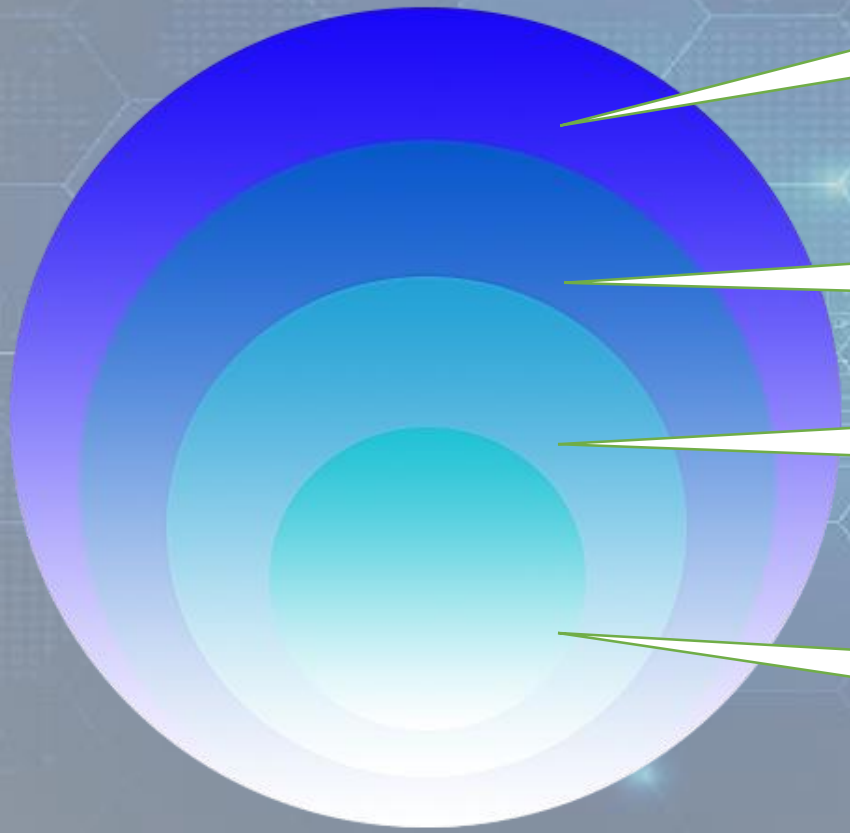
Jak elegantně splnit požadavky na bezpečné uložení a separaci šifrovacích klíčů

Jan Géring
technický konzultant pro kybernetickou bezpečnost

IDnomic THALES nextsense ASKON international s.r.o.

Ochrana perimetrů



Fyzický přístup

Přístup do infrastruktury

Přístup k aplikacím

Přístup k datům

Ochrana přístupu k datům

- Posledním perimetrem, finálním bodem, který potřebujeme ochránit jsou data samotná. Jedná se především o know-how společností, citlivé údaje, které by neměly být dostupné kde komu, ale hlavně by neměly být v takové podobě, aby byly zneužitelné v případě útoku na infrastrukturu.

