Kryptografická politika (Cryptographic Policy)

Verze: 1.0

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / Vedoucí IT

Vazba na ISO/IEC 27001:2022:

- A.8.24 – Používání kryptografických kontrol

---

1. Účel

Účelem této politiky je stanovit závazná pravidla pro používání kryptografických mechanismů k ochraně důvěrnosti, integrity a autenticity informačních aktiv organizace, zejména v prostředí telemetrických systémů a backendové infrastruktury.

2. Schválené kryptografické standardy

Organizace povoluje výhradně průmyslově uznávané, aktuálně bezpečné kryptografické algoritmy. Používání vlastních, experimentálních nebo považovaných za prolomené algoritmy je zakázáno.

Účel	Minimální standard	Poznámka
Šifrování dat v klidu (at rest)	AES-256	Databáze, zálohy
Šifrování přenosu (in transit)	TLS 1.2 / TLS 1.3	API, webové rozhraní
Digitální podpisy	RSA ≥ 3072 bit / ECC	Code signing firmware
Hašování hesel	Argon2 / bcrypt	Povinný salt

Zakázané algoritmy: MD5, DES, 3DES, RC4, SHA-1 a ekvivalentní.

3. Digitální podepisování firmwaru

(Reakce na RISK-FW-01)

- **Povinnost podpisu:** Každá distribuovaná verze firmwaru (FW-01) musí být digitálně podepsána schváleným podpisovým klíčem.
- **Ověření integrity:** Telemetrická jednotka musí ověřit platnost podpisu před instalací aktualizace.
- **Zákaz obcházení:** Instalace nepodepsaného nebo nevalidního firmwaru do produkčního prostředí je zakázána.

4. Správa kryptografických klíčů

Správa klíčů je považována za kritický bezpečnostní proces.

- **Generování:** Klíče musí být generovány v prostředí s dostatečnou entropií a řízeným přístupem.
- **Uložení:** Soukromé klíče nesmí být ukládány do zdrojového kódu, repozitářů ani konfiguračních souborů. Preferováno je použití HSM, cloudového Key Vaultu nebo šifrovaného trezoru.
- **Rotace:** Klíče a certifikáty musí být rotovány pravidelně dle jejich typu nebo bezodkladně při podezření na kompromitaci.
- **Zálohování klíčů:** Klíče nezbytné pro obnovu dat mohou být zálohovány pouze řízeným způsobem (key escrow) s omezeným přístupem.

5. Kryptografie v telemetrické komunikaci

- **Vrstvená ochrana:** Šifrování TLS je kombinováno s izolací komunikace pomocí privátní APN nebo VPN.
- **Certifikáty:** API a backendové služby používají certifikáty vydané důvěryhodnou certifikační autoritou (CA).
- **Autentizace:** Identita zařízení i backendu musí být ověřena pomocí certifikátů nebo jiných kryptografických prostředků.

6. Odpovědnosti

- **Vedoucí IT:** Schvaluje kryptografické standardy a výjimky (pokud jsou povoleny).
- **Vývojový tým:** Odpovídá za správnou implementaci kryptografie a zákaz hard-codingu klíčů.
- **IT Administrátor:** Odpovídá za správu certifikátů, jejich platnost a včasnou obnovu.

7. Auditní důkazy

Pro potřeby auditu jsou uchovávány:

- Seznam schválených algoritmů a minimálních délek klíčů.
- Evidence podepsaných verzí firmwaru.
- Záznamy o rotaci a správě klíčů.
- Přehled platnosti TLS certifikátů.