

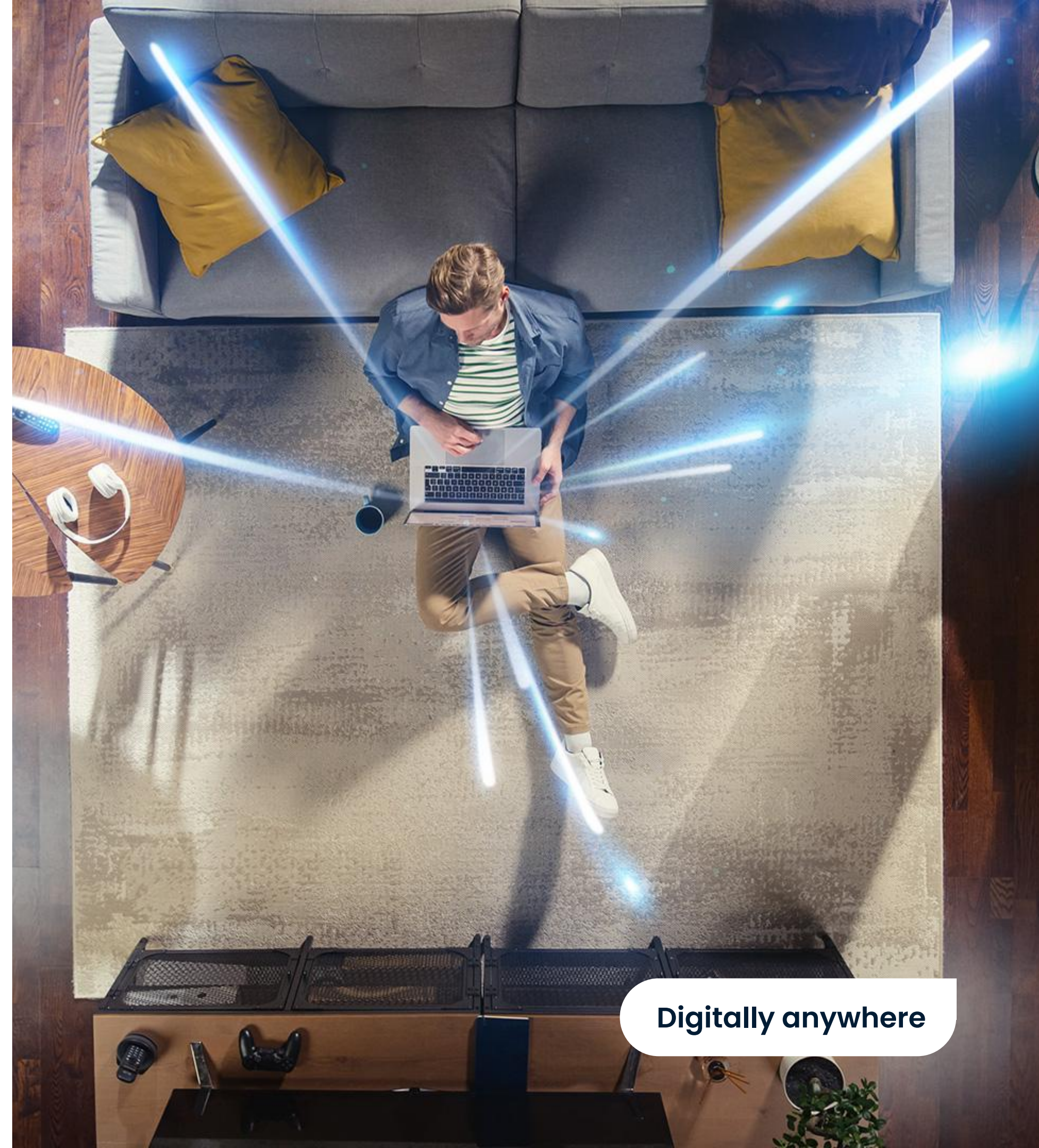
MONET +

Abeceda technické identity: Proč se věnovat CLM a KMS?

