MONET +

Ochrana technických prvků

Prezentace

ProID

Monet+

specializovaný software house

25+
let v aplikované kryptografii

350+
zákazníků ve světě

350+
specialistů na IT projekty

1 MISSION

Digitally move
identities and money

8
business solutions

€ 23 mil.
obrat v roce 2023

20+
zemí s aktivními projekty

ProID

Enterprise Security platform for Workforce & Technical Identity

150+
organizací

170.000
Aktivních uživatelů

Enterprise

Workforce ID

Vícefaktorová autentizace
Elektronický podpis
Fyzický přístup

Tech ID

Správa životního cyklu certifikátů
Public Key Infrastructure (PKI)
Správa šifrovacích klíčů

ProID

Enterprise Security platform for Workforce & Technical Identity

150+
organizací

170.000
Aktivních uživatelů

Enterprise

Workforce ID

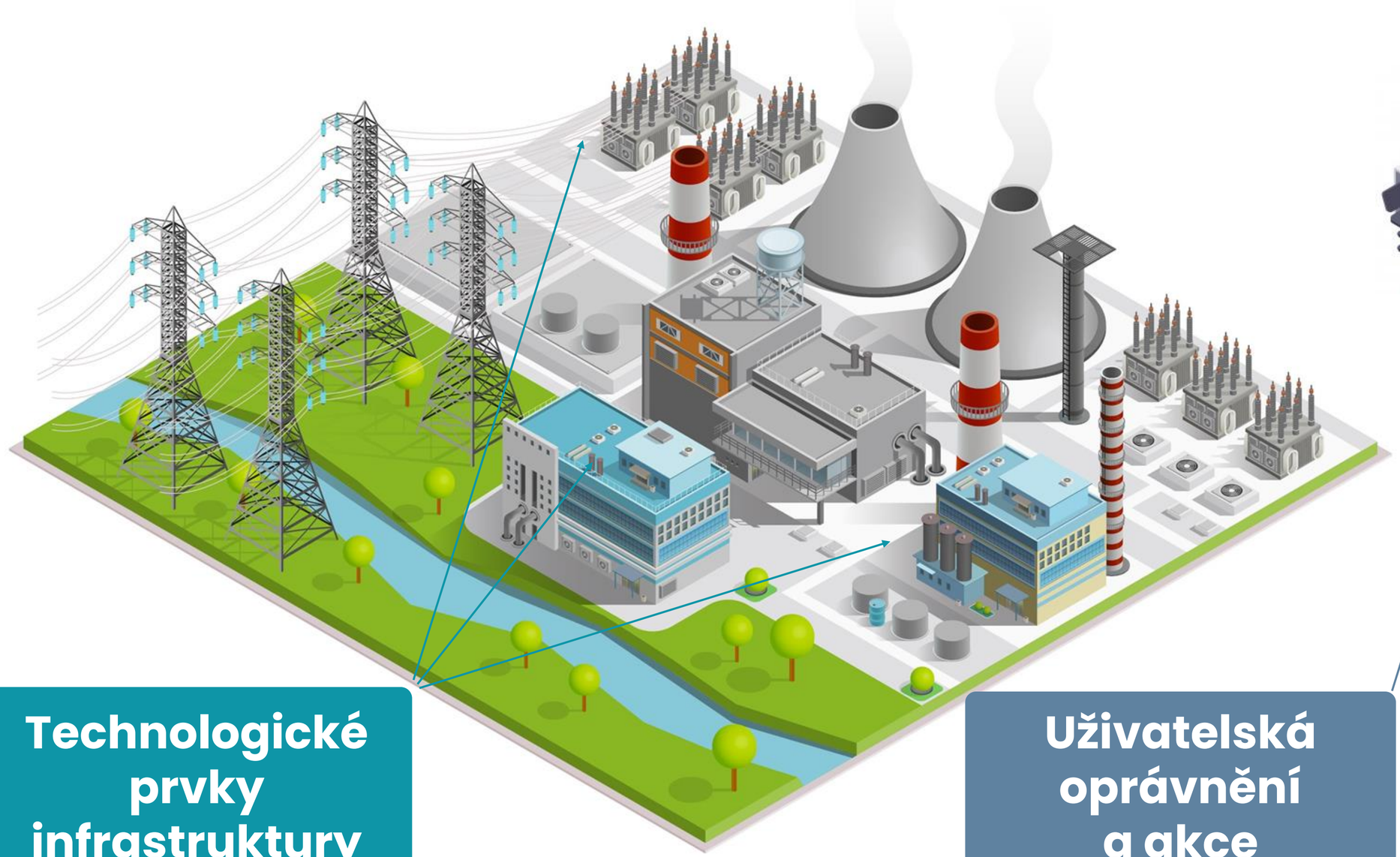
Vícefaktorová autentizace
Elektronický podpis
Fyzický přístup

Tech ID

Správa životního cyklu certifikátů
Public Key Infrastructure (PKI)
Správa šifrovacích klíčů

