ProID

Zavedení dvoufázové autentizace a kryptografie pro NIS 2

Petr Ciprys
ProID by Monet+

solutions by MONET +

MONET+ v číslech

25 *LET*

130 *ZÁKAZNÍKŮ*

250+ *PROFESIONÁLŮ*

1 MISSION

To create a trusted digital world

5 *OBCHONÍCH ZAMĚŘENÍ*

390 **mil.** *OBRAT 2020*

15 *ZEMÍ*

solutions by **MONET+**

Směrnice na mnoha místech zmiňuje zavedení technických řešení, zejména **šifrování**, **dvoufázového ověření** a **řízení identit a přístupů**.

Bezpečnost “na papíře” je pouze falešný pocit.
Skutečnou bezpečnost zajistí technické řešení!

NIS 2

80 %

úspěšných hackerských útoků je způsobeno prolomením přihlašovacích údajů a slabých hesel

solutions by MONET +

Jaké normy/zákony musí organizace splnit?

- *Zákon o kybernetické bezpečnosti*
  či vyhlášku o kritické infrastruktuře
- *Evropské nařízení eIDAS (elektronický podpis apod.)*
- *Nařízení a varování NÚKIB*
- *ISO normy 27000 či TISAX (pro automotive)*
- *Ochrana citlivých dat dle GDPR*
- *…a mnoho dalších*

10 nejdůležitějších témat NIS2

1. Analýza rizik a politiky bezpečnosti informací;
2. Zvládání incidentů;
3. Kontinuita činností (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
4. Bezpečnost v rámci dodavatelského řetězce;
5. Bezpečnost v rámci pořízení, vývoje a údržby systémů;
6. Politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (tj. audit);
7. Praktiky základní počítačové hygieny a vzdělávání v oblasti kybernetické bezpečnosti;
8. Politiky a postupy týkající se **využívání kryptografie** a tam, kde je to vhodné, **také šifrování;**
9. **Bezpečnost lidských zdrojů**, řízení přístupů a aktiv;
10. Využívání **vícefaktorového ověření identity**, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci.

Zdroj: https://osveta.nukib.cz/mod/page/view.php?id=2618

Digitální ekosystém organizace

Technologické prvky infrastruktury

Uživatelská oprávnění a akce

Zabezpečení identity uživatele

solutions by MONET+

Vybrané části směrnice:

odst. 79

"Subjekty by měly v rámci svých opatření k řízení kybernetických bezpečnostních rizik zabývat rovněž bezpečností lidských zdrojů a **zavést vhodné politiky kontroly přístupu**."

odst. 89

"Subjekty by měly přijmout širokou škálu základních postupů v oblasti kybernetické hygieny, k nimž patří **architektura nulové důvěry**, … , **řízení identity a přístupu.**"

článek 21, odst. 2 (i)

"… **postupy kontroly přístupu a správu aktiv**

článek 21, odst. 2 (j)

"…. používání **vícefaktorových autentizačních řešení** nebo trvalých autentizačních řešení"

Možnosti ověření uživatele

Vícefaktorové přihlášení nahrazuje používání uživatelského jména a hesla
nástroji pro bezpečné, šifrované přihlášení s přidáním dalšího faktoru - biometrika, PIN apod.

Jméno / Heslo

Snadné prolomení
či zcizení

Jméno / Heslo
+ další faktor (ProID)

Doplnění o bezpečnostní
prvek

Passwordless
(ProID)

Nejvyšší stupeň
zabezpečení

solutions by **MONET +**

Zabezpečení identity uživatele

Logická identita

Fyzická identita

Identifikace zaměstnance

Přihlášení do PC

Přihlášení do aplikací

Přihlášení do VPN

Přistup do Souborů a dat

Elektronický podpis

Šifrování komunikace

Přístup do prostor

Ovládání přístrojů

Evidence Obědů, docházky atd.

Základní potřeby organizace

Flexibilita, Univerzálnost použití

Bezpečné uživatelské nástroje

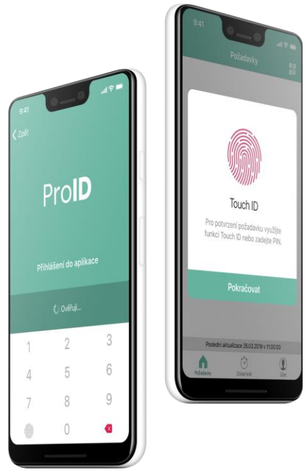
Rozhraní pro správce

Jednoduché nasazení

Nástroje pro vícefaktorové ověření

Čipové karty ProID

Multifunkční karta pro bezpečnou identitu, ochranu prostor, dvoufaktorová autentizace v jednom řešení.