Security Brunch

Jakub Čumpelík
Sales Manager

Digitally anywhere



Tech ID v Monet+

- Výstavba PKI infrastruktury
- Budování certifikačních autorit
- Tvorba certifikačních politik
- Dodávky a instalace HSM modulů
- Asymetrická a postkvantová kryptografie
- Specializované moduly
- **Key Management System (KMS)**
- **Certificate Lifecycle Management (CLM)**



CLM & KMS
A → Z?

MONET +

Automatizace a ACME

- automatizace rutinních procesů
- CLM – využití protokolu ACME (SCEP i EST)



Fyzické
servery



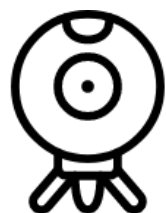
Virtuální
servery



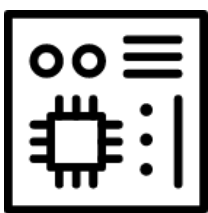
Prvky
infrastruktury



Mobilní
zařízení



Prvky
IoT



Lékařské
přístroje



Smart
Metering



Bezpečnost

- bezpečná distribuce klíčů a certifikátů mezi koncovými body
- využívání moderních kryptografických algoritmů
- bez nutnosti lidského zásahu



Centrální body správy

- řízení z jednoho místa v organizaci
- vertikální i horizontální řízení rolí (CLM)
- centrální místo pro uložení krypt. materiálu
 - klíčový sklad (KMS)



DORA

- **Article 9**, Protection and prevention
- **Article 10**, Detection
- **Article 11**, Response and recovery
- **Article 12**, Backup policies and procedures, restoration and recovery procedures and methods



Efektivní eliminace výpadků

- automatizované řízení životních cyklů klíčů a certifikátů
- eliminace výpadků při expiraci
- odpadá manuální řízení certifikátů (excel, tabulky)



