



ProID

Bezpečná pracovní identita zdravotníka

Michaela Lehká

Závěr roku patřil hackerům. Globální průšvih má prapůvod v Brně

Ekonom.cz | 7. 1.

Závěr již tak složitého a divokého loňského roku dostal další ránu. Hackerům se podařilo využít softwarových zranitelností v rámci aplikací...



Kyberzločinci využívají v ČR pandemie k intenzivnějším útokům na klíčové instituce

22. 4. 2020

Kyberzločin v průběhu koronavirové pandemie nabírá na intenzitě. Útočníci podvodnými emaily využívají strachu ve společnosti k šíření virů či...



Hackeri napadli informační systémy městské části Prahy 3 a Povodí Vltavy

🕒 7. dubna 2020

V úterý napadli hackeri informační systémy městské části Prahy 3 i státního podniku Povodí Vltavy....

Masivní kybernetický útok. Systém veřejné správy napadli ve čtvrtek hackeri

5.3.2021 | AKTUALIZOVÁNO 5.3.2021

ČTK



Systém veřejné správy napadli ve čtvrtek hackeri. O masivním kybernetickém útoku informuje na twitteru pražský primátor Zdeněk Hřib

Útok na Nemocnici Benešov způsobil škodu 59 milionů korun, pachatel se nenašel

18.8.2020 | AKTU



Zdeněk K



OKD přerušila těžbu ve všech dolech, čelí útoku hackerů

🕒 aktualizováno 23. prosince 2019

Společnost OKD z bezpečnostních důvodů okamžitě přerušila těžbu ve všech svých dolech. Důvodem je...



Další útok hackerů. Napadli nemocnici dlouhodobě nemocných, policie případ vyšetřuje

Podle zjištění Aktuálně.cz napadli hackeri Nemocnici následné péče v Horažďovicích na Plzeňsku, nemocnice hospitalizuje 1100 lidí.



Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty

Fakultní nemocnice v Brně Bohunicích, která prověřuje testy na koronavirus, čelí kybernetickému útoku. Odloženy jsou všechny...

13.3.2020 7:21 Brno



Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve

🕒 17. dubna 2020

Fakultní nemocnici Brno vznikla při březnovém kybernetickém útoku škoda v desítkách milionů korun....

NIS 2 – Nová povinná strategie ochrany

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.

Kdo další vyžaduje zavedení bezpečné digitální identity?



- Zákon o kybernetické bezpečnosti.
- Evropské nařízení eIDAS (elektronický podpis apod.).
- ISO normy (27001 a další).
- GDPR (ochrana citlivých dat).
- ...a mnoho dalších.