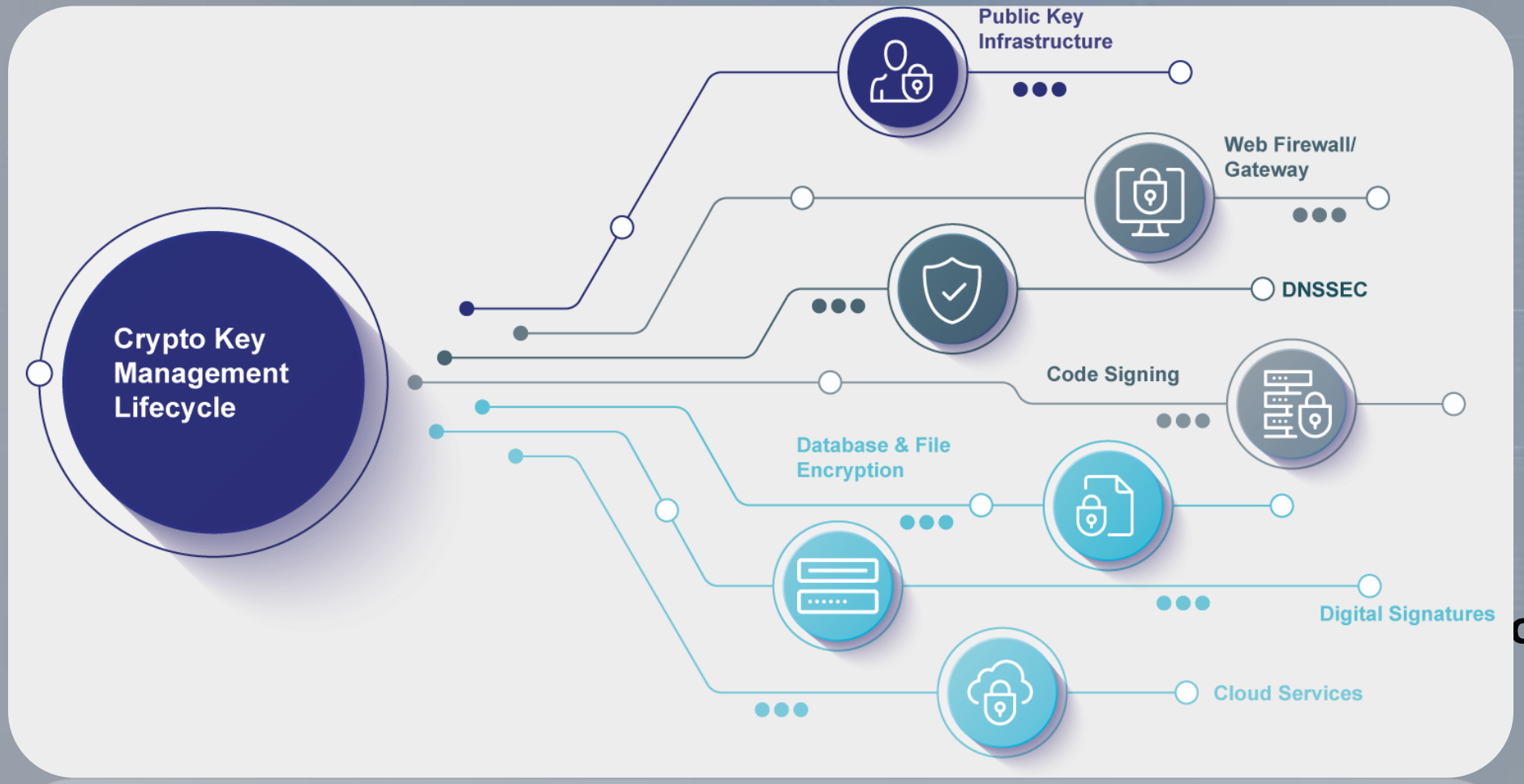
Požadavky a nařízení

- 181/2014 Sb. Zákon o kybernetické bezpečnosti - Vyhláška č. 82/2018 Sb.
- Obecné nařízení o ochraně osobních údajů - GDPR
- TISAX

Proč mít separované a spravované šifrovací klíče?

- Ochrana infrastruktury
- Ochrana know-how
- Při kompromitaci stroje získá útočník pouze šifrovaná data bez klíče
- Jsme schopni definovat politiky přístupu ke klíči
- Můžeme bezpečně verzovat a rotovat klíče
- Klíč máme bezpečně v naší režii
- V případě uložených dat v cloudu nám stačí zahodit šifrovací klíč, bez obav, že se k datům dostane Cloud Provider

Platforma CipherTrust



ovat data

IDnomic THALES nextsense ASKON international s.r.o.

Příklady nasazení z praxe

- Nejjednodušší způsob separace klíčů – KMIP
- Transparent Data Encryption + Live Data Transformation
- DB encryption - Native DB Encryption, Column Based-Line Based
- Tokenizace dat – Vault / Vaultless

Životní cyklus klíče

Dokážete si odpovědět na otázky

- JAK šifrovat
- KDY šifrovat
- KDO by měl mít přístup
- CO budeme šifrovat
- KDE budou šifrovací klíče
- a za JAKÝCH podmínek budou přístupné?

V případě dalších dotazů se na mě neváhejte obrátit.

Mgr. Jan Géring
technical consultant
Askon International s.r.o.
jgering@askon.cz