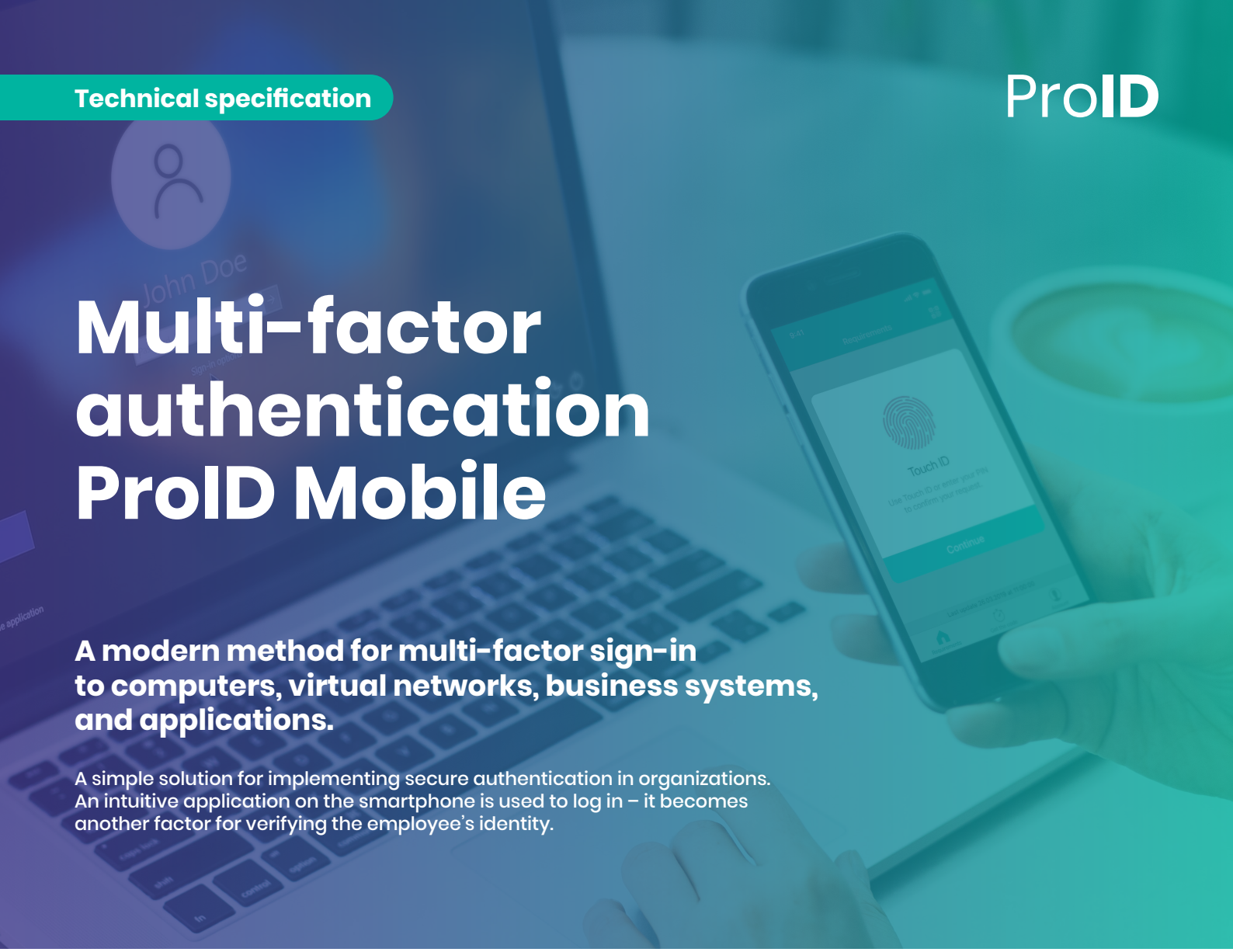
Technical specification

ProID

Multi-factor authentication ProID Mobile



A modern method for multi-factor sign-in to computers, virtual networks, business systems, and applications.