Přehled TechID

Digitální ekosystém průmyslové firmy



Technologické prvky infrastruktury

Uživatelská oprávnění a akce

Tech ID

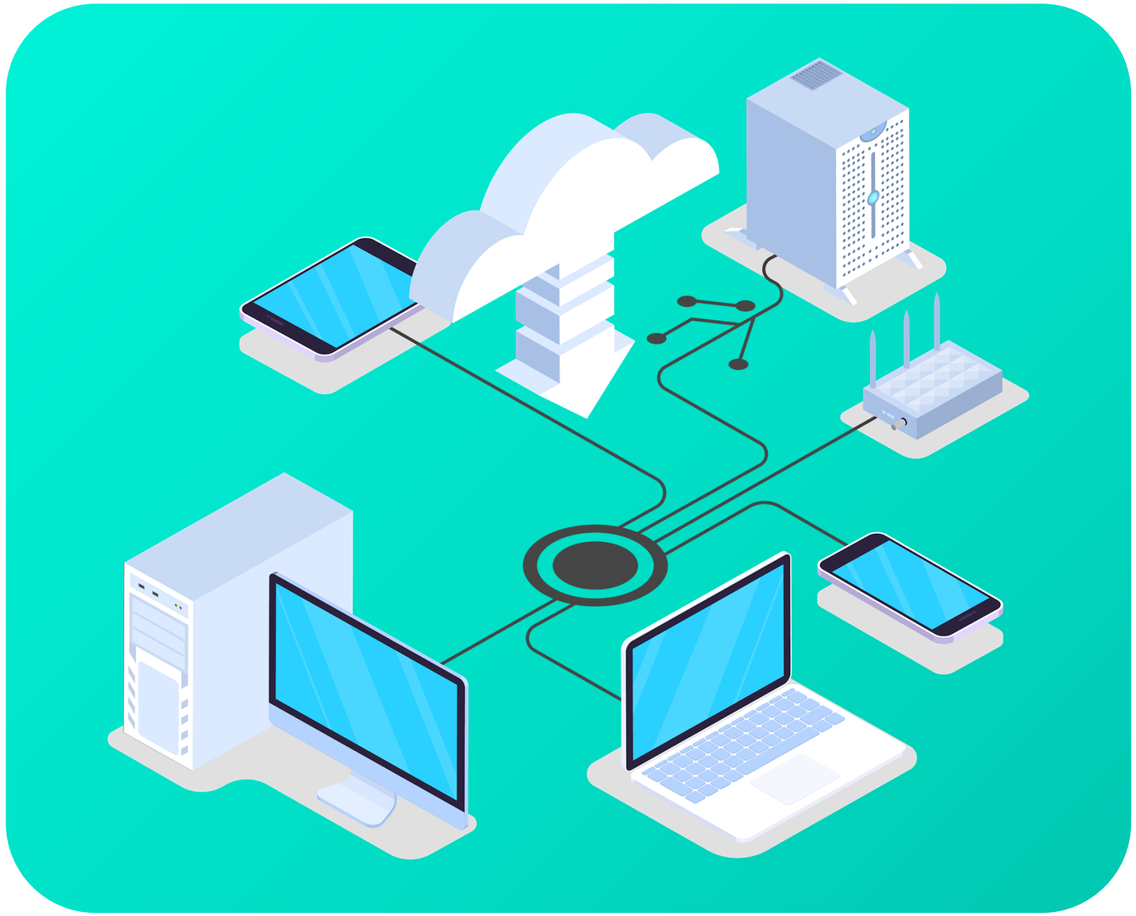
- Bezpečná distribuce certifikátů pro koncové systémy
- Automatizovaná správa životního cyklu certifikátů a klíčů
- Eliminace výpadků při expiraci
- Minimalizace nutných manuálních zásahů administrátorem

