIDO2/WebAuthN
- SAML, OIDC
- RADIUS REST API
- Custom Libraries
- Mobile SDKs

Auth. Destination
- Web Application
- Mobile Application
- In-App Webview
- Server (SSH)
- VPN, Remote Desktop

User Experience
- WebAuthN
- QR-Code Login
- Push Login
- Offline Login Multi-Device Support

AuthN Core

Features included in everything we do.

- ✓ 100% Passwordless
- ✓ Zero-trust
- ✓ Zero-knowledge
- ✓ Zero Private Data (PII)
- ✓ No Credentials Database
- ✓ Identity Proofing
- ✓ Multi-account
- ✓ Multi-device

Table of Contents

Security

There are few things as critical as security when it comes to authentication. Our Zero Trust, Zero Knowledge and Zero PII architecture ensures that you will never have to worry about phishing or password-based threats.

Zero Trust

Reduce the complexity of your IT security stack and protect your business' data with AuthN's Zero Trust Architecture that strictly follows "never trust, always verify" at every interaction.

Decentralized Credentials

Reduce the risk of massive credential breaches by removing the central credentials database, the single point of failure that hackers seek to exploit.

100% Passwordless

Eliminate all password-related threats from your list of potential threats, because with AuthN passwords just do not exist.

Zero Knowledge

Ensure that the user's credentials are never exposed to AuthN, any of IDEE's servers, or anyone else.

Zero PII

Achieve compliance and be assured that IDEE never stores any private information and only processes the absolute minimum amount of data needed to run its service.

Identity Proofing

Verify the identity of your users during registration. AuthN offers IAL1 such as Email and Phone number verification by default as well as stricter verification such as video-identification (IAL3) or ID verification (IAL2).

Active Connection Manager

Always gives your users an overview of their active sessions, so they can easily see where they're logged in or detect suspicious activity.

Remote Logout

Allow users to end a session remotely from any device e.g. if they forgot to log out.

Backup & Recovery

Ensure uninterrupted access to user's accounts even if they lose their phone, allowing them to restore their accounts with a secure key that only they know.

Multi-Factor Authentication

Prevent 99.9% of all attacks on your users' accounts with secure, and passwordless Multi-Factor Authentication.

Multi-Party Authorization

Secure privileged access management by requiring multiple users to approve a transaction e.g. when accessing files on critical infrastructure.

Insider Threat Prevention

Protect yourself from insider threats with the most extreme form of Zero Trust. No need to trust your own database administrators. No need to trust IDEE.

User Binding

Makes sure that the identity is bound to the device and to the app instance.

Transitive Trust

Make sure that the chain of trust is unbroken throughout the user lifecycle. This means from registration, to authentication, to verification a user is in complete control of their identity. External or internal attackers cannot interfere.

Management & Compliance

Being able to manage, monitor and control who has access with as little effort as possible and in a compliant manner is key. Features such as our user Self-Service Portal, the Audit Trail and Management APIs help you automate, so that resources can be spend on more important things.

Self Service Portal

Reduce administrative overhead by providing a secure and seamless experience for users to manage their devices and accounts themselves.

Ghost Account Management

Stop worrying about ghost accounts from partners or suppliers that have long left their company but still have access to your data by automatically disabling them after a given criteria.

Immutable Audit Trail

Simplify compliance assessment and easily trace non-compliant behavior without violating privacy.

Admin Dashboard

Control & manage users and devices in an easy to use web interface.

Logging API

Enhance your internal monitoring capabilities by gathering log events via our Logging API.

Device API

Manage AuthN registered devices directly from within your own systems through our Device API.

Account API

Manage AuthN registered user accounts directly from within your own systems through our Account API.

Integration

Integrating secure authentication should be a plug and play experience. AuthN supports integration using global standards such as SAML for your cloud-native applications as well as custom libraries and mobile SDKs to speed up integration into legacy systems.

SAML 2.0

Integrate MFA capabilities into any application that supports SAML 2.0 for external identity providers such as AWS, Office365, Salesforce and more.

OIDC

Integrate MFA capabilities into any application that supports OIDC for external identity providers.

Radius

Integrate MFA capabilities into any application that supports Radius such as e.g. VPN providers.

REST API

Integrate MFA capabilities into your own custom web service on your application server through our REST API.