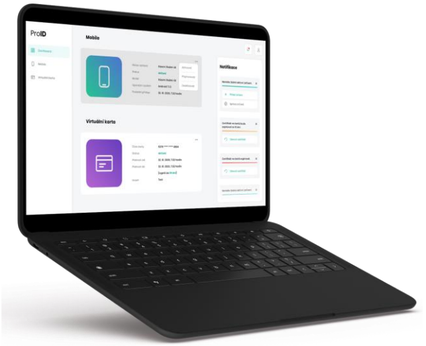


Mobilní aplikace ProID Mobile

Přihlášení do počítačů a systémů s multifaktorovou autentizací pomocí mobilního zařízení. Nejmodernější způsob řešení pracovní identity se snadnou správou.

USB token s mobilní aplikací

Přihlášení do počítačů a multifaktorová autentizace pomocí USB klíče a mobilní aplikace.



Autentizace pomocí TPM čipu

Přihlášení do počítačů a aplikací pomocí integrovaného TPM v počítačích. Nejdosažitelnější způsob zvýšení uživatelské bezpečnosti.

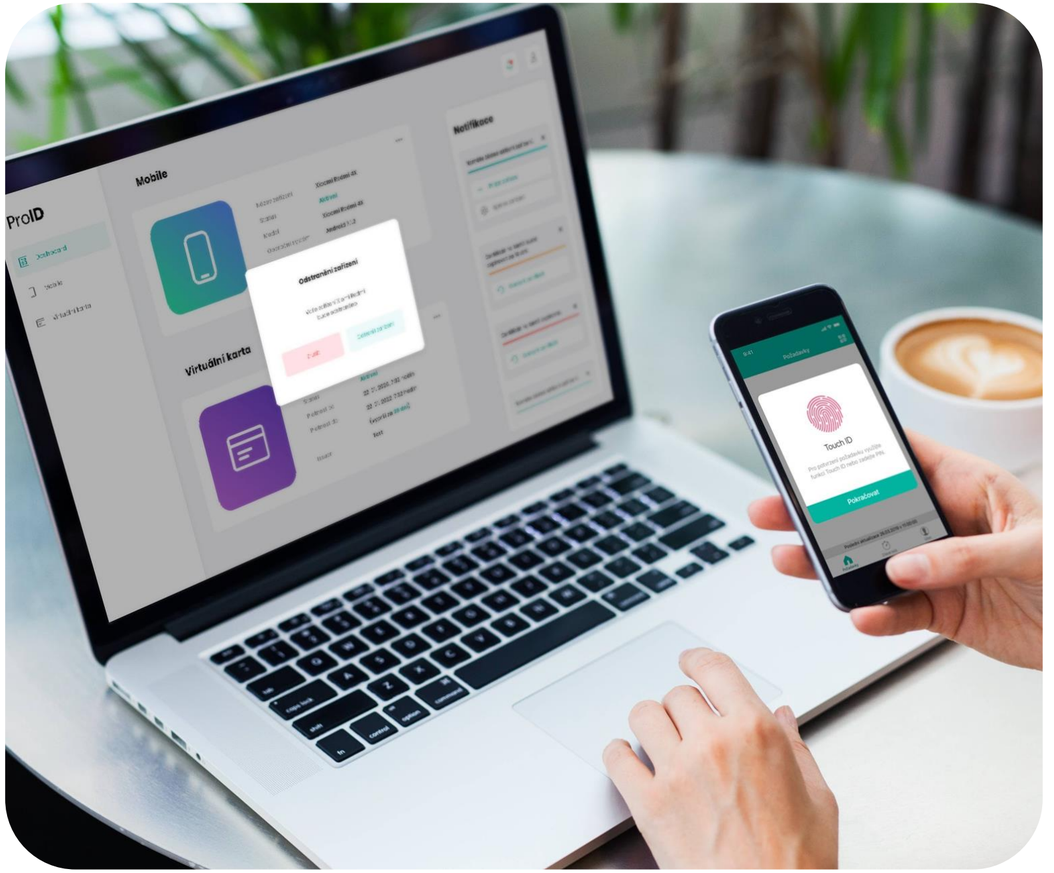
Čipové karty ProID a USB tokeny

- Silná (vícefaktorová) autentizace do počítačů
- Šifrované přihlášení do VPN (externisté)
- Kvalifikovaný elektronický podpis - eIDAS
- Přihlášení do ostatních systémů a aplikací
- Šifrování komunikace a zaslaných dokumentů
- Zaměstnanecký průkaz - vizuální identifikace
- Identifikace v bezkontaktním systému

solutions by **MONET+**

Autentizace smartphonem - ProID Mobile

- Řešení pro vícefaktorovou autentizace pomocí mobilního telefonu
- Silná autentizace pomocí PKI nebo standardizované protokoly
- Push notifikace, OTP, SMS
- Integrovaný systém na vyhodnocování nebezpečí Talsec.app
- Použití jako cloudová služba nebo on-premise řešení
- Hybridní varianta TOTP