Fyzické servery

Virtuální servery

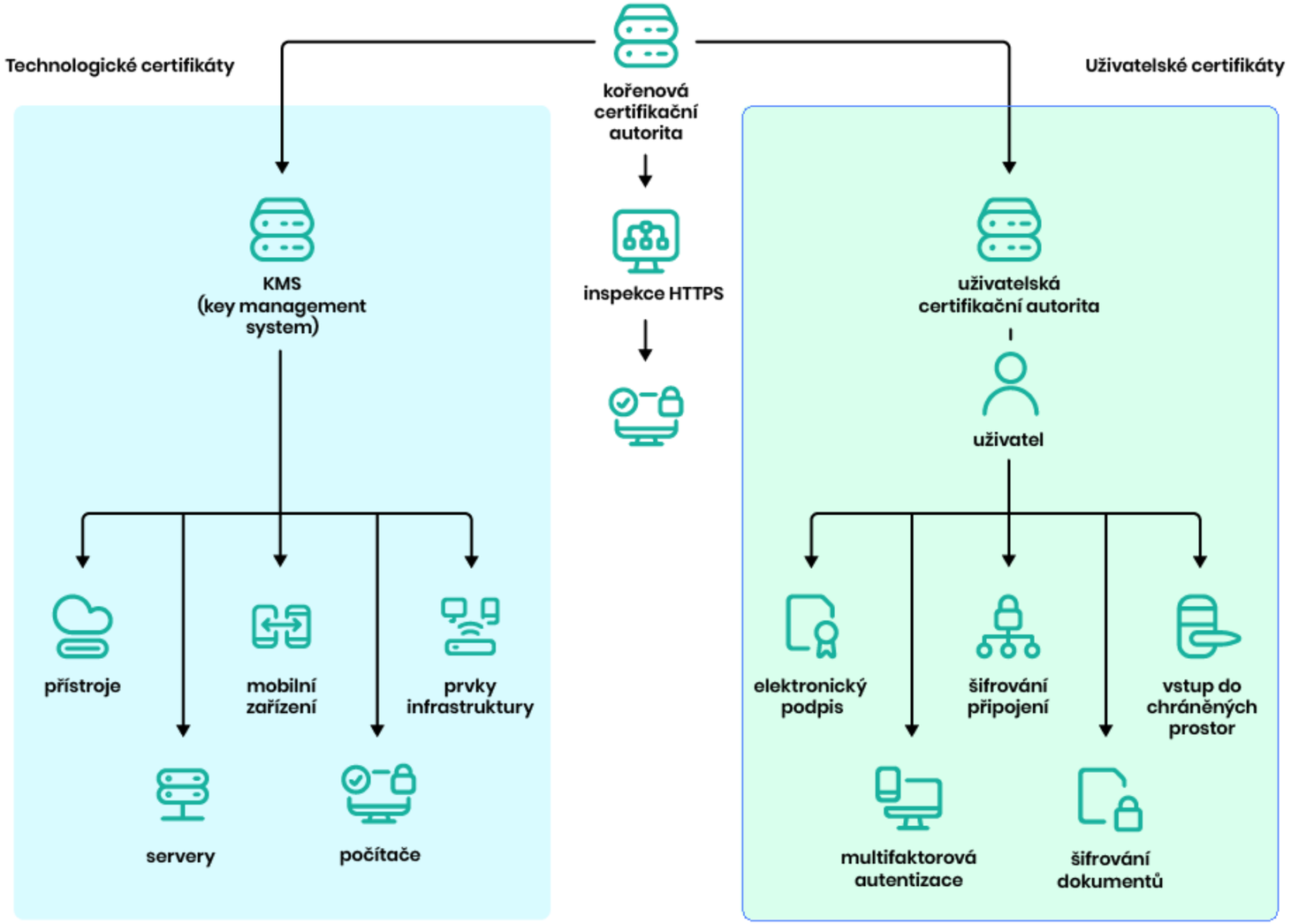
Prvky infrastruktury

Prvky IoT

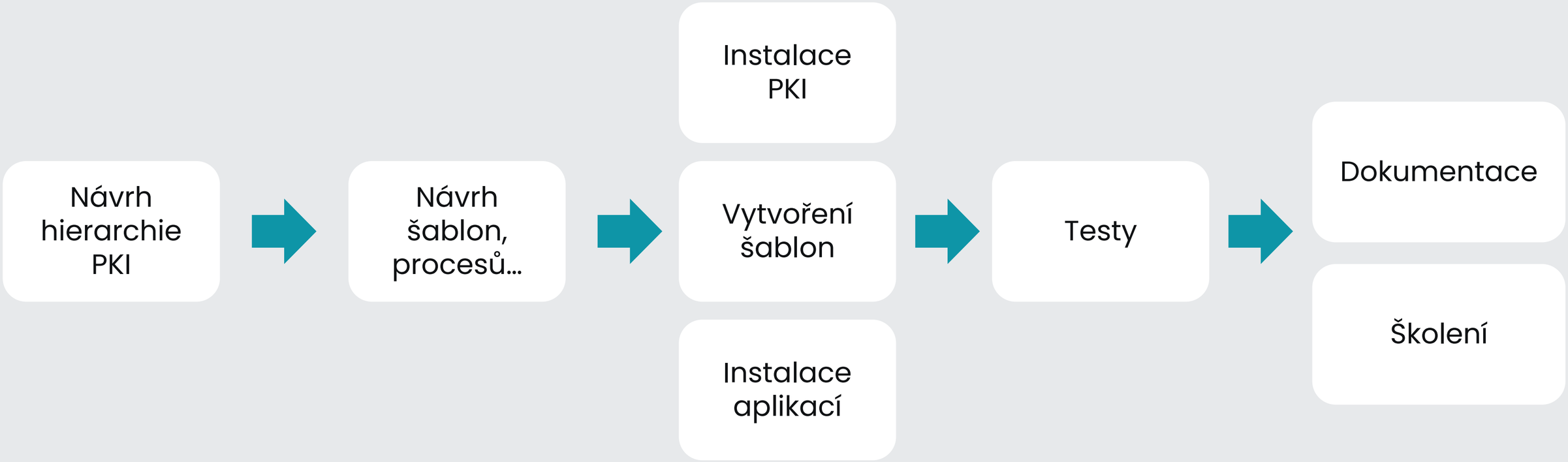


solutions by **MONET +**

Doménové PKI jako základ

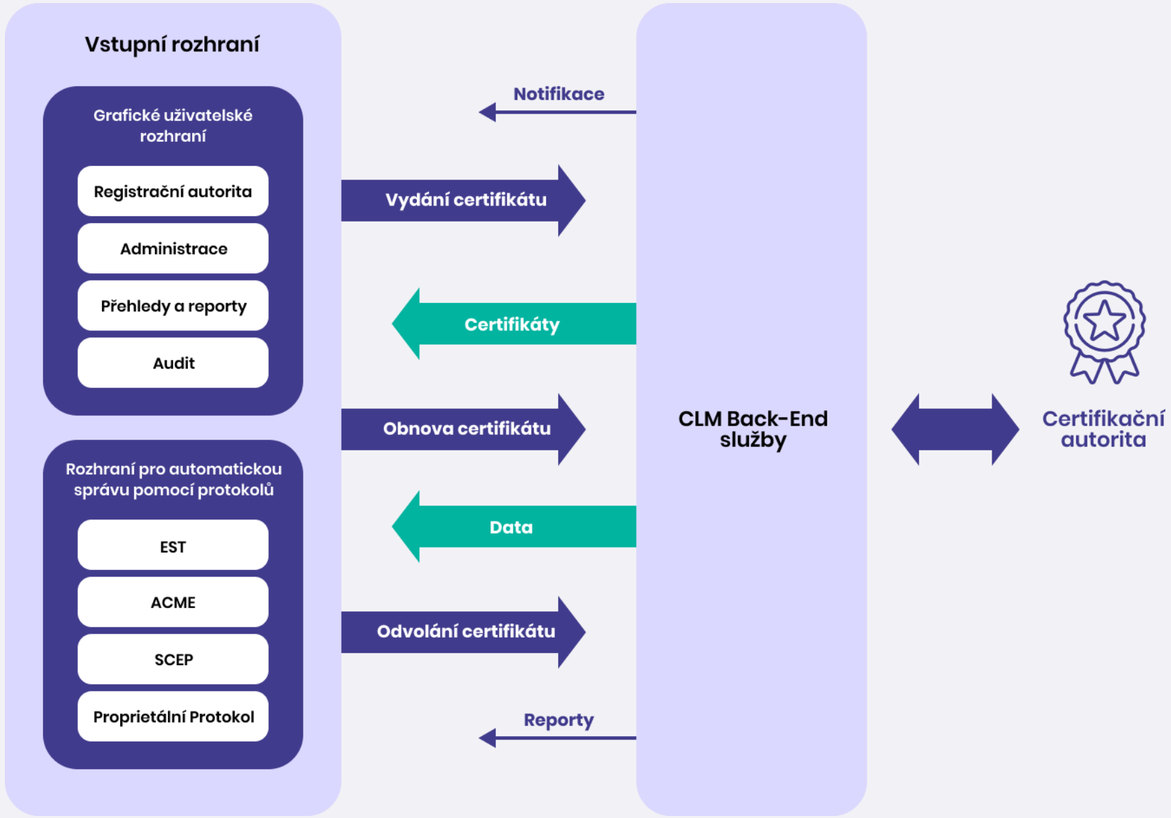


Budování doménové PKI



Certificate Lifecycle Management

- Centrální systém pro správu a administraci
- Přehledy, reporty, notifikace
- Správa uživatelů a rolí
- Bezpečnostní procesy v rámci vydání certifikátů - kontrola položek žádostí o certifikát, autorizace žádosti podpisovým certifikátem, atp.
- Procesy pro řízení životního cyklu technologických certifikátů
  - Vydání
  - Obnova
  - Odvolání



Automatizace

ACME

- implementace obecného ACME serveru dle RFC 8555
- kompatibilita s globálně nejčastěji využívanými ACME klienty
- unikátní koncept ACME External Account Binding - vytvořen na míru pro koncept interního ACME serveru pro vydávání certifikátů z interní certifikační autority
- vhodné pro SSL certifikáty (Domain Validation certifikáty)