Funkcionalita

CLM – Certificate Lifecycle Management

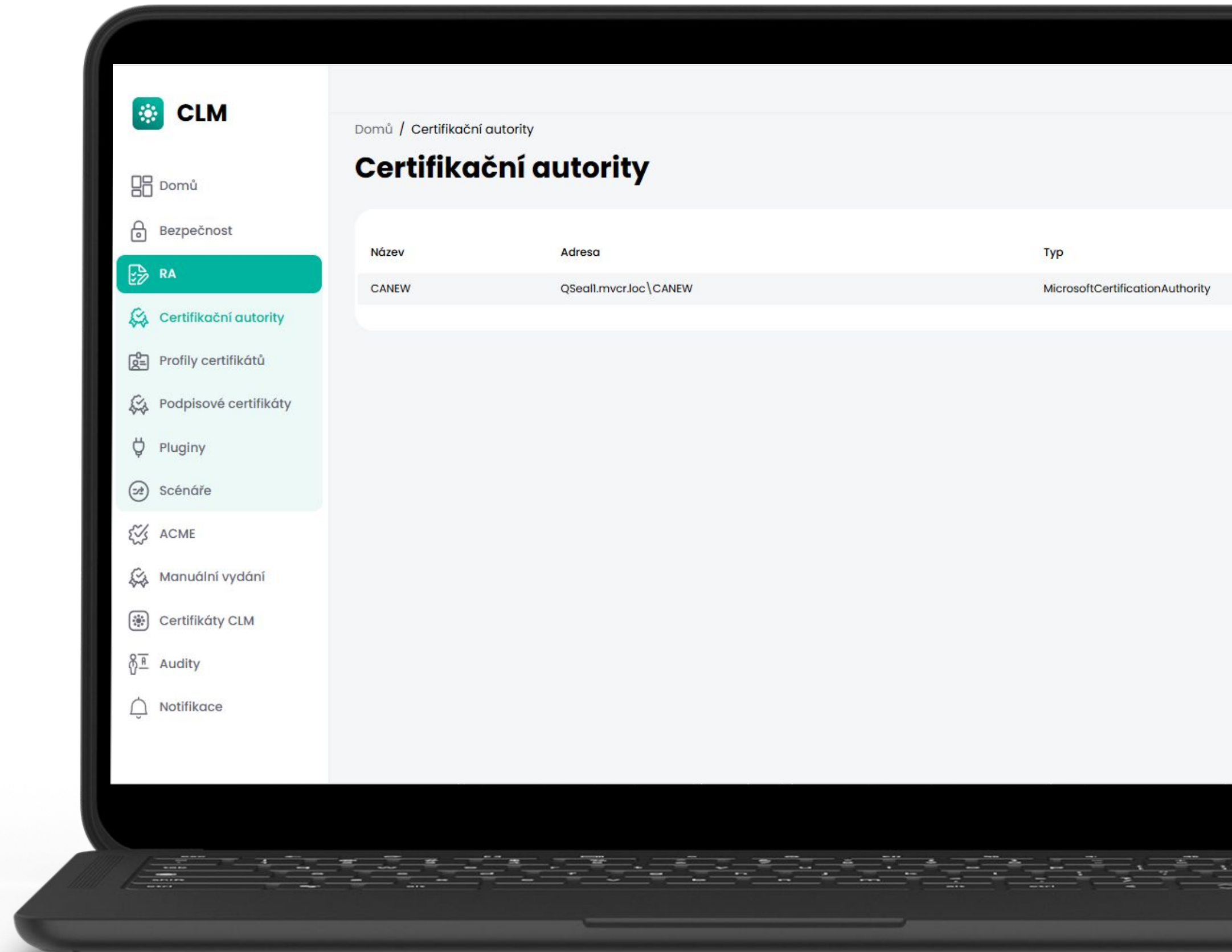
- Vysoce **škálovatelný** systém pro správu životního cyklu certifikátů
- Zajištění **bezpečnosti** vynucením Security Compliance v procesu správy certifikátů
- Zajištění používání **moderních kryptografických algoritmů**
- Znemožnění vydání certifikátu neautorizované roli, technickému prvku nebo uživateli
- Sestavování **vlastních scénářů** pro vydání certifikátu
- Definování **uživatelských rolí a bezpečnostních profilů** svázaných se scénáři vydávání certifikátů
- Dynamickou validaci žadatelů a možnost podpisu žádosti o certifikát autorizačním certifikátem

KMS – Key Management System

- Jednotné místo pro přehled zařízení a jejich aktivních certifikátů
- Eliminace **výpadků při expiraci certifikátů** (server-client komunikace, P2P)
- **Centrální místo pro uložení krypt. materiálu** – klíčový sklad
- Import certifikátů do klíčového skladu
- Minimalizace nutných manuálních zásahů administrátorem ITS

