ProID

Produktový whitepaper

ProID

Bezpečná digitální identita zaměstnanců a organizací

Digitální identita nás dnes provází na každém kroku, usnadňuje nám každodenní život. A to i ten pracovní. Jak ale zajistit, aby byla opravdu bezpečná a zároveň zůstala uživatelsky přívětivá?

V průběhu posledních let se dramaticky zvýšil počet kybernetických útoků nejen na jednotlivce ale také na organizace všech typů a velikostí. Tyto útoky způsobují dlouhodobé výpadky služeb a obrovské finanční škody. S postupující digitalizací firemních procesů a vývojem mezinárodní situce se dá očekávat, že **kybernetické hrozby budou stále narůstat**.

Je smutnou pravdou, že **80 % úspěšných kyberútoků** je způsobeno prolomením nebo **krádeží přihlašovacích údajů** samotných **zaměstnanců** či **privilegovaných účtů** administrátorů, kteří mají přístup do všech systémů a rozhraní. S nástupem moderních technologií se navíc toto riziko rozšířilo i na samotné přístroje a technické prvky (serverů, OT infrastruktury, chytrých měřidel apod.).

Bezpečná digitální identita už ale nemusí být strašák. Řešením přitom nejsou ještě delší, složitější a prakticky nezapamatovatelná hesla. Jde to totiž i jinak. Pohodlně, uživatelsky přívětivě a přesto maximálně bezpečně.

ProID Enterprise Security Platform

ProID je modulární platforma pro zabezpečení organizací, **zaměřená na pracovní a technickou identitu**, kompletně vyvinutá firmou MONET+.

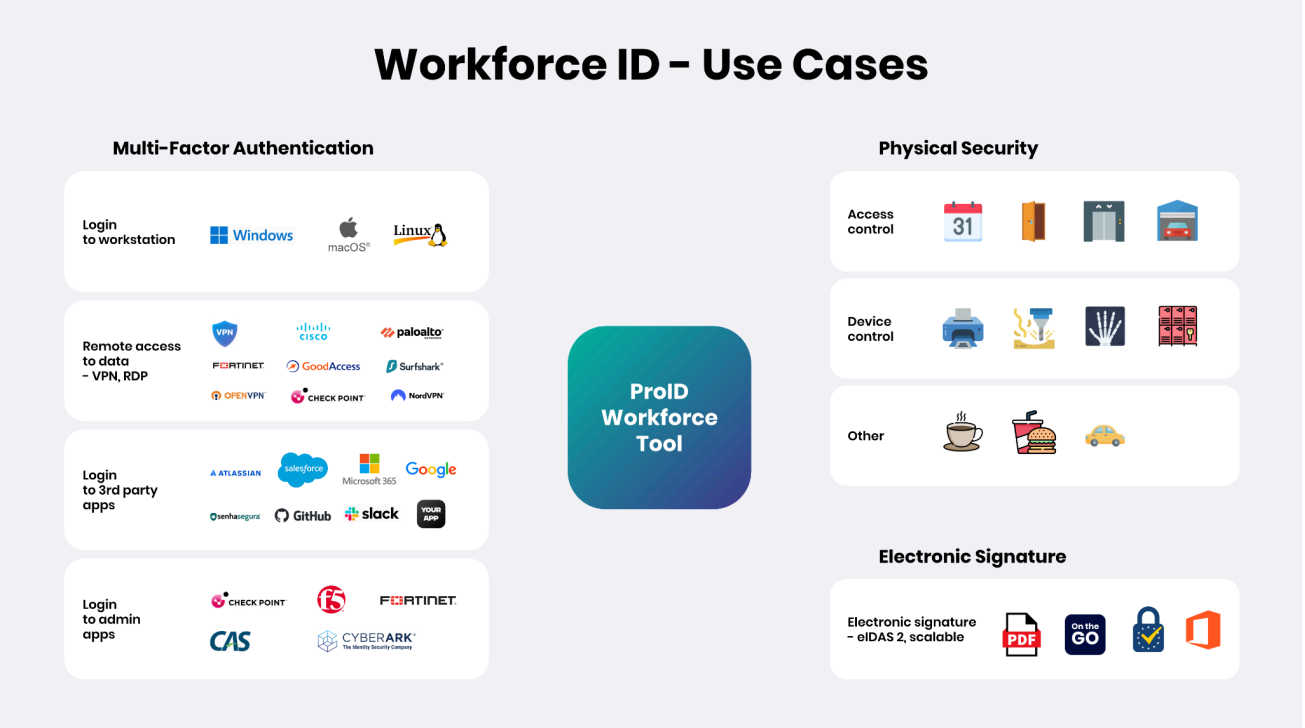
Poskytuje ochranu pro **více než 170 tisíc uživatelů** ve více než **180 organizacích z nejrůznějších vertikál** – fintech, telco, zdravotnictví, utility, výroba, veřejný sektor a další.