EST

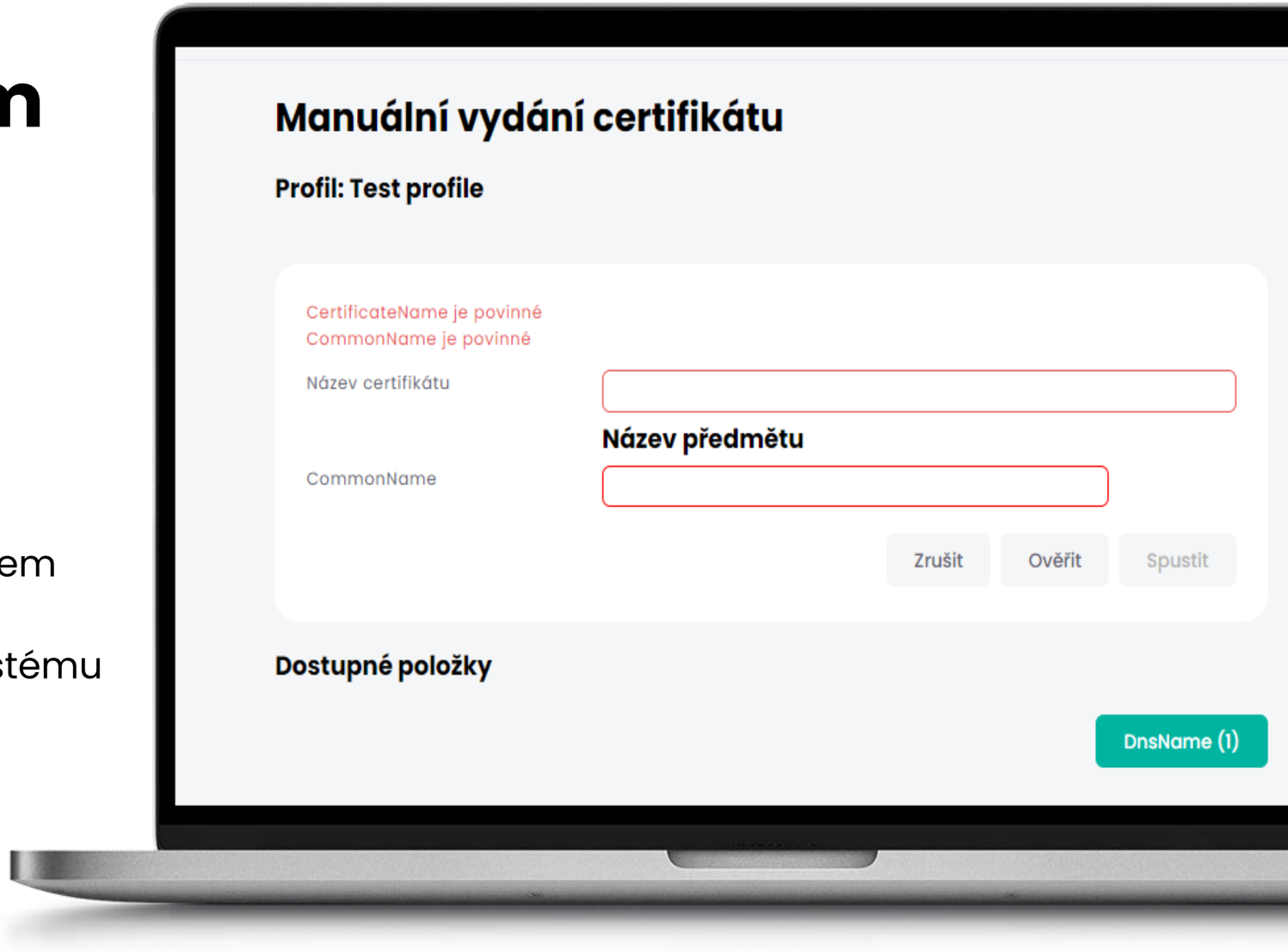
- implementace EST protokolu dle RFC 7030
- dynamická konfigurace autorizačních pravidel EST endpointů (pro autentizaci klientským certifikátem nebo jménem / heslem)
- vhodné (nejen) pro certifikáty síťových prvků

SCEP

- implementace SCEP protokolu dle RFC 8894vhodné (nejen) pro certifikáty síťových prvků

Manuální vydání certifikátu správcem

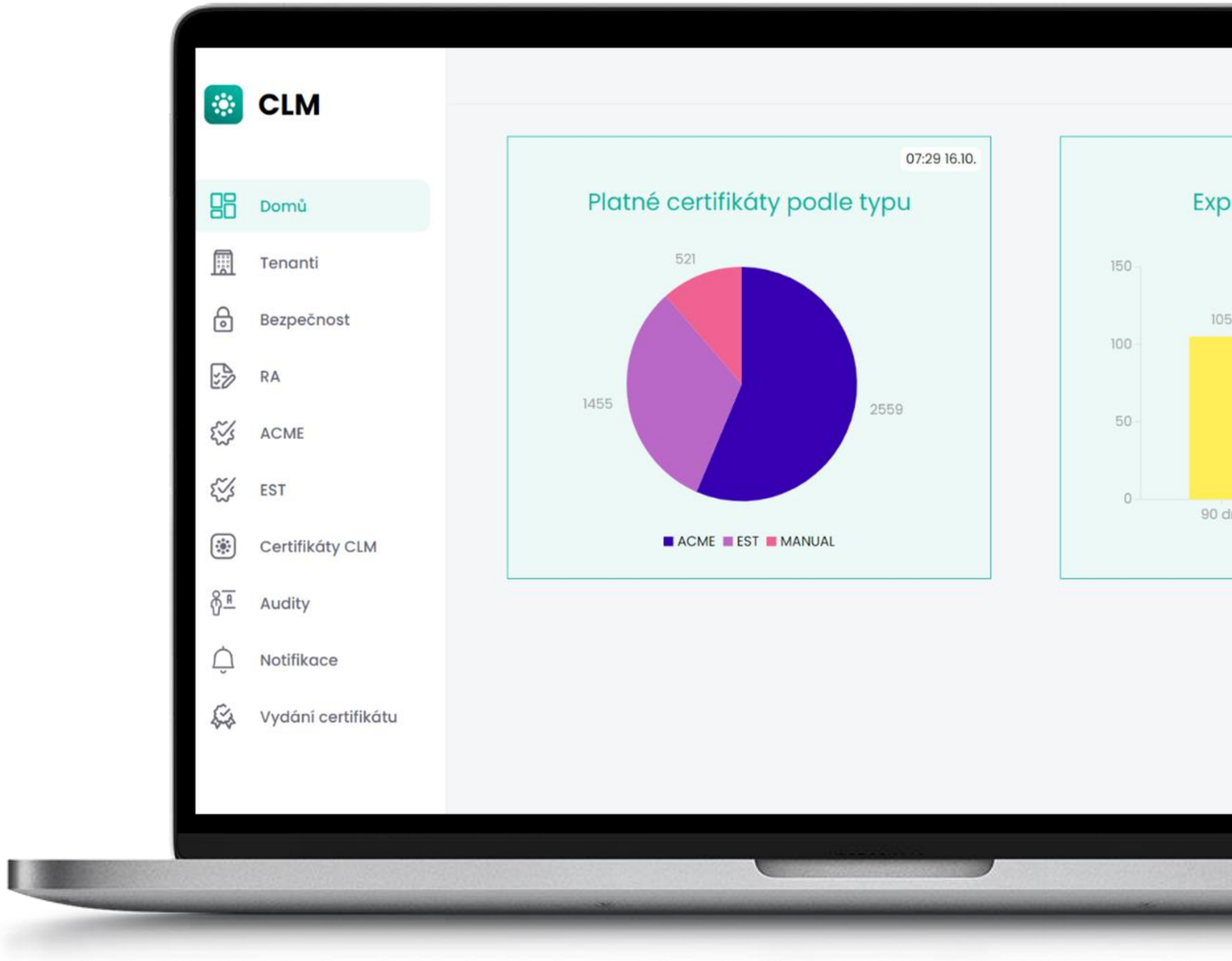
- uživatelské rozhraní pro možnost obslužného vydání certifikátu podle definovaného profilu
- možnost vydání certifikátu podle předem vytvořené žádosti, nebo s možností vygenerování klíčů a žádosti v CLM systému