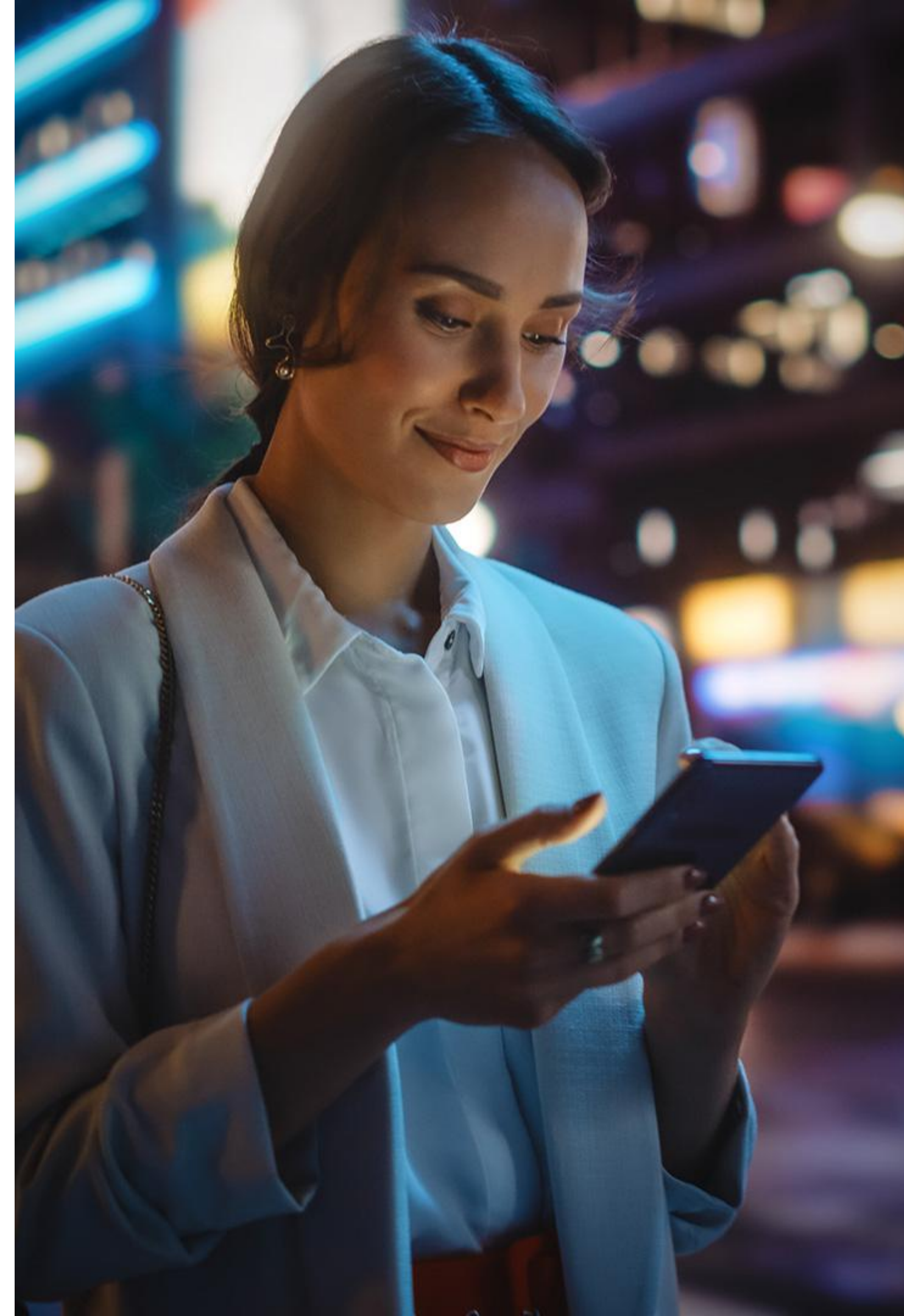
Grafické rozhraní

- využití uživatelsky přívětivého grafického rozhraní (CLM)



