Technická specifikace

ProID

Vícefaktorová autentizace ProID Mobile

Moderní metoda pro vícefaktorové přihlášení do počítačů, virtuálních sítí, firemních systémů a aplikací.

Jednoduché řešení pro zavedení bezpečné autentizace v organizacích. K přihlášení slouží intuitivní aplikace v chytrém telefonu – ta se stává dalším faktorem pro ověření identity zaměstnance.

Možnosti autentizace

	Využití pro osobní počítač			Využití v mobilním telefonu	
	Windows OS	macOS	Linux	Android	iOS
Přihlášení do aplikací třetích stran (on-premise i cloudové aplikace) *P	✓	✓	✓	✓	✓
Přihlášení do vámi vyvíjených aplikací *P	✓	✓	✓	✓	✓
Přihlášení do aplikací pro administrátory (RADIUS)	✓	✓	✓	✓	✓
Přihlášení do VPN (RADIUS)	✓	✓	✓	✓	✓
Přihlášení do VPN (PKI) *P	✓	✓	Q2/2023	–	–
Přihlášení do aplikací využívající PKI certifikáty *P	✓	Q1/2023	Q2/2023	–	–
Doménové přihlášení do PC a notebooků *P	✓	Q1/2023	Q2/2023	–	–
Zaručený elektronický podpis *P	✓	✓	✓	✓	✓

*P **Lze i passwordless** - Metoda je navržena tak, aby maximálně podporovala přihlašování bez hesel. Přihlášení je možné potvrdit otiskem prstu, face ID a dalšími způsoby, v závislosti na konkrétním systému a zařízení.

– **Neumožňuje**

Aplikace ProID Mobile

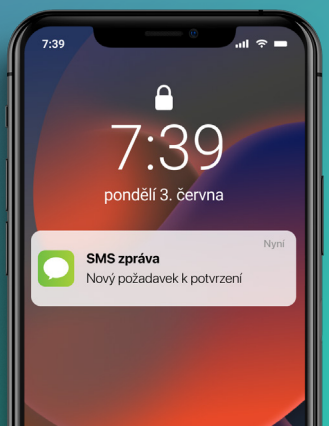
Aplikaci jsme vyvinuli pro snadné zavedení vícefaktorové autentizace uvnitř organizací jakékoliv velikosti a oboru. Umožňuje bezpečné přihlášení s ověřením v mobilním telefonu. Ten se stává skutečným digitálním klíčem – prvkem, bez kterého se nedá vstoupit do vnitřních systémů. Aplikace nabízí tři nezávislé způsoby.

Způsoby ověření

Push notifikace (mobilní token)
ověření biometrických údajů nebo 6 místný PIN

Jednorázové heslo (one-time password)

SMS s autentizačním kódem



Zabezpečení

talsec

Aplikace má integrovaný bezpečností RASP modul (Runtime Application Self-Protection), který aktivně chrání mobil a nainstalované aplikace před útoky, monitoruje jejich zabezpečení a detekuje malware i další hrozby.

Modul kontroluje integritu systému, zabezpečení biometriky, pokusy o narušení aplikace a mnoho dalších prvků.

Kryptografický materiál uživatele je uložen na externím HSM modulu, který je součástí cloudové služby i instalace on-premise.