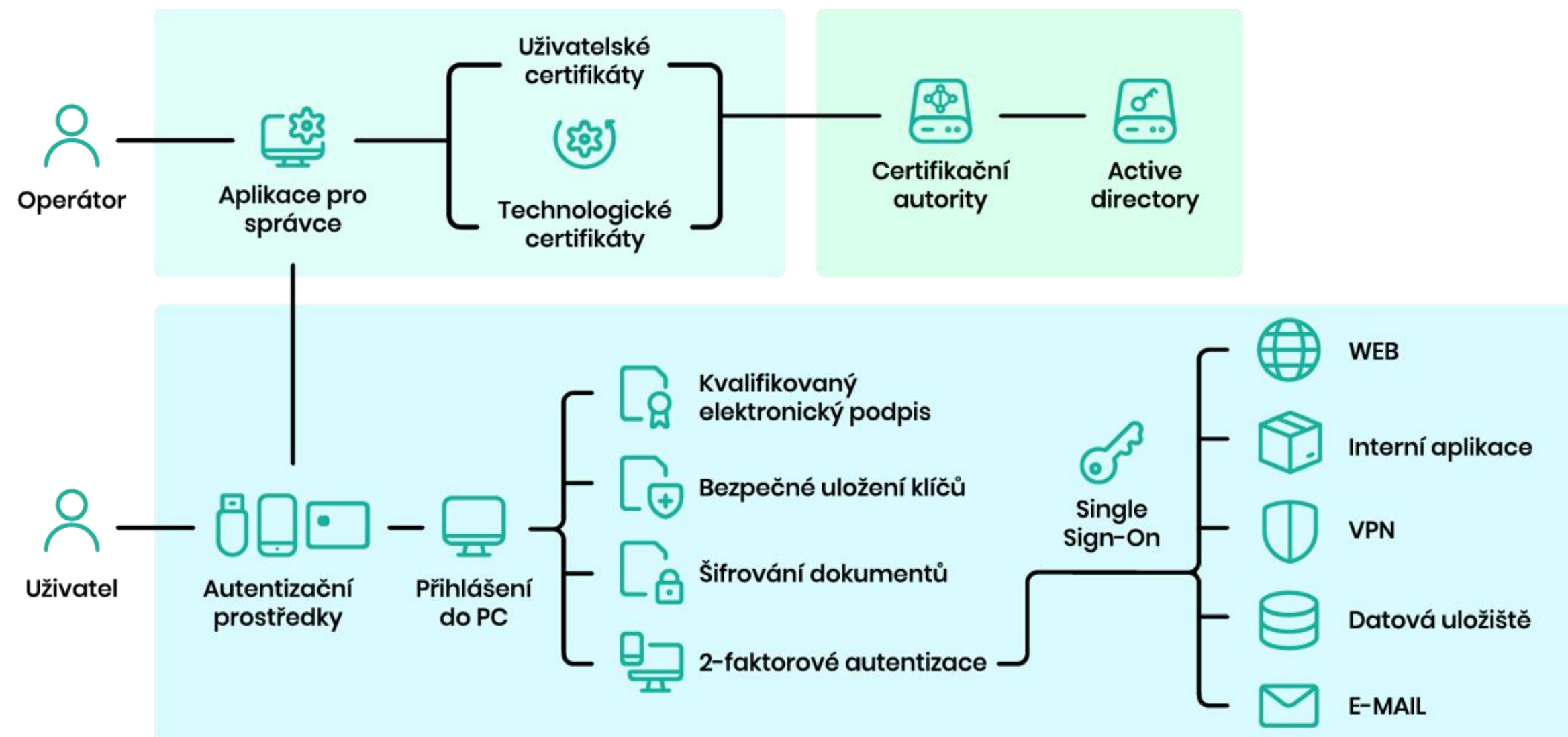
Digitální ekosystém nemocnice z pohledu personálu



- Lékaři a výzkumní pracovníci.
- Zdravotnický personál, laboratorní technici.
- Management, externisté, back office.
- IT manažeři a administrátoři.

Identita zaměstnance v provozu nemocnice

- Vybudování Certifikační autority.
- Napojení na nástroje, které používají reální uživatelé (čipové karty, tokeny...).
- Instalace modulů pro automatickou správu digitálních certifikátů.



Lékaři a výzkumní pracovníci



- Přihlášení do počítače.
- Podepisování eReceptů, eNeschopenek atd.
- Bezpečný příjem/odeslání výsledků vyšetření.
- Bezpečný přístup ke zdravotnické dokumentaci.
- Přístup do nemocniční informačních systémů.
- Identifikace v bezkontaktních systémech.

Naše řešení:

- Čipové karty a USB tokeny.
- S funkcí pro el. podpis a multifaktorové přihlášení.
- Modul pro uložení QPinu.

Zdravotnický personál a laboratoře



- Vizuální identifikace.
- Přístup do prostor, otevírání dveří, ovládání výtahů.
- Přihlášení do sdíleného počítače pod svým ID.
- Přístup k lékařské dokumentaci.
- Přístup do IS nemocnice.
- Pečetění/podepsání výsledků laboratorních vyšetření.

Naše řešení:

- Čipové karty s funkcí průkazu a certifikáty pro podpis a přihlášení.
- Modul pro automatickou notifikaci do e-mailu před expirací certifikátu.
- Kvalifikovaná elektronická pečeť ProID QSeal.

Management/Externisté/Back office



- Zabezpečení komunikace se soudy a sociální správou.
- Podepisování dokumentů pro zdravotní pojišťovny.
- Bezpečný vzdálený přístup pro externisty.
- Přístup do IS nemocnice a do fakturačních programů.
- Práce s grantovou a projektovou dokumentací.
- HR – výdej a recyklace karet (až desítky nových zaměstnanců každý měsíc).

Naše řešení:

- Šifrované připojení do VPN pro vzdálenou práci.
- Mobilní aplikace pro multifaktorové přihlášení do systémů.
- Usnadnění práce s kval. certifikáty.

