



ProID

Ochrana prístupov do systémov a dát organizácie

Ing. Richard Reichert
Obchodný manažér

Monet+

29

rokov na trhu

350+

zákazníků

350+

špičkových odborníků

1 MISSION

Digitally move
identities and money

8

business řešení

€ 23 million

tržby v roku 2023

20+

krajín vo svete

**Najzraniteľnejší článok
organizácie?**

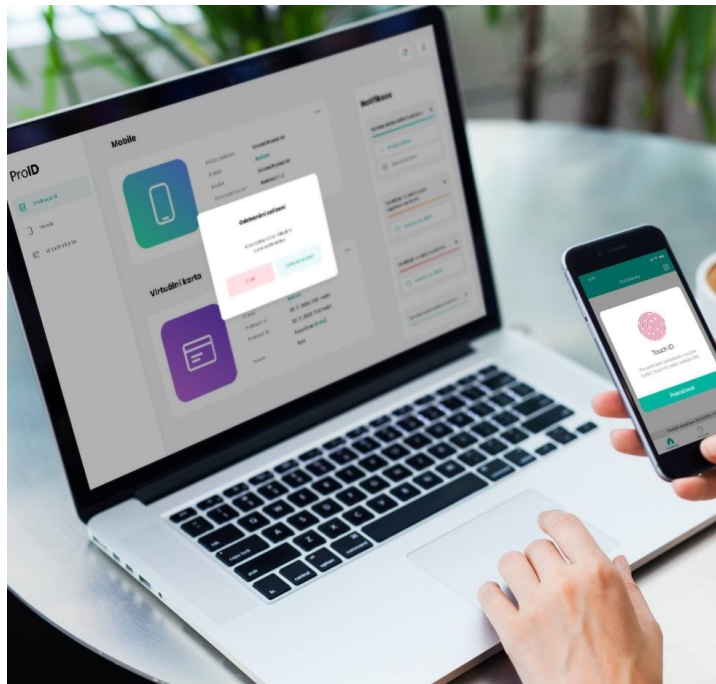
Zamestnanec.

A person wearing a dark hoodie is shown from the chest up, hunched over a laptop. The scene is dimly lit with a strong blue light source, likely the laptop screen, which casts a glow on the person's face and the surrounding environment. The background is dark and out of focus.

80 %

**Úspešných kyber útokov je
prostredníctvom prelomenej
identity zamestnanca**

Najčastejšie spôsoby prelomenia účtov



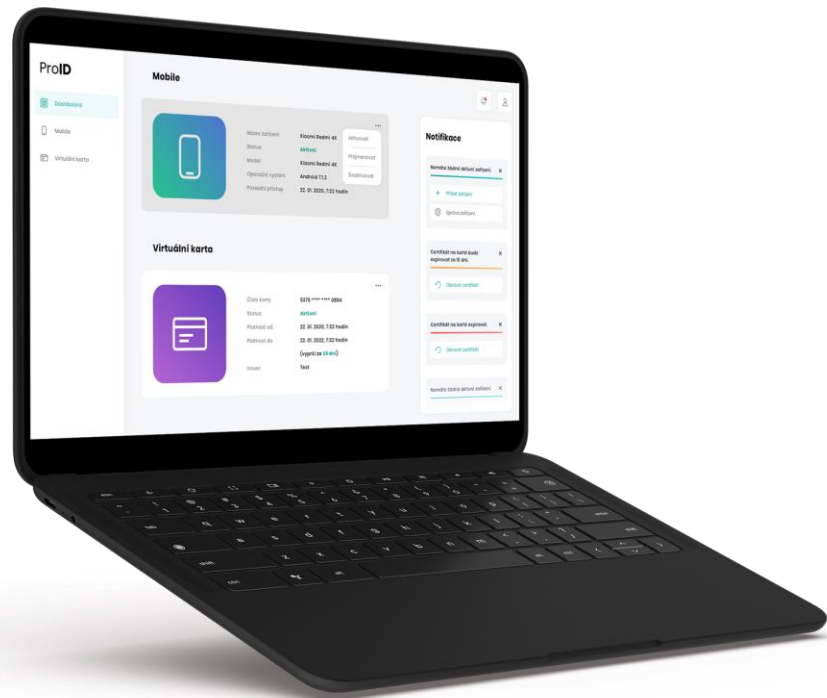
- Slabé, ľahko odhadnuteľné heslo
- Pripojenie cez nezabezpečenú WiFi
- Jedno heslo všade (práca i súkromie)
- Nechcené predanie hesla útočníkom
- Zámerné predanie údajov útočníkom

Reakcia?