Mobile SDKs

Enable your own mobile applications to become secure authenticator devices through our SDKs for iOS and Android.

Custom Libraries

Simplify integration of MFA capabilities into your own custom web services with our handy wrapper libraries for your application servers.

Multi-Domain Support

Integrate multiple domains from the same provider (e.g. Azure AD) in our integration portal.

Integration Portal

Delploy AuthN in minutes using our Web Portal where administrators can manage users and integrations.

Authentication Destinations

Use AuthN to authenticate to almost any destination, such as to Web Applications, mobile Apps, your Servers and even to Remote Desktop Clients.

Web Application (Desktop)

Enable MFA for any web service accessed through a web browser on Desktop machines.

Web Application (Mobile)

Enable MFA for any web service accessed through a mobile web browser on smartphones.

In-app Webview (Mobile)

Enable MFA authentication for any WebView inside your mobile application.

Mobile Application

Enable MFA for any iOS, iPadOS or Android mobile application

Server (SSH)

Enable MFA to servers via SSH to secure your critical infrastructure.

VPN

Increase security of the remote access to your network by enabling MFA for VPNs.

Remote Desktop

Increase security of the remote access to Remote Desktop Clients by enabling MFA.

Blockchain

Technology evolves. That's why it's crucial to ensure that we build solutions that leverage new and upcoming technology. Our private distributed hyperledger allows you to make sure that not even your own administrators can impersonate a user, that audit trails can never be changed once written and that authentication works even in the most extreme scenarios.

Extreme Availability

Rely on authentication that's available even in the case IDEE's servers are down. Your authentications don't require us to be online.

Immutable Audit Trail

Compliance on steroids. With the immutable audit trail, manipulated or faked audit trails are simply a thing of the past.

Multi-Cloud Support

Distribute your workload and gain redundancy across clouds in different regions or with different providers.

Custom Branding Options

A coherent identity in front of your customers, users and employees is important. Our custom branding options such as the branded mobile application and the branded Self-Service Portal allow you to adapt our products to reflect your brand's corporate identity guidelines such as logo and colors.

Branded Authentication Pages

Adapt user facing authentication pages to suit your brand's corporate identity such as with your brand's colors and your brand's logo when authenticating to your web apps.

Branded Mobile Application

Stand out and adapt our mobile application to suit your brand's corporate identity such as with your own app icon, your brand's colors and your brand's logo.

Branded Self-Service Portal

Adapt user facing Self-Service portal to suit your brand's corporate identity such as with your brand's colors and your brand's logo.

Branded E-mails

Adapt user facing e-mails to suit your brand's corporate identity such as with your brand's colors and your brand's logo.

Advanced Customizations

Customization needs are different for every enterprise. For customers that want to adapt apps and services beyond logos and colors, they can.

Custom Application

Make it your own and extend the branded application beyond just logo and colors. Restrictions apply.

User Experience

Studies have shown that a great user experience makes users more productive, happier and ties them closer to your organization. Our user experience is focused on maximizing user productivity and staying ahead of the curve such as letting your users login simply by unlocking the device.

Secure App-link

Allow users to login by using an app-link. Users click on the link and unlock their phone to (e.g. using Fingerprint or Facial Recognition) to register and login.

QR-Code Login

Be on top of the user experience curve by making authentication as simple as scanning a QR code with the user's smartphone and unlocking their phone (e.g. using Fingerprint or Facial Recogni-tion).

Push Login

Allow users to login without a camera. Users receive a Push Notification on their phone and unlock it (e.g. using Fingerprint or Facial Recognition) to authenticate.

Web-AuthN Login

Allow users to login without a phone and using WebAuthn, a brand new W3C standard. The user simply unlocks their device (e.g. using Fingerprint or Facial Recognition) to authenticate.

Offline Login

Ensure availability even in areas where there is no internet connection on the smartphone with our secure Offline Login.

Secure Magic-Link Login

Provide passwordless authentication to users by simply proving possession of their mailbox. The Secure Magic-Link ensures that the person initiating the login is indeed the one logging in.

Account Transfer

Users can easily transfer their account from one authenticator device to another by simply approving a push notification.