Podporované metody a protokoly

PKI certifikáty | RADIUS | SAML2.0 | OAuth2 | OpenID Connect

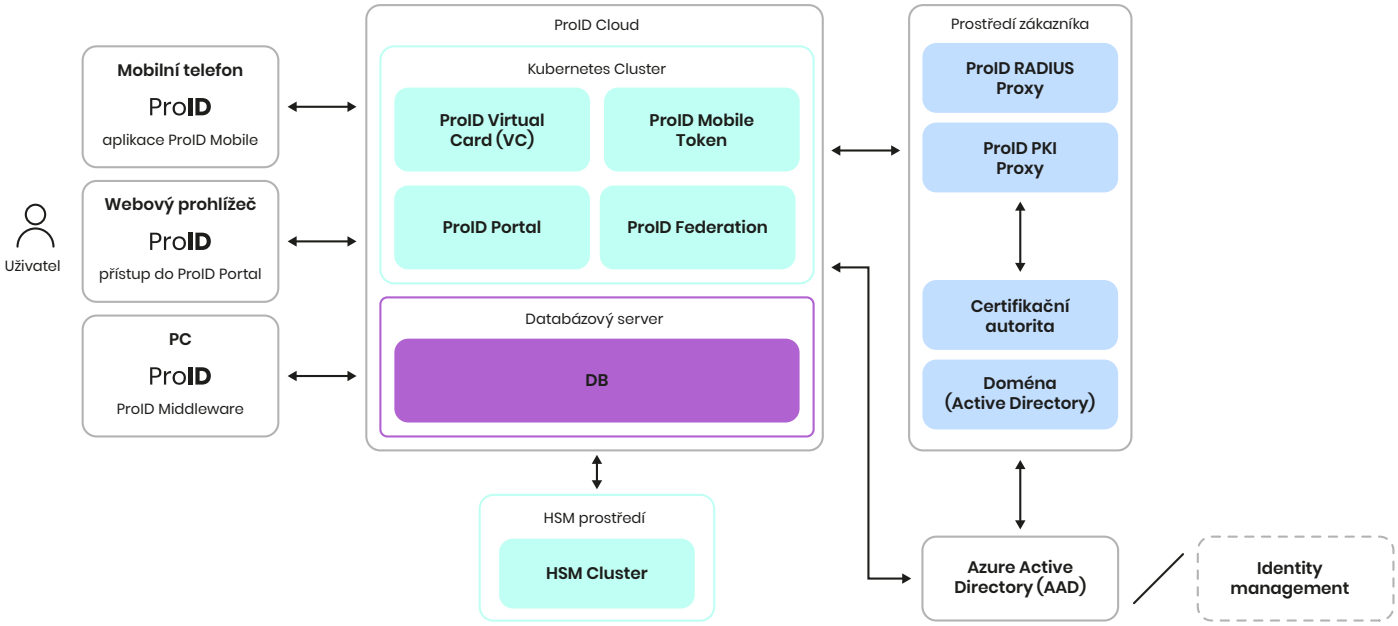
Aplikace pro Android i iOS

*Aplikace je plně funkční po aktivaci celé metody

Download on the App Store

GET IT ON Google Play

Architektura řešení



*Potřebné komponenty

	Aplikace ProID Mobile	ProID Middleware	ProID PKI Proxy	ProID RADIUS Proxy
Přihlášení do aplikací třetích stran (on-premise i cloudové aplikace) *P	●	–	–	–
Přihlášení do vámi vyvíjených aplikací *P	●	–	–	–
Přihlášení do aplikací pro administrátory (RADIUS)	●	–	–	●
Přihlášení do VPN (RADIUS)	●	–	–	●
Přihlášení do VPN (PKI) *P	●	●	●	–
Přihlášení do aplikací využívající PKI certifikáty *P	●	●	●	–
Doménové přihlášení do PC a notebooků *P	●	●	●	–
Zaručený elektronický podpis *P	●	●	●	–

- **Aplikace ProID Mobile** – mobilní aplikace pro vícefaktorovou autentizaci.
- **ProID Middleware** – zajišťuje procesy s certifikáty a komunikaci s backendovými systémy ProID. Tato aplikace se instaluje do PC uživatele (MSI balíček).
- **ProID PKI Proxy** – Windows služba, která komunikuje s certifikační autoritou zákazníka (vydání certifikátu) a backendovými systémy produktu.
- **ProID RADIUS Proxy** – Windows služba, která komunikuje s on-premise RADIUS serverem a backendovými systémy produktu. ProID RADIUS Proxy lze také využít jako vlastní RADIUS server.