A simple solution for implementing secure authentication in organizations. An intuitive application on the smartphone is used to log in – it becomes another factor for verifying the employee's identity.

Authentication options

	Use for personal computer			Usage on your mobile phone	
	Windows OS	macOS	Linux	Android	iOS
Sign in to third-party apps (on-premise and cloud applications) *P	✓	✓	✓	✓	✓
Login to the applications you develop *P	✓	✓	✓	✓	✓
Login to applications for administrators (RADIUS)	✓	✓	✓	✓	✓
Login to VPN (RADIUS)	✓	✓	✓	✓	✓
VPN Login (PKI) *P	✓	✓	Q2/2023	–	–
Login to applications using PKI certificates *P	✓	Q1/2023	Q2/2023	–	–
Domain login to PCs and laptops *P	✓	Q1/2023	Q2/2023	–	–
Advanced Electronic Signature *P	✓	✓	✓	✓	✓

*P **Possibility to be password-less** - The method is designed to support login without passwords as much as possible. Login can be confirmed by fingerprint, face ID and other ways, depending on the specific system and device.

– **Does not allow**

ProID Mobile app

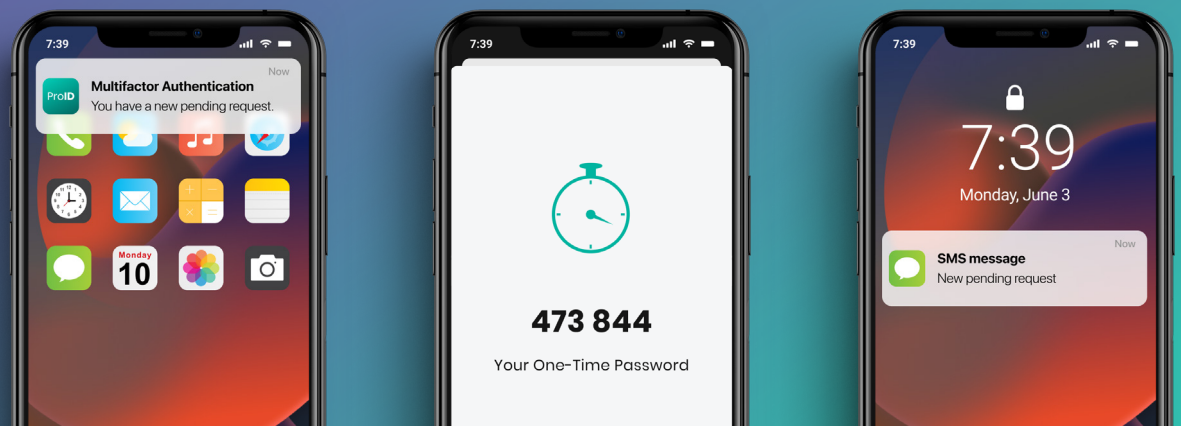
We developed the application for easy implementation of multi-factor authentication within organizations of any size and industry. Allows secure login with mobile phone authentication. It becomes a real digital key – an element without which it is impossible to enter internal systems. The app offers three independent ways.

Verification methods

Push notifications (Mobile token)
biometric data verification or 6-digit PIN

One-time password

SMS with authentication code



Security

.talsec

The application has an integrated security RASP module (Runtime Application Self-Protection), which actively protects the mobile and installed applications from attacks, monitors their security and detects malware and other threats.

The module checks the integrity of the system, biometric security, attempts to disrupt the application and many other elements.

The user's cryptographic material is stored on an external HSM module, which is part of the cloud service of the on-premise installation.