Windows macOS® VPN Microsoft 365 CHECK POINT YOU DESERVE THE BEST SECURITY f5 CISCO ATLASSIAN Experts & Solutions Partners FORTINET + další

solutions by MONET +

Bezpečnostní USB token s mobilní aplikací – Bittron

Propojení HW tokenu s mobilem a znalostí tajemství

- *Autentizační token s integrovanou kartou = stejné možnosti jako čipová karta*
- *Mobilní aplikace zajišťuje přítomnost dalšího faktoru*
- *Aplikační párování Bittron – Mobilní aplikace a podporuje iOS a Android*
- *Podporuje SPE (ověření PIN, změna PIN, odblokování, inicializace)*
- *Podporuje FIDO2 s ověřením uživatele pomocí PIN na telefonu (samostatný PIN, nezávislý na PIN karty)*
- *Middleware podporuje systémy MS Windows a MacOS*
- *Tělo obsahuje tlačítko pro spárování a diodu pro indikaci připojení*

solutions by MONET+

Zavedení kryptografie

Vybrané části směrnice:

odst. 98

"... používání šifrovacích technologií, zejména **šifrování mezi koncovými body**"

článek 21, odst. 2 (h)

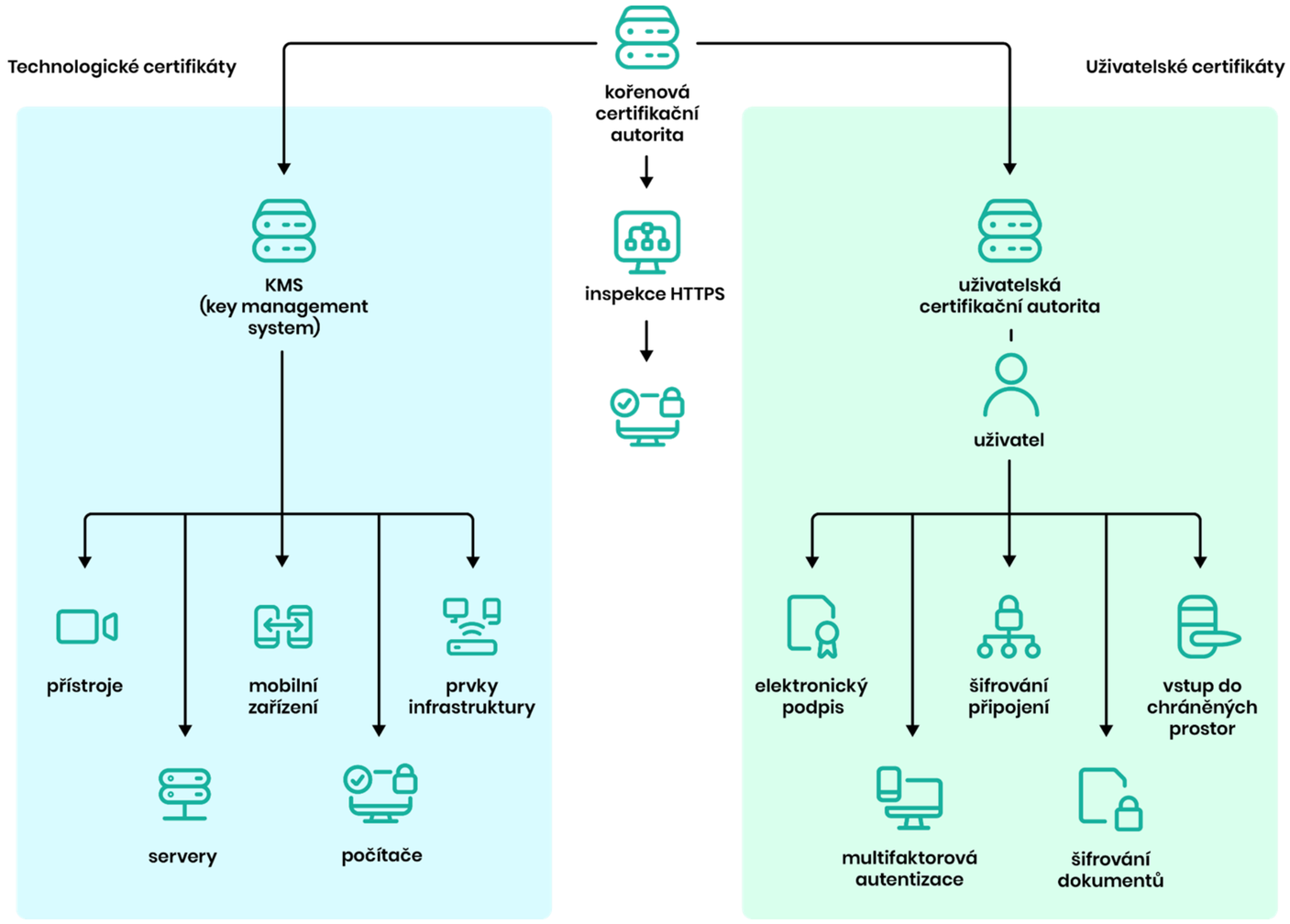
“.... politiky a postupy týkající se **používání kryptografie a případně šifrování**;”