High Availability

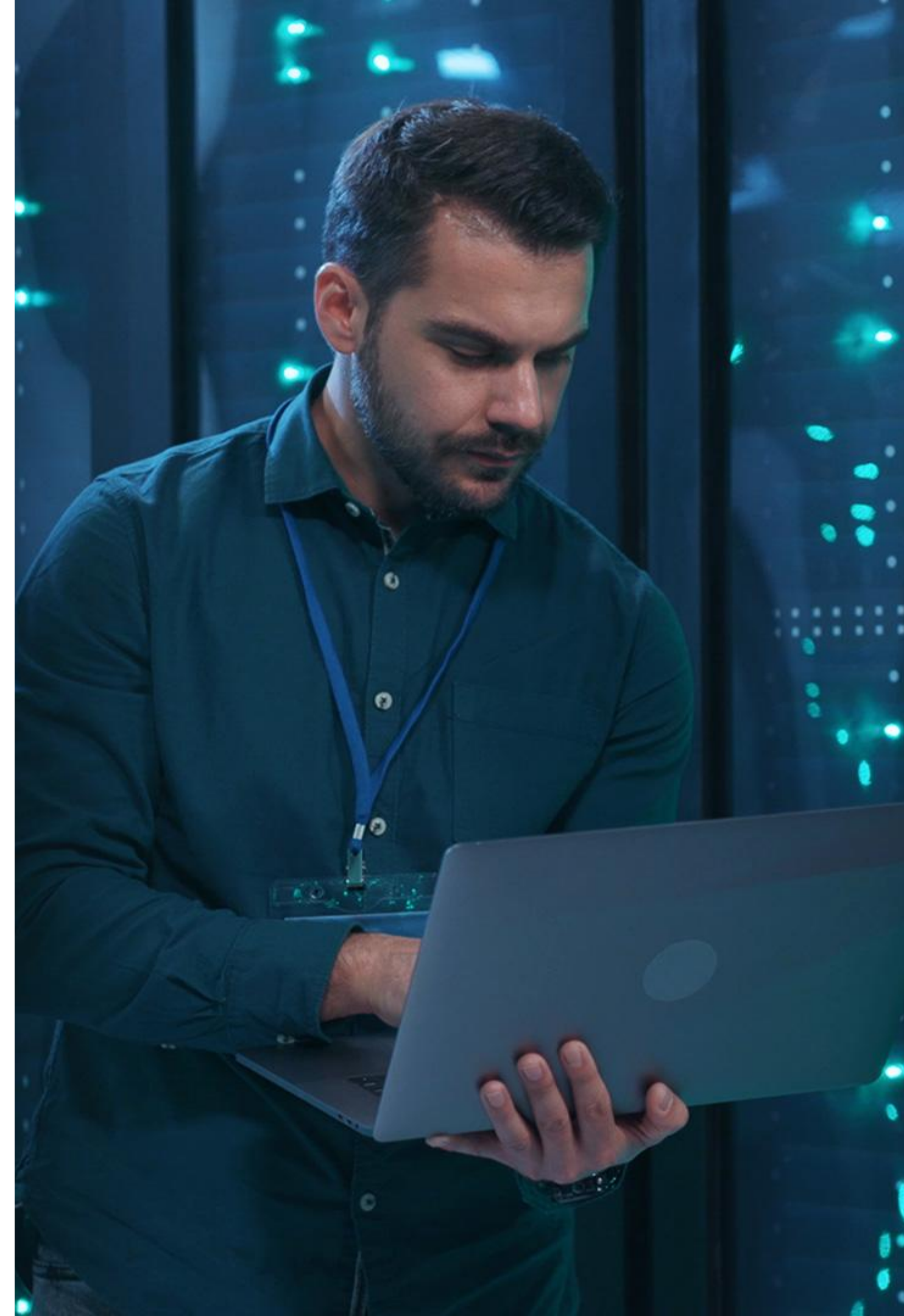
- možnost provozu systémů
v režimu vysoké dostupnosti