Supported methods and protocols

PKI certificates **RADIUS** **SAML2.0** **OAuth2** **OpenID Connect**

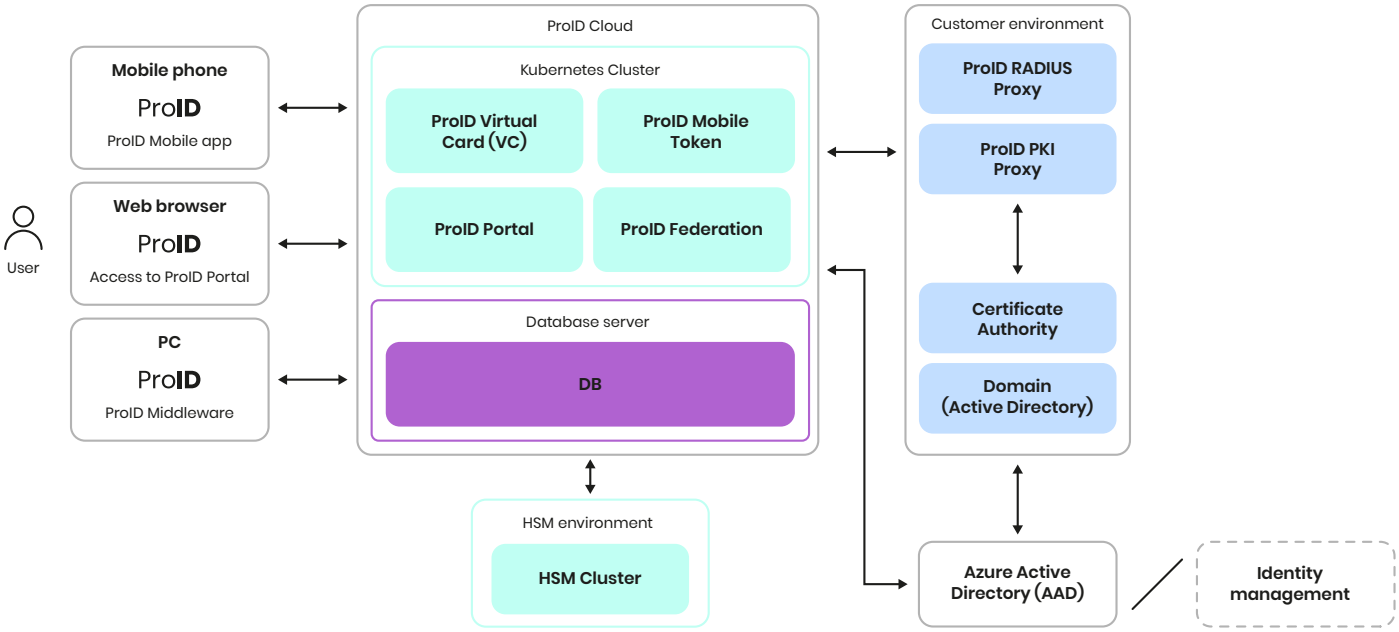
Apps for Android and iOS

*The application is fully functional after activation of the method

Download on the App Store

GET IT ON Google Play

Solution architecture



*Required components

	ProID Mobile app	ProID Middleware	ProID PKI Proxy	ProID RADIUS Proxy
Sign in to third-party apps (on-premise and cloud applications) *P	●	–	–	–
Login to the applications you develop *P	●	–	–	–
Login to applications for administrators (RADIUS)	●	–	–	●
Login to VPN (RADIUS)	●	–	–	●
VPN Login (PKI) *P	●	●	●	–
Login to applications using PKI certificates *P	●	●	●	–
Domain login to PCs and laptops *P	●	●	●	–
Advanced Electronic Signature *P	●	●	●	–

- **ProID Mobile application** – mobile application for multi-factor authentication.
- **ProID Middleware** – Provides certificate processes and communication with ProID backend systems. This application is installed on the user's PC (MSI package).
- **ProID PKI Proxy** – A Windows service that communicates with the customer's certification authority (certificate issuance) and the product's backend systems.
- **ProID RADIUS Proxy** – A Windows service that communicates with the on-premise RADIUS server and backend systems of the product. ProID RADIUS Proxy can also be used as a custom RADIUS server.