Politika strašidelných hesiel.

pX3!qR7zW\$v9mK2yT&b1
dJ8#kL2xZ%t6nG9aP!w4m
vC5\$bN9hY&u3jM6eS#z8p
fG1!sH4rT@o7iD3cW\$x9nE5j

Prečo je politika strašidelných hesiel zlé riešenie?



- Častá frekvencia obmeny
- Nekomfort pre užívateľov
- Zvýšená záťaž pre IT
- Obchádzanie pravidiel
- Falošný pocit bezpečia

Skutočné riešenie?



Multifaktorová autentizácia

- Kombinácia aspoň 2 na sebe nezávislých faktorov identifikácie
- Nahradzuje / odstraňuje používanie hesiel
- Poskytuje bezpečný a šifrovaný prístup k firemným dátam
- Najčastejšie má formu HW tokenu s hodnotou PIN alebo mobilnej aplikácie a biometriky

Scenáre využitia MFA

Prihlásenie do OS



VPN a vzdialený prístup



Aplikácie tretích strán



Aplikácie pre administrátorov



Základné otázky pred zavedením MFA

10 základných otázok pred zavedením MFA

1. Koľko užívateľov v organizácii bude využívať tento spôsob autentizácie?
2. Sú pracovné stanice v spoločnej doméne?
3. Čo je v procese autentizácie užívateľov zdrojom identít?
4. Na ktoré scenáre chceme MFA uplatniť? (OS, VPN, Cloud)
5. Chceme systém doplniť aj o fyzickú identifikáciu a ovládanie prístrojov?
6. Má byť súčasťou riešenia aj elektronický podpis?
7. Má koncové riešenie spĺňa určitú normu alebo štandard?
8. V akom stave je naša tzv. infraštruktúra verejných kľúčov (PKI)?
9. Chceme riešenie on-premise alebo ako cloudovú službu?
10. Má byť autentizácia funkčná aj v režime offline?



Postup zavedenie MFA

- Analýza súčasného stavu
- Definícia konkrétnych scenárov využitia
- Prieskum trhu
- Pilotný projekt pre určitú skupinu užívateľov
- Následná celoplošná implementácia
- Postupný rozvoj a pokrývanie širšieho spektra užívateľským scenárov