Kryptografie v praktickém použití

- Zabrání odposlechu a falšování dat, ale především průniku do vnitřního perimetru organizace.
  - Autentizace přístupu
  - Šifrování (komunikace, emaily, disky…)
  - Integrita zpráv/Neměnnost
  - Nepopiratelnost - el. podepisování
- Využívá digitální certifikáty a klíče (privátní či veřejné)
- Práce s kryptografickým materiálem zajišťuje Certifikační autorita, PKI infrastruktura a HSM.
- Neustálý vývoj: RSA / ECC / Postkvantová kryptografie

Public Key Infrastructure (PKI) - vnitřní důvěra

PKI - Správa a distribuce bezpečnostních certifikátů a kryptografických klíčů.



- Návrh a výstavba PKI
- Analýza stávající PKI
- Bezpečné uložení klíčů v HSM
- Správa šablon certifikátů
- Dokumentace
  - Havarijní
  - Bezpečnostní
  - Provozní
  - A další

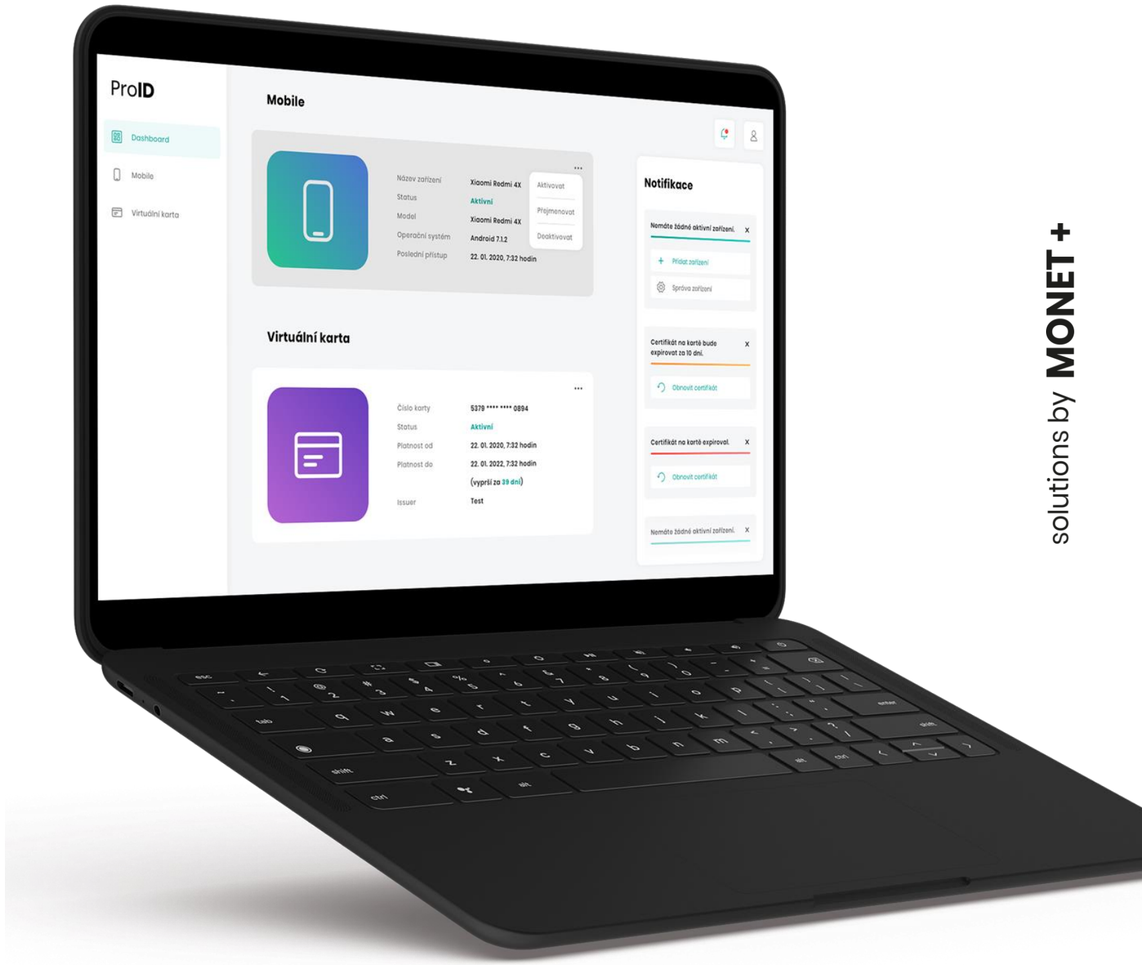
solutions by **MONET +**

Moduly pro správu digitálních klíčů a certifikátů

- Poskytují aplikační podporu pro správce organizace