Zdroj identit uživatelů

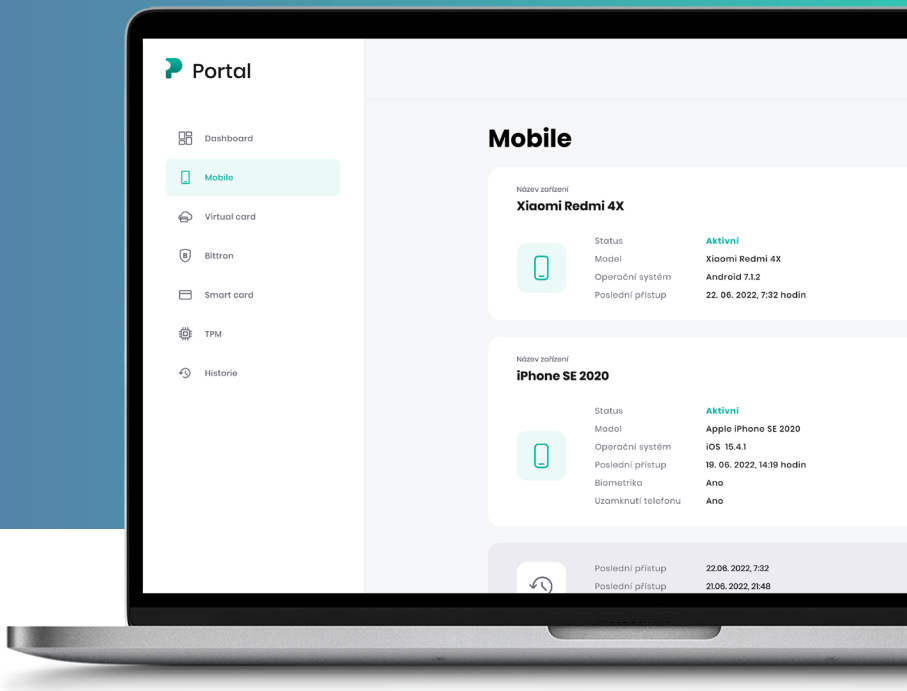
- Microsoft Azure Active Directory
- Konektor pro externí IAM systémy (pomocí LDAP)

Dostupnost a technická podpora

- Vysoká dostupnost (geocluster)
- Podpora 24/7

ProID Portal

Webové rozhraní pro uživatele i správce organizací. Umožňuje jednoduchou správu certifikátů a mobilních telefonů. Portál je multitenantní a nabízí řadu funkcí pro administrátory organizací.



Možnosti nasazení řešení

Cloudová služba (SaaS)

- Cloudová multitenantní služba s licencováním dle počtu uživatelů za kalendářní měsíc.
- Hostováno na Azure Kubernetes Service (AKS) – architektura, která používá orchestrizaci mikroslužeb v Docker kontejnerech (datové centrum je umístěno ve Frankfurtu nad Mohanem).
- Krytografické tajemství uživatele uloženo v certifikovaných **HSM modulech** nCipher nShield Connect XC podporující HA geocluster (splňuje certifikace: eIDAS / Common Criteria EAL4+ AVA_VAN.5 and ALC_ FLR.2 na Protection Profile EN 419 221-5, zveřejněno jako QSCD na listu FIPS 140-2 Level 3).
- Certifikáty pro PKI scénáře jsou generovány certifikační autoritou (CA) zákazníka. Pro komunikaci s CA se používá ProID PKI Proxy modul.
- Pro aplikace a VPN podporující RADIUS protokol lze využít stávající RADIUS server (Network Policy Server – NPS, Radiator a podobně). Pro komunikaci se používá modul ProID RADIUS Proxy.

On-premise nasazení

- Standardní licence za poskytnuté řešení s možností maintenance a SLA.
- Nasazení platformy ProID a všech modulů v on-premise prostředí zákazníka.
- Virtualizační platforma musí podporovat Kubernetes clustering (VMware, RedHat OpenShift a podobně).
- Podpora databází Microsoft SQL Server a PostgreSQL.

Podporované aplikace

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

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

Zaujalo vás naše řešení?

Kontaktujte nás

info@proid.cz
www.proid.cz