Platforma ProID ako unifikované riešenie

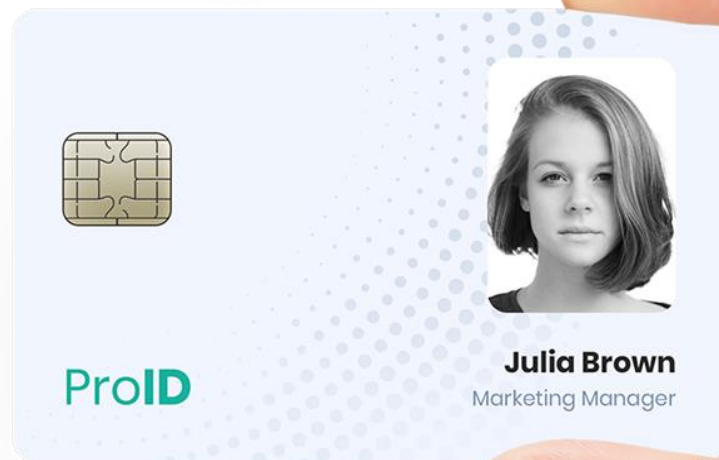
Hybridná čipová karta ProID



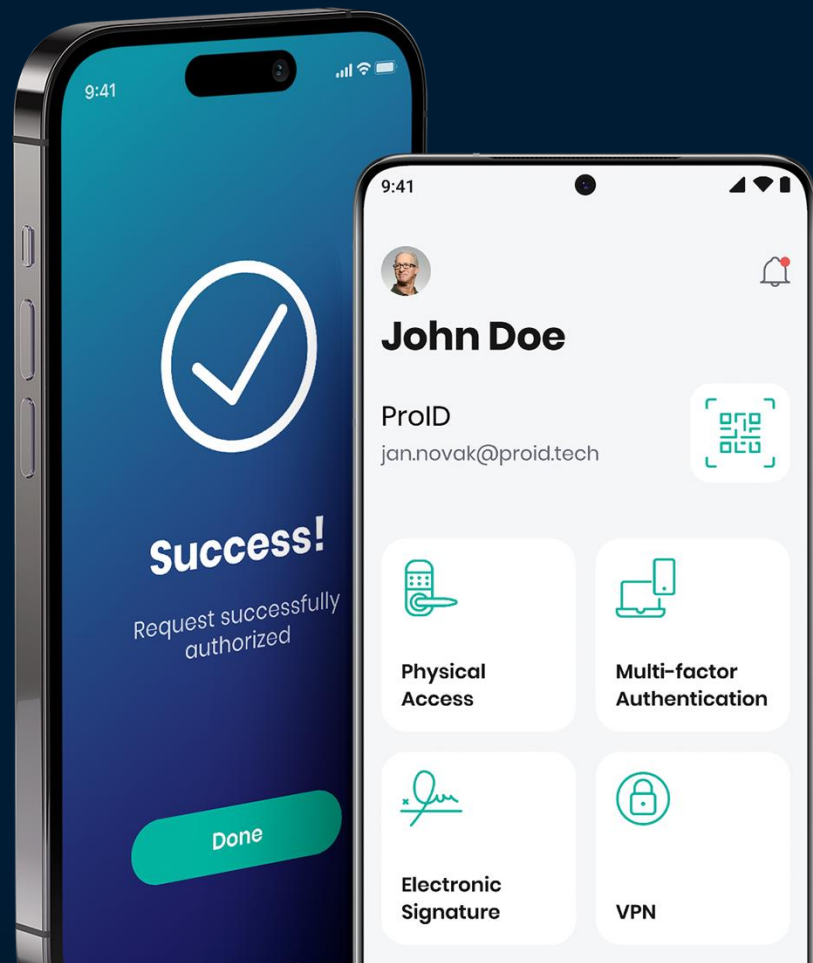
Hybridná čipová karta ProID

Jedna karta obslúži:

1. Multifaktorová autentizácia
 - a. Operačný systém
 - b. Vzdialený prístup (VPN / RDP)
 - c. Aplikácie 3. strán
2. Elektronický podpis
 - a. jednoduchý
 - b. kvalifikovaný
3. Bezkontaktné scenáre
 - a. fyzický prístup do priestorov
 - b. evidencia dochádzky
 - c. ovládanie tlačiarň atď.
4. Vizuálna identifikácia

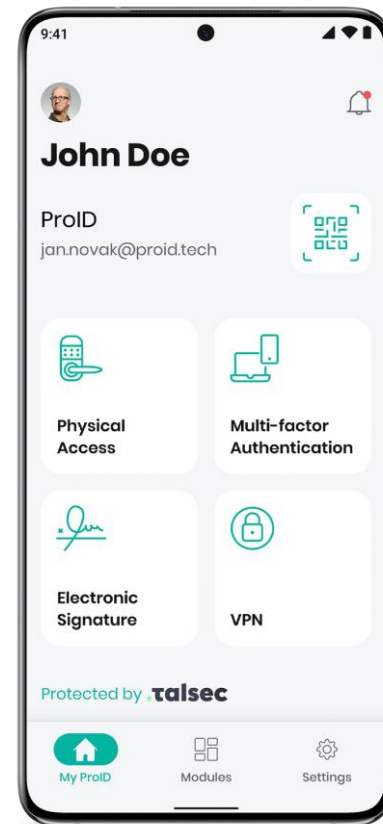


ProID Mobile



MFA mobilným telefónom

- *Ultra bezpečné prihlasovanie* **biometrikou bez použitia hesla** *do:*
 - *Operačný systém*
 - *Vzdialený prístup (VPN / RDP)*
 - *Administrátorské aplikácie*
 - *Kancelárske aplikácie*
- *Poskytujeme ako cloudovú službu*
- *Vlastný produkt spoločnosti MONET+*



Richard Reichert

Sales Manager

rreichert@monetplus.cz

+420 793 924 905

proid.cz | monetplus.cz