Portál CLM

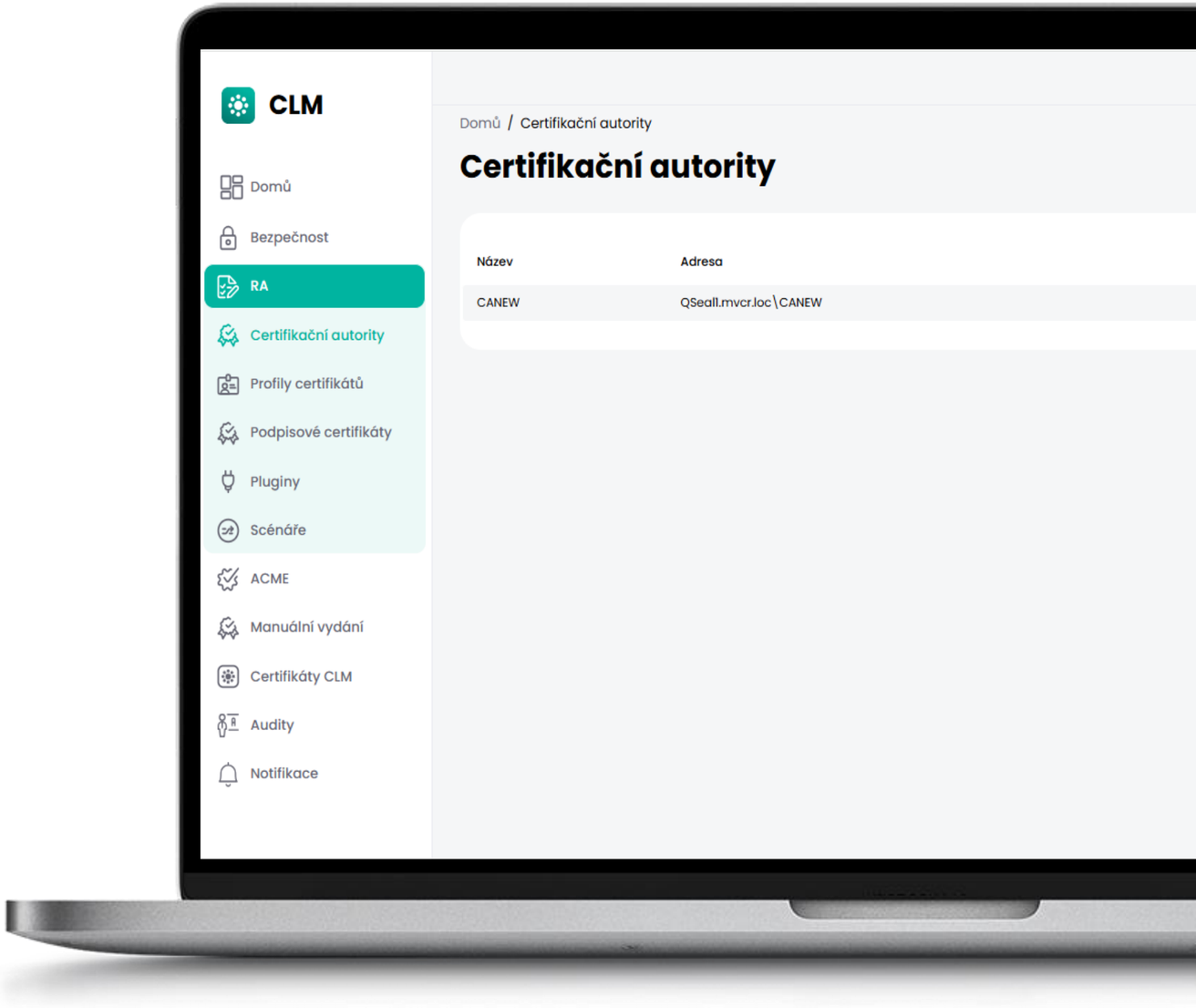
Intuitivní správa systému přes grafické rozhraní