Multi-Device Support

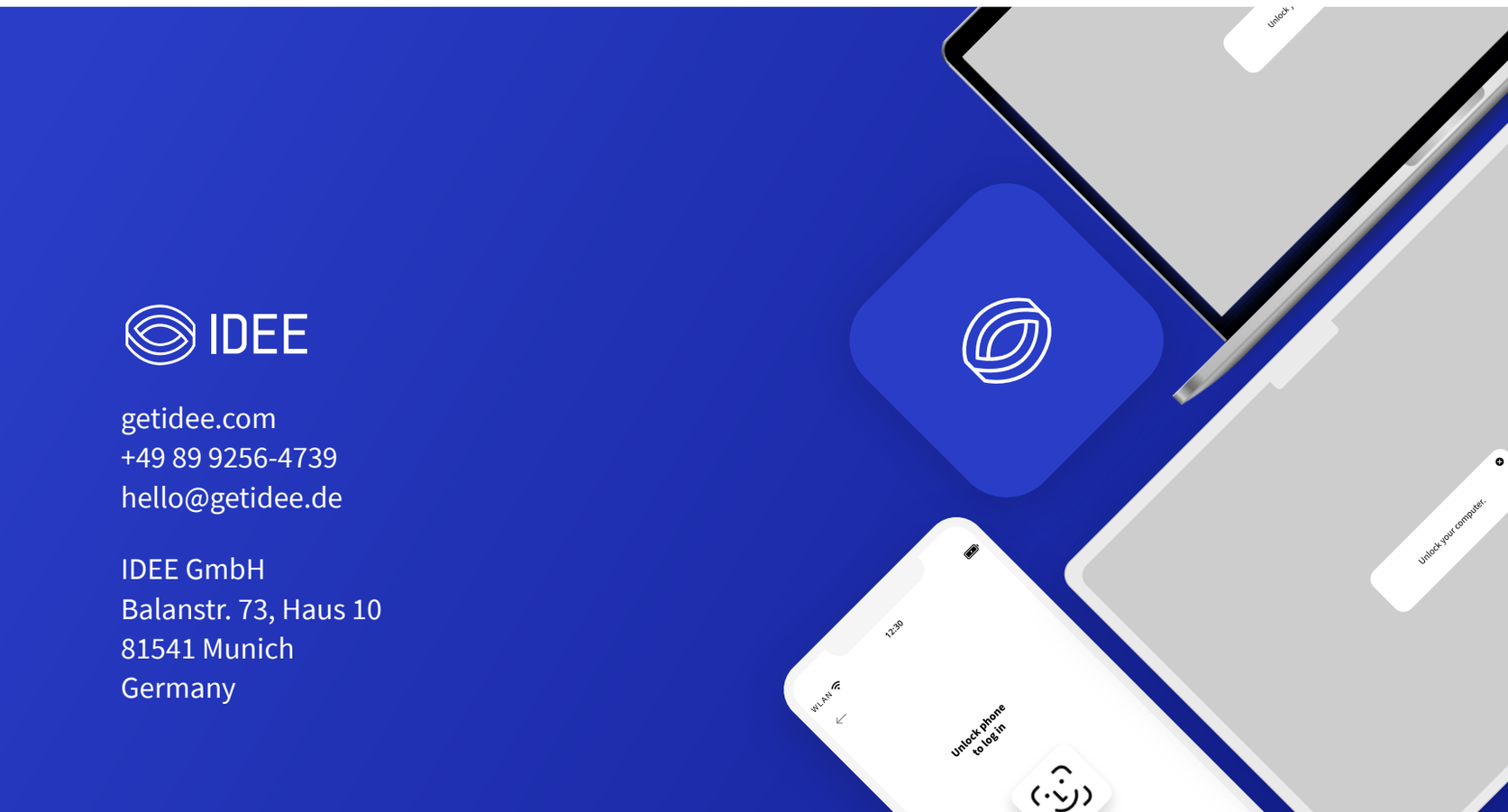
Ensure users always have the right authenticator device by enabling them to register multiple smartphones with their account.
Adding a device requires authorization from an existing device.

AuthN by IDEE

AuthN by IDEE

AuthN is the most secure MFA on the market.

It prevents all phishing and password-based attacks.



IDEE

getidee.com
+49 89 9256-4739
hello@getidee.de

IDEE GmbH
Balanstr. 73, Haus 10
81541 Munich
Germany