- Automatizují složité procesy, pracují v reálném čase

Umožňují důležité operace:

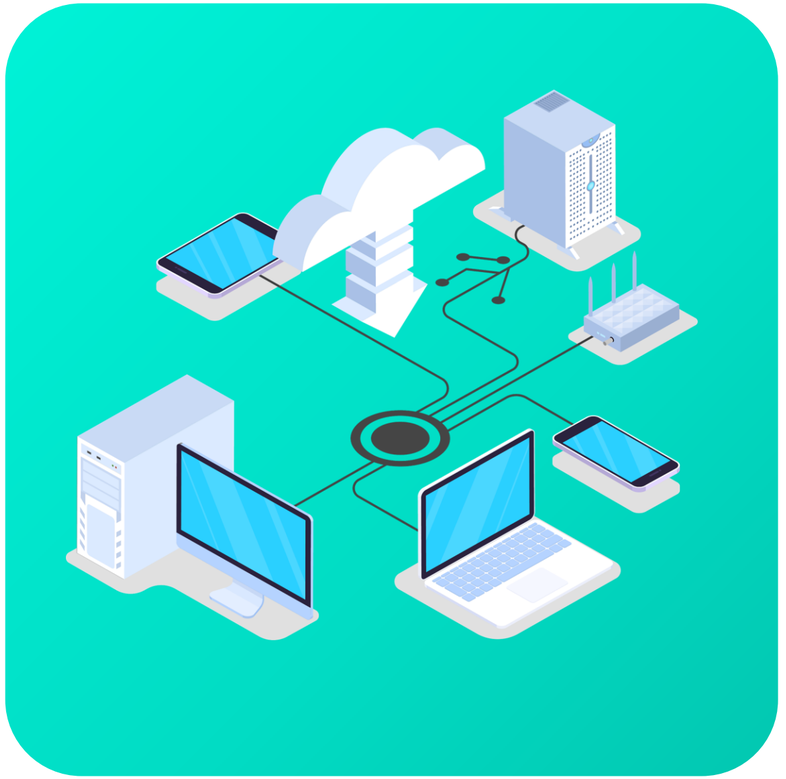
- Evidenci dat o uživatelích, autentizačních nástrojích a certifikátech (včetně blokace či obnovy)
- Automatizovanou obnovu certifikátů a jejich vydávání
- Notifikace o expiraci certifikátů
- Agregace dat o bezpečnostních hrozbách
- Rozsáhlý datamining, zálohování a centrální správu



solutions by **MONET +**

Šifrování komunikace koncových bodů

- Je řešeno tzv. **KMS** (Key Management System)
- Bezpečná distribuce klíčů a certifikátů mezi koncovými body
- Automatizovaná správa životního cyklu certifikátů a klíčů
- Eliminace výpadků při expiraci
- Minimalizace nutných manuálních zásahů adminem



Fyzické servery

Virtuální servery

Prvky infrastruktury

Mobilní zařízení

Prvky IoT

Lékařské přístroje

Smart Metering

solutions by **MONET+**

Reference

solutions by MONET+

Děkuji!

Petr Ciprys
Business Development Manager

pciprys@monetplus.cz
+420 774 831 507
www.proid.cz