- Správa rolí a oprávnění
- Konfigurace bezpečnostních pravidel pro vydávání certifikátů
- Přehled vydaných certifikátů, auditních událostí, atp.



Rozvoj CLM

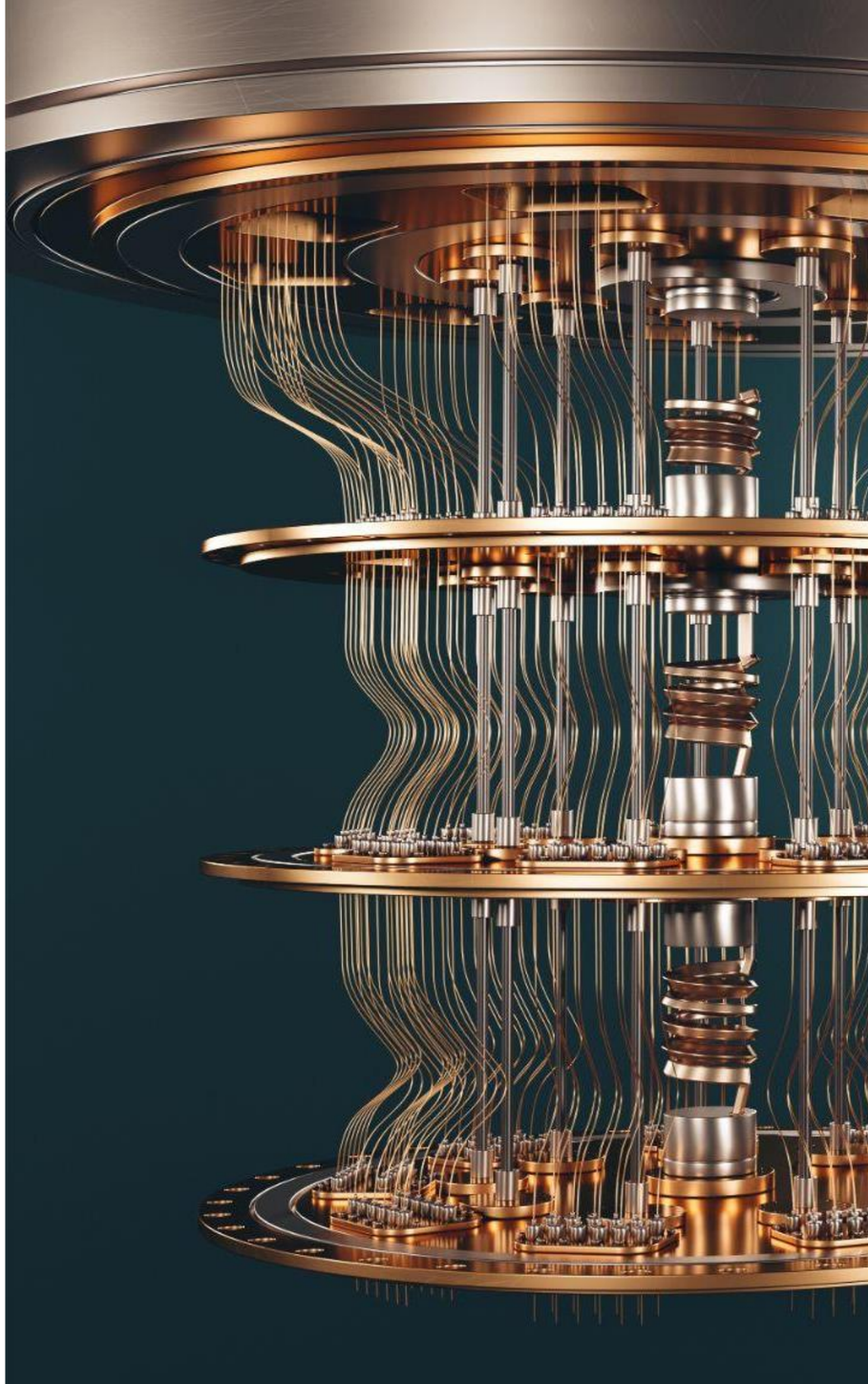
- **1) Certificate discovery**
- řešení, při kterém organizace automatizovaně zjišťuje, kde všude jsou v její infrastruktuře používány digitální certifikáty
- **2) Integrace Public CA do systému CLM**
- Integrace na veřejné certifikační autority, které vydávají certifikáty pro veřejné využití (Digicert, GlobalSign a další…)