Interní infrastruktura

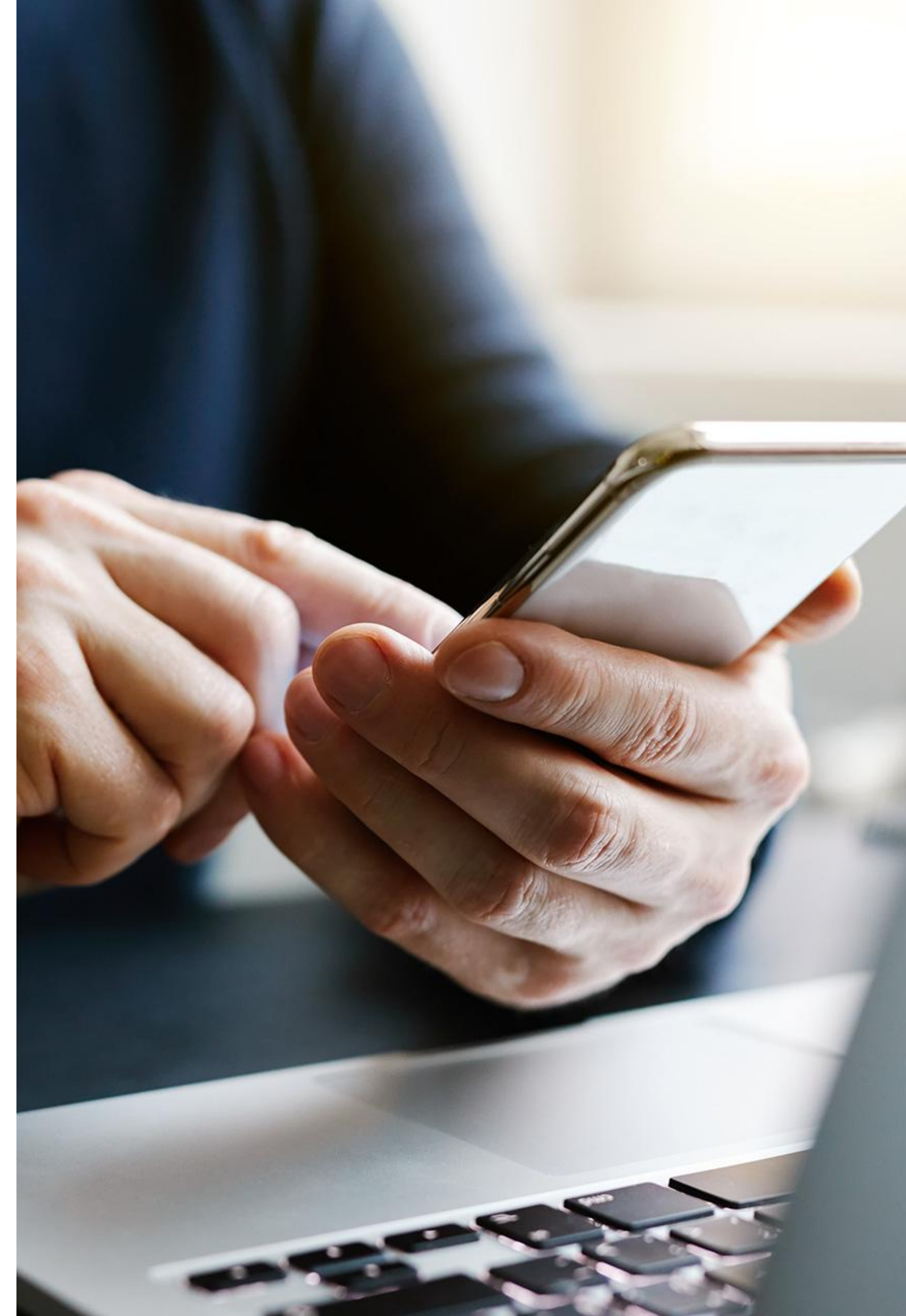
- posílení péče o interní infrastrukturu klíčů a certifikátů
- uvolnění kapacit a zvýšení bezpečnosti
- snížení chybovosti

“Lidem myšlení, strojům dřinu.” Tomáš Baťa



Jiné protokoly a úlohy

- možnost dovyvinout použití jiný protokolů než jsou ACME, EST a SCEP (CLM)
- možnost přizpůsobení systémů (např. smart metering)



Kritické procesy & KMIP

- automatizované vydávání certifikátů s využitím globálně používaných protokolů
- kontrola schválených identifikačních údajů v žádosti o certifikát
- kontrola podporovaných kryptografických algoritmů atd.

