
Proces správy kryptografických klíčů (Key Management Process)

Verze: 1.1

Platnost od: 27. 01. 2026

Garant procesu: Vedoucí IT / Security Officer

Vazba na ISO/IEC 27001:2022:

- A.8.24 – Používání kryptografických kontrol

---

1. Účel

Účelem tohoto procesu je stanovit jednotná technická a organizační pravidla pro bezpečnou správu kryptografických klíčů po celou dobu jejich životního cyklu. Cílem je zajistit důvěrnost, integritu a dostupnost telemetrického systému a zabránit kompromitaci kryptografických mechanismů.

2. Rozsah

Proces se vztahuje na:

- Šifrovací klíče pro data at rest (databáze, zálohy).
- Klíče a certifikáty pro TLS komunikaci (API, backend).
- Podpisové klíče pro firmware a software (Code Signing).
- Klíče používané v CI/CD pipeline a provozních systémech.

3. Životní cyklus kryptografických klíčů

- **3.1 Generování:** Klíče jsou generovány výhradně pomocí schválených kryptografických knihoven. Používají se kryptograficky bezpečné generátory náhodných čísel (CSPRNG). Délka klíčů a algoritmy musí odpovídat *Kryptografické politice*.
- **3.2 Distribuce:** Přenos klíčů probíhá pouze přes šifrované kanály (TLS, SSH) nebo prostřednictvím zabezpečeného Key Vaultu. Přímé sdílení klíčů e-mailem nebo v repozitářích je zakázáno.
- **3.3 Uložení:** Klíče jsou ukládány odděleně od dat, která chrání. Produkční klíče musí být uloženy v HSM nebo schváleném Key Vault řešení. Uložení klíčů v kódu (hardcoding) je přísně zakázáno.

- **3.4 Používání:** Každý klíč má jednoznačně definovaný účel. Použití klíče k jinému účelu, než pro který byl vytvořen, je zakázáno. Přístup ke klíčům je řízen principem least privilege.
- **3.5 Rotace a expirace:** Klíče a certifikáty jsou rotovány periodicky dle stanovených lhůt nebo okamžitě při podezření na kompromitaci. Expirace certifikátů musí být monitorována automatizovaně.
- **3.6 Archivace a obnova:** Šifrovací klíče nutné pro obnovu dat jsou bezpečně zálohovány (key escrow). Podpisové klíče se po vyřazení archivují pouze pro ověření historických verzí.

4. Správa podpisových klíčů pro firmware (Code Signing)

(Reakce na RISK-FW-01)

- **Oddělení klíčů:** Produkční a testovací podpisové klíče musí být striktně odděleny.
- **Offline ochrana:** Kořenový podpisový klíč je uložen offline nebo v HSM s MFA.
- **Schvalování:** Každý akt podepsání firmware vyžaduje schválení Vedoucím IT.
- **Logování:** Všechny podpisové operace jsou auditně logovány.

5. Správa TLS certifikátů (Backend, API)

- **Centrální evidence:** IT Administrátor udržuje seznam všech certifikátů.
- **Monitoring expirace:** Automatická upozornění minimálně 60 a 30 dní před expirací.
- **Výměna certifikátů:** Probíhá řízeně dle *Politiky řízení změn*.
- **Důvěryhodnost:** Používají se pouze certifikáty vydané důvěryhodnou CA.

6. Postup při kompromitaci kryptografického klíče

Při podezření na kompromitaci se postupuje bezodkladně:

1. **Revokace:** Okamžité zneplatnění klíče nebo certifikátu (CRL / OCSP).
2. **Rotace:** Vygenerování a nasazení nové sady klíčů.
3. **Analýza dopadů:** Vyhodnocení vlivu na data, firmware a komunikaci.
4. **Incident management:** Postup dle *Směrnice pro řešení bezpečnostních incidentů*.

7. Odpovědnosti

- **Vedoucí IT / Security Officer:** Definuje standardy správy klíčů, schvaluje přístup k citlivým klíčům, odpovídá za soulad s ISMS.
- **IT Administrátor:** Spravuje Key Vault / HSM, zajišťuje rotaci a monitoring expirací.

- **Lead Developer:** Odpovídá za správnou implementaci kryptografie, zajišťuje, že klíče nejsou součástí zdrojového kódu.

8. Auditní důkazy

Organizace uchovává:

- Záznamy o generování, rotaci a revokaci klíčů.
- Logy přístupů ke Key Vaultu / HSM.
- Seznam platných a zneplatněných certifikátů.
- Schvalovací protokoly k podpisu firmware.