- EIDAS 2
- NIS 2
- ISO 27001
- TISAX
- DORA

info@proid.cz | +420 577 110 411 | www.proid.cz

ProID Workforce – Bezpečná zaměstnanecká identita

ProID Workforce nabízí metody a nástroje, které se nezaměřují pouze na problematiku bezpečnosti jednotlivých částí. Snaží se naopak poskytnout komplexní řešení, které pokrývá veškeré potřeby zaměstnance během jeho každodenní pracovní rutiny.



ProID Workforce pokrývá všechny 3 základní oblasti digitální identity zaměstnanců:

1. **Multifaktorová autentizace –** Bezpečné a zároveň i uživatelsky přívětivé přihlašování do nejrůznějších systémů a aplikací.
2. **Elektronické podepisování a pečetění** digitálních dokumentů až do nejvyšší kvalifikované úrovně.
3. **Fyzická identifikace** zaměstnanců pomocí bezkontaktního čipu (fyzický přístup, tiskové řešení, docházka, přístupové a stravovací systémy atd.)

Nástroje a správa ProID Workforce

ProID Workforce nabízí ověřené nástroje pro zaměstnaneckou identitu, které jsou schopné naplnit i nejnáročnější požadavky a scénáře zákazníků:

1. Multifunkční ProID **čipová karta** a její varianty
2. Zaměstnanecká **mobilní aplikace** ProID Mobile
3. Bittron **Token s mobilní autentizační aplikací**

Součástí ProID Workforce je modulární management pro automatizaci procesů a jednoduchou správu nástrojů ProID.

Všechny nástroje je možné kombinovat v rámci jedné organizace dle potřeb jednotlivých uživatelů a zároveň každý uživatel může disponovat vícero nástroji pro tu nejvhodnější kombinaci.

Celou platformu ProID je možné dodat on-premise do prostředí zákazníka a nebo ji využívat formou služby (SaaS).

Multifunkční čipová karta ProID

Čipové karty jsou osvědčeným a léty prověřeným prostředkem pro zajištění identity zaměstnance. Historicky se používaly především pro zabezpečení přístupů do chráněných prostor. V našem portfoliu jsme je doplnili o další funkce, které z nich činí komplexní nástroj pro zajištění jak fyzické, tak i logické bezpečnosti.

Klíčové vlastnosti

- Splňuje FIDO 2 - “passwordless” ověřování a to i bezkontaktní cestou
- Bestseller, osvědčený nástroj pro zajištění digitální identity zaměstnance
- Bezpečné úložiště digitálních klíčů a certifikátů
- Funguje i v offline režimu
- Certifikovaný nástroj uvedený na Trusted Listu EU

Využití multifunkční čipové karty ProID:

- **Zaměstnanecký průkaz**
  Plní funkci osobních průkazů díky možnosti grafické personalizace karet.
- **Multifaktorová autentizace**
  Nástroj pro MFA ověření do systémů a aplikací (MS, Linux, MacOS), VPN, RDP a aplikací třetích stran.
- **Bezkontaktní funkce**
  Karty podporují většinu bezkontaktních technologií/výrobců (Mifare DESfire, HID, Legic, atd.) a lze je propojit s docházkovými systémy, evidencí plateb (např. obědy) a externími zařízeními (tiskárny, turnikety, výtahy…)
- **Elektronický podpis**
  Čipové karty jsou vybaveny certifikovaným QSCD čipem a umožňují vytváření kvalifikovaných elektronických podpisů dle platné legislativy a nařízení EU.
- **Offline režim**
  Není závislá na online ověřování certifikátů.

Ke kartám dodáváme i související produkty (čtečky karet, tiskárny pro potisk, atd.) a širokou paletu modulů pro správce a administrátory.

Mobilní aplikace ProID Mobile

Mobilní telefon se stal nedílnou součástí pracovní rutiny většiny zaměstnanců. Je to zařízení, které mají u sebe vždy a všude a jsou na něm zvyklí řešit stále více pracovních úkonů. My jsme z něj učinili nový nástroj pro firemní bezpečnost.

Naše mobilní aplikace ProID Mobile je dostupná pro Android i iOS a podporuje **passwordless přístup** s využitím biometriky.