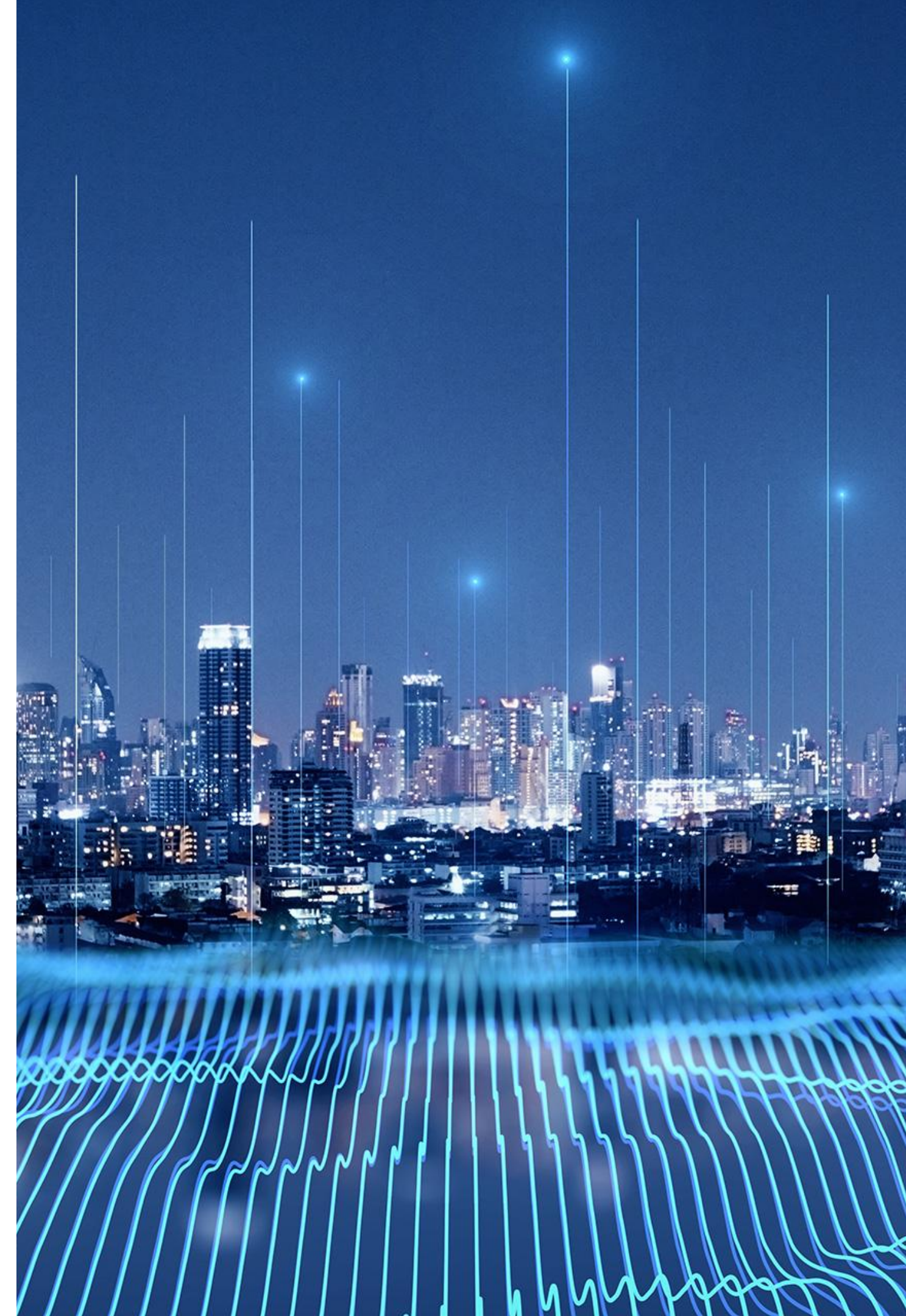
KMIP

- protokol s velmi širokou škálou použití (např. šifrování záloh, interoperabilita systémů, přidávání bezp. systémů do infra.)