Postkvantová kryptografie

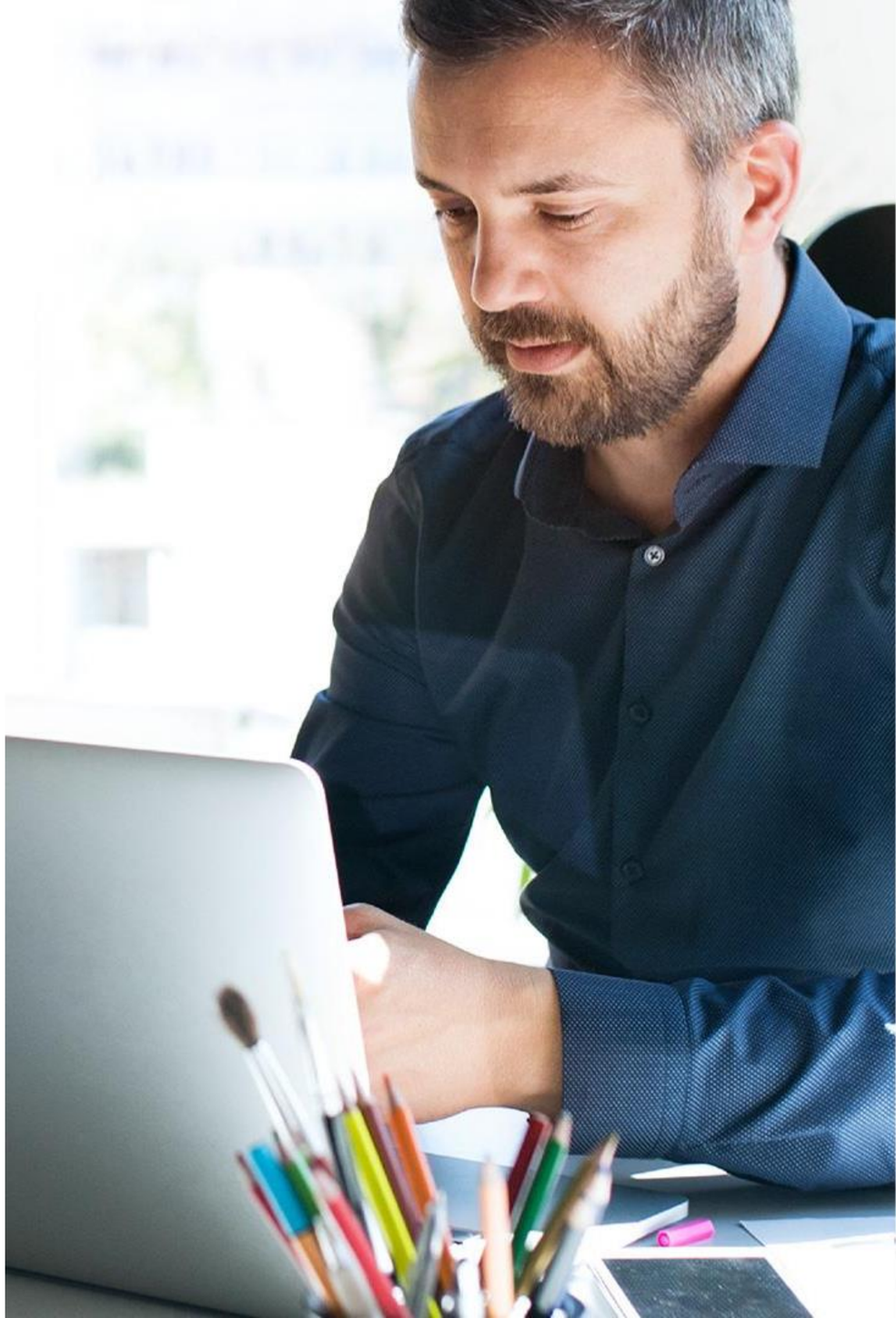
Post-quantum cryptography (PQC)

- Kryptografie odolná vůči útokům kvantových počítačů
- Kvantový počítač využívá principů kvantové mechaniky a díky tomu dokáže řešit určité problémy výrazně rychleji než klasické počítače:
  - Faktorizace velkých čísel → hrozba pro RSA
  - Diskrétní logaritmus → hrozba pro ECC
- Postkvantové algoritmy jsou realizovatelné na klasických počítačích



Kryptografická inventura

- Aktivita spočívající v identifikaci všech míst a účelů, kde a proč je v systému použita konkrétní kryptografie
- – nezbytný předpoklad pro plánování a stanovení priorit migrace.
- Nezahrnuje pouze kód, ale také dokumentaci.



Migration playbook

- Kryptografická inventura
- Identifikace aktiv a jejich závislostí
- Kritičnost a životnost bezpečnosti aktiv
- Prioritizace migrace a její fáze
- Strategie migrace
- Požadované změny a dopady
- Navrhované nástroje/knihovny/řešení
- Očekávané náklady
- Strategie testování a validace

TEĎ!

Je nejlepší čas na zahájení přípravy na postkvantovou kryptografii

Děkuji!

vdoktor@monetplus.cz

+420 739 131 489

proid.tech | monetplus.com

Sales Manager