Klíčové vlastnosti

- Uživatelsky velmi příjemná metoda s vysokou mírou zabezpečení
- Eliminace hesel (podpora biometriky)
- Umožňuje více způsobů ověření (push notifikace, generování OTP, SMS)
- “Ostrovní režim” (offline scénáře) pro případ krizových situací
- Nabízí jak nasazení formou Saas tak také plnohotné nasazení on-premise
- Podporuje bezkontaktní identifikaci uživatele (Legic, HID, atd.)

Využití aplikace ProID Mobile:

- **Multifaktorová autentizace**
  Nástroj pro MFA ověření do systémů a aplikací, VPN, RDP a aplikací třetích stran, případně vlastních aplikací
- **Využití bezkontaktních funkcí**
  Umožňuje bezkontaktní funkce, jako je ovládání turniketů a výtahů, odemykání zámků či ovládání externích zařízení (podpora Legic Connect, HID Origo a Mifare 2Go)
- **Elektronický podpis**
  Umožňuje vytvářet zaručený i kvalifikovaný elektronický podpis přímo z mobilního telefonu / tabletu

HW Token Bittron s mobilní autentizační aplikací

Nástroj kombinuje unikátní vlastnosti USB HW tokenu a mobilní autentizační aplikace. Je kompletně vyvinut naší společností a splňuje nejvyšší nároky na bezpečnost. Obsahuje kvalifikovaný čip integrovaný se čtečkou do USB tokenu. Jednotlivé akce (potvrzení, el. podpis…) se pak odehrávají v připojené mobilní aplikaci.

Klíčové vlastnosti

- Nejvíce zabezpečená metoda díky dalšímu faktoru (aplikace s využitím biometrie)
- Podporuje FIDO2
- Funguje i v offline režimu

Využití HW tokenu Bittron:

- **Multifaktorová autentizace**
  Nástroj pro MFA ověření do systémů a aplikací (MS, Linux, MacOS), VPN, RDP a aplikací třetích stran pohodlně s využitím biometriky (Touch ID, Face ID), případně PINu.
- **Podpora FIDO2**
  Přihlašování do webových aplikací s podporou tohoto protokolu.
- **Automatické odhlášení při vzdálení se od PC**
  Pokud USB klíč detekuje, že se mobilní telefon vzdálil od počítače, automaticky uživatele odhlásí a zamkne počítač (volitelné).
- **Kvalifikovaný elektronický podpis**
  Náš USB Klíč je certifikovaným identifikačním prostředkem dle Evropského nařízení eIDAS s vysokou úrovní důvěry, můžete s ním tedy podepisovat i ty nejdůležitější dokumenty.
- **Offline režim**
  Není závislý na online ověřování certifikátů, protože je všechny nosíte na čipu s sebou. S mobilem komunikuje přes šifrovaný bluetooth kanál.

Moduly pro management nástrojů ProID

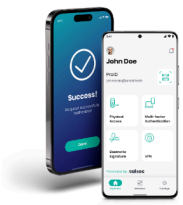
Pro zjednodušení správy nástrojů ProID Workforce nabízíme modulární management pro uživatele a správce organizace. **Centralizuje a automatizuje** složité operace spojené se správou nástrojů. Jednoduše **implementuje požadované procesy** a umožňuje **snadnou konfiguraci požadavků** na řízení životního cyklu ProID nástrojů.

Klíčové vlastnosti

- Výrazné zrychlení a automatizace všech procesů
- Eliminace chybovosti
- Zajištění systémové bezpečnosti organizace
- Úspora nákladů a času
- Intuitivní ovládání

Možnosti využití modulů ProID:

- **Organizace pod kontrolou**
  Moduly nabízí dokonalý přehled nad všemi nástroji, uživateli a certifikáty uvnitř organizace bez ohledu na její velikost
- **Pokrytí důležitých scénářů**
  Onboarding uživatele, přidělení uživatelských nástrojů a jejich management, případně řízení klíčů a certifikátu, potisk karet, atd. To vše v reálném čase a bez složitých kroků
- **Součást interní bezpečnosti**
  Moduly jsou centrální databází a zálohou certifikátů a klíčů pro případ krizových scénářů, včetně možnosti vyhledávání a logování
- **Uživatelské role**
  Moduly jsou určeny jak pro adminy a správce, tak pro HR oddělení (vydávání či potisk čipových karet) i koncové uživatele (automatická obnova expirujících certifikátů, ukládání QPINu atd.)
- **Cloud nebo On-premise**
  Moduly lze instalovat jak u zákazníka na jeho serverech a pracovních stanicích, tak provozovat jako službu (SaaS)