Lifecycle

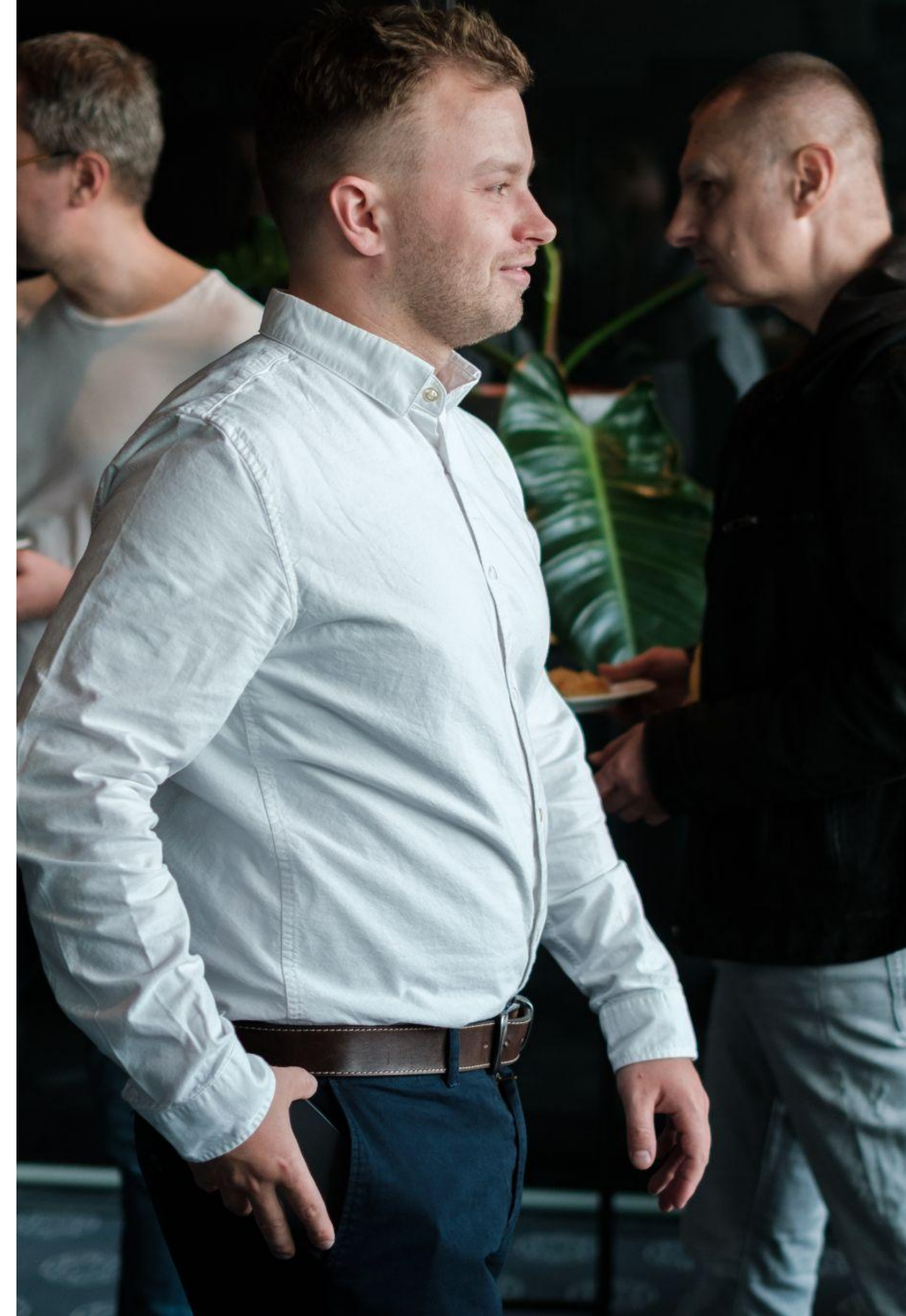
- Automatické vydávání certifikátů
- Automatická obnova certifikátů
- Automatické odvolání/revokace
- Audit



Monet+

- Certificate Lifecycle Management
- Key Management System

- vlastní vývoj
- in-house podpora
- možnost přizpůsobení, rozšíření a provázání s dalšími systémy



CLM & KMS

$A \rightarrow M+$

MONET +

CLM & KMS

A → **M**+

Automatizace a ACME

Bezpečnost

Centrální body správy

DORA

Efektivní eliminace výpadků

Funkcionality

Grafické rozhraní (CLM)

High Availability

Interní infrastruktura

Jiné protokoly a úlohy

Kritické procesy

Lifecycle

MONET+

...více písmen netřeba.

MONET +

Děkuji za pozornost.



[Contact me](#)

Jakub Čumpelík

jcumpelik@monetplus.cz