IT správci organizace



- Komplexní pohled na vydané karty a certifikáty.
- Bezpečný přístup do administrátorských konzolí.
- Bezpečný přístup do VPN a aplikací.
- Hromadné operace nad zaměstnanci a certifikáty.
- Možnost okamžitého zneplatnění certifikátů a karet.
- Přenos rutinních úkonů na HR/Back office.

Naše řešení:

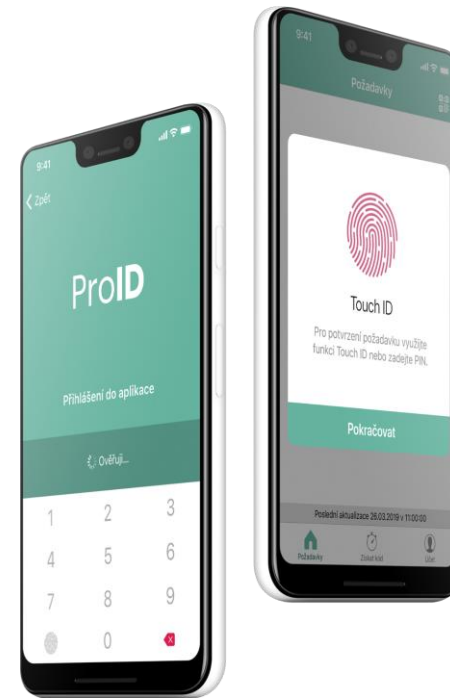
- Passwordless přihlašování do admin. rozhraní.
- Moduly pro datamining, zálohování a operace v reálném čase.
- Sada modulů pro automatizaci práce nad certifikáty.

Dostupné nástroje



Čipové karty ProID

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



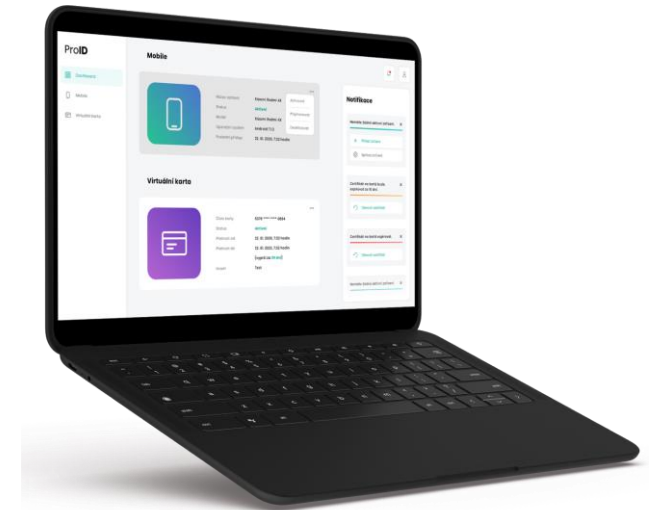
Mobilní aplikace ProID Mobile

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.



TPM čip v laptopu

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

Identita zdravotnického personálu

Logická identita

Fyzická identita



Identifikace
zaměstnance



Přihlášení
do PC



Přihlášení
do aplikací



Přihlášení
do VPN



Přístup 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

Je to složité?



- Nemocnice již teď používají HW prostředky (ProID, nebo jiné).
- Neřeší však s nimi logickou bezpečnost.
- Přitom rozšíření funkcí je jednoduché.

Nejedná se o složitý proces, ale o doplnění funkcí na nástroje, které již běžně používáte.

Lékařský personál nebude nucen složitě přecházet na nová řešení, ale bude nadále používat to, na co je zvyklý.

S čím vám rádi pomůžeme

- Analýza současného stavu.
- Zavedení nástrojů pro bezpečné přihlašování a ověřování identity uživatelů a správců.
- Zjednodušení životního cyklu certifikátů.
- Vybudování doménového PKI.
- Soulad s legislativou a nařízeními.

The logo for ProID is displayed within a rounded rectangular box. The box has a vertical gradient, transitioning from a light teal color at the top to a darker blue at the bottom. The word "ProID" is centered in the box, rendered in a white, bold, sans-serif typeface. The "P" and "I" are slightly larger than the other letters, and the "D" has a distinctive shape with a vertical bar.

ProID

Děkuji!

Michaela Lehká
Sales manager

mlehka@monetplus.cz
+420 703 199 929
www.proid.cz

www.proid.cz