Visual ID	✓	✗	✗
Login to computer	✓	✓	✓
Login to VPN	✓	✓	✓
Login to RDP	✓	✓	✓
Login to various applications (M365, Gsuite, ...)	✓	✓	✓
Electronic signature	✓	✓	✓
Access control	✓	✓	✗
Device control	✓	✓	✗
FIDO2	✓	✗	✓

ProID eSign - Systém pro vzdálený kvalifikovaný elektronický podpis

S digitalizací dokumentů a ideou “paperless” je nutné zajistit takovým dokumentům stejnou právní váhu jako mají ty tištěné. To umožňují prostředky jako jsou kvalifikovaný elektronický podpis, pečeť i časové razítko. Jednou z nejefektivnějších možností jak je mohou organizace vytvářet vzdáleně. Odpadá tím používání prostředků s uloženým certifikátem, podpis je dostupný odkudkoliv, funguje i v mobilním telefonu a umožňuje centrální správu všech certifikátů.

ProID eSign spojuje komfort vzdáleného podpisu s maximální bezpečností. Instaluje se on-premise, přímo uvnitř organizace, včetně všech potřebných komponent.

Součástí řešení je náš vlastní certifikovaný SAM modul, který je uveden na Trusted Listu EU. Slouží k autorizaci podpisového procesu.

Proč zvolit toto řešení?

- Poskytuje uživatelům komfort, snadno se používá a eliminuje nutnost fyzické přítomnosti na pobočce.
- Intuitivní ovládání, passwordless
- Správa a vytváření digitálních dokumentů s plnou právní vahou jednoduše a odkudkoliv
- Nezávislost na konkrétním zařízení, lze použít na notebooku, tabletu i mobilu
- Certifikované řešení dle nařízení eIDAS 2

Možnosti využití systému eSign:

- **Podpis, pečeť, razítko**
  Kvalifikovaný elektronický podpis, kvalifikovaná el. pečeť a časové razítko odkudkoliv a z libovolných zařízení, včetně smartphonů a tabletů
- **Integrace do systémů organizace**
  Možnost propojení se spisovou službou či se stávajícími aplikacemi (CRM, ERP, fakturační a objednávkové systémy atd.)
- **Obchodní příležitost**
  Organizace sama může být poskytovatelem elektronického podpisu pro své zákazníky, dodavatele či podřízené subjekty

Tech ID – systémy pro řízení technologických certifikátů

Nejen člověk, ale také nejrůznější přístroje a technická zařízení už mají svou digitální identitu. Množství takových technologických prvků navíc exponenciálně roste a s ním i spojená bezpečnostní rizika.

OT infrastruktury, servery, čidla, měřicí soustavy, sofistikované výrobní stroje, nemocniční přístroje a celá řada dalších zařízení denně komunikují s firemní síti a přijímají či odesílají citlivá data. Jejich napadení pak může zapříčinit kolaps celé organizace a přerušení provozu klidně i na mnoho dnů. Proto jsme naše identitní řešení rozšířili o část, chránící právě zranitelné technické prvky.

Proč zvolit toto řešení?

- Univerzální použití pro řízení identit technických prvků napříč celou organizací
- Možnost propojení se zaměstnaneckou identitou
- Využití nejmodernějších kryptografických algoritmů
- Založeno na technologii Public Key Infrastructure

Možnosti využití systémů:

- **Centrální bod správy**
  Systémy poskytují centrální místo pro bezpečné uložení kryptografického materiálu, provádění kryptografických operací a řízení přístupu na základě uživatelských rolí
- **Vše v jednom řešení**
  Systémy jsou integrovány s moduly pro řízení certifikátů, doménovým PKI a certifikační autoritou
- **KMS (Key Management System)**
  Umožňuje šifrovanou komunikaci přístrojů, serverů a aplikací, importy a distribuci kryptografických klíčů
- **Certificate Lifecycle Management (CLM)**
  Efektivně řídí životní cyklus technologických certifikátů. Zajišťuje kritické scénáře (automatizované vydávání, kontrolu identifikačních údajů a žádosti o certifikát…) i podpůrné procesy pro centrální správu certifikátů
- **Podpora globálních protokolů**
  Systémy pracují s široce používanými protokoly a zajišťují jejich integraci do jednotného rozhraní (ACME, SCEP, EST, Proprietární protokol…)
- **Podpůrný HW**
  Součástí našich řešení jsou i dodávky potřebných HW prostředků (HMS servery, tokeny, čipové karty…)