User identity source

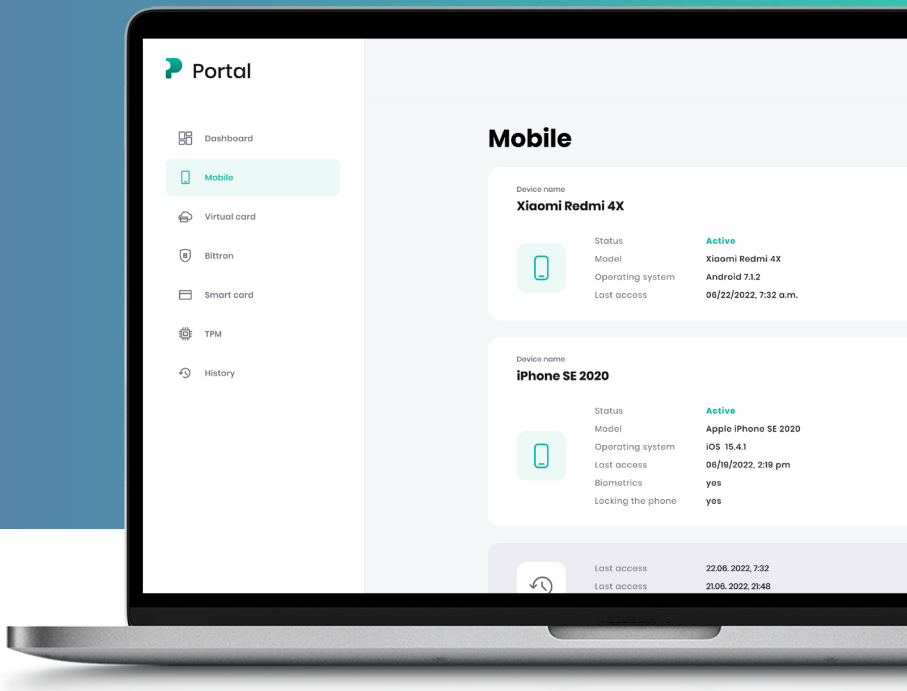
- Microsoft Azure Active Directory
- Connector for external IAM systems (using LDAP)

Availability and technical support

- High availability (geo cluster)
- 24/7 support

ProID Portal

Web interface for both users
and administrators of organizations.
It allows easy management
of certificates and mobile phones.
The portal is multitenant
and offers a number of features
for administrators of organizations.



Possibilities of solution deployment

Cloud service (SaaS)

- Cloud multitenant service with licensing according to the number of users per calendar month.
- Hosted on Azure Kubernetes Service (AKS) - an architecture that uses the orchestration of microservices in Docker containers (the data centre is located in Frankfurt am Main).
- User's cryptographic secret stored in certified nCipher nShield Connect XC **HSM modules** supporting HA geocluster (meets certification: eIDAS / Common Criteria EAL4+ AVA_VAN.5 and ALC_ FLR.2on Protection Profile EN 419 221-5, published as QSCD on FIPS sheet 140-2 Level 3).
- Certificates for PKI scenarios are generated by the customer's certification authority (CA). The ProID PKI Proxy module is used for communication with the CA.
- For applications and VPNs supporting the RADIUS protocol, you can use an existing RADIUS server (Network Policy Server – NPS, Radiator, etc.). The Radius Proxy ProID module is used for communication.

On-premise deployment

- Standard license for the provided solution with the possibility of maintenance and SLA.
- Deployment of the ProID platform and all modules in the customer's on-premise environment.
- The virtualization platform must support Kubernetes clustering (VMware, RedHat OpenShift, and so on).
- Support for Microsoft SQL Server and PostgreSQL databases.

Supported apps

ATLASSIAN · salesforce · Microsoft 365 · CHECK POINT YOU DESERVE THE BEST SECURITY · G

VPN · f5 · CISCO · FORTINET · a další...

Are you interested
in our solution?

Contact Us

info@proid.tech
www.proid.tech