NOREG

MARGARÉTA A TANÚSÍTVÁNYOK ÁTFOGÓ MENEDZSMENTJÉHEZ

Növekvő igény a felhasználók és az eszközök azonosítására

A Ponemon Institute 2022-es nemzetközi felmérésében a megkérdezett IT-szakemberek **66%**-a azt válaszolta, hogy egyre több tanúsítványt használnak informatikai környezetükben.

A felhasználók és eszközök közötti titkosított kommunikáció és azonosítás megvalósítása során a szervezetek nagy számú kriptográfiai kulcsra és digitális tanúsítványra támaszkodnak. Ugyanakkor a szakemberek a szükséges bizalom kiépítésével párhuzamosan egyre összetettebb kihívásokkal néznek szembe. Hatékony megoldásra van szükségük a kulcsok és tanúsítványok életciklus kezeléséhez.

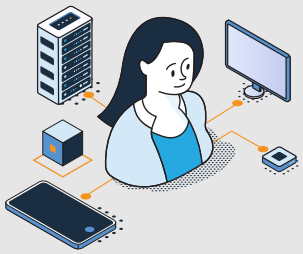


Milyen problémákat vethet fel a tanúsítványok nem megfelelő életciklus menedzsmentje?



ÁLTALÁNOS KIHÍVÁSOK

- A szervezeten belül eltérő folyamatok mentén, akár több különböző forrásból is beszerezhetők a tanúsítványok.
- Nehezen követhető, hogy milyen tanúsítványokat használnak a szervezetben és azok milyen jellemzőkkel rendelkeznek.
- Információ hiányában nehézkes az esetleges problémák felderítése és azok hatékony megoldása.



MUNKATÁRSAKAT ÉRINTŐ PROBLÉMÁK

- A távozó kolléga titkosított levelezéséhez nem fér hozzá a menedzsment.
- A távozó kolléga tanúsítványai továbbra is érvényesek maradnak.
- A számítógép váratlan meghibásodása esetén a felhasználó nem fér hozzá a titkosított állományokhoz.
- Otthon felejtett kulcshordozó esetén az érintett kolléga aznap nem tudja elvégezni a feladatait.
- A tanúsítványok kiadását és a titkosító kulcsok visszaállítását egyetlen személy végzi.



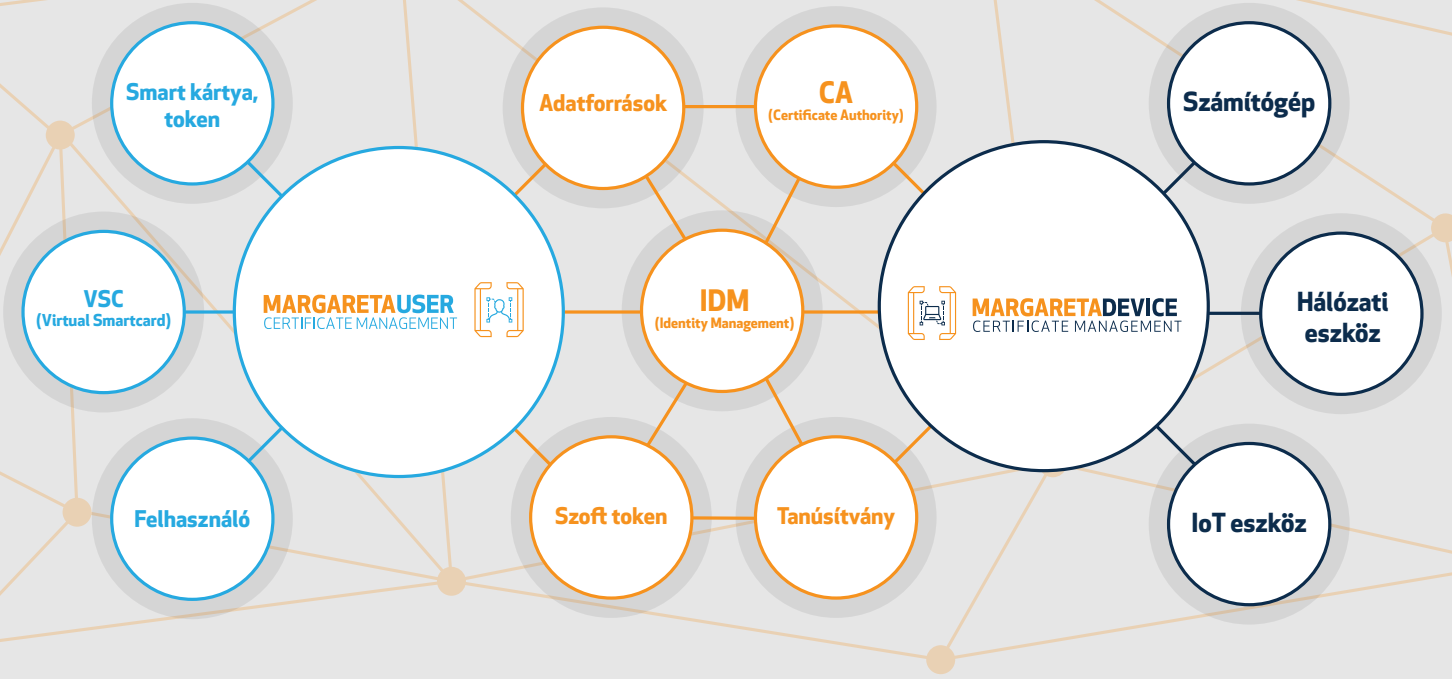
ESZKÖZÖKET ÉRINTŐ KIHÍVÁSOK

- Lejáró tanúsítványok okozta üzemeltetés- és szolgáltatáskiesés, amely hírnév vesztést és közvetlen anyagi kárt eredményezhet.
- Nehézkes a tanúsítványok eszközökbe történő betöltése.
- Problémás a tanúsítványok üzemeltetőhöz rendelése.

A MARGARÉTA MEGOLDÁST JELENT A FENTI PROBLÉMÁKRA!

NOREG

A MARGARÉTA MODULJAI



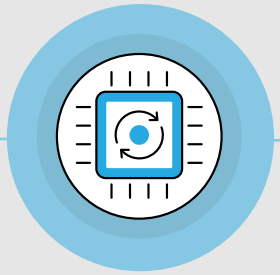
A Margaréta egységes eszközt biztosít a tanúsítványok és kulcstároló eszközök teljes életciklusának kezelésére. Magas fokú automatizálás mellett valósítja meg a tanúsítványmenedzsment összes feladatát.

A Margaréta nemcsak egy általános kártya- és tanúsítványmenedzsment rendszer, hanem egy olyan megoldás, amely alkalmas a PKI folyamatokhoz kapcsolódó valamennyi rendszer és eszköz összekötésére.

MODUL	MARGARETAUSER CERTIFICATE MANAGEMENT	MARGARETADEVICE CERTIFICATE MANAGEMENT
MIT NYÚJT?	Átláthatóságot, központi nyilvántartást és menedzsmentet biztosít a vállalat valamennyi felhasználói tanúsítványához, azok származásától függetlenül	Több ezer IoT és egyéb eszköz részére biztosít automatizmusokat a tanúsítványok kiadására, visszavonására és megújítására, elkerülendő az alapértelmezett vagy azonos tanúsítványok hosszútávú alkalmazását.
KINEK AJÁNLOTT?	Olyan, sok felhasználóval rendelkező vállalat számára ideális, amely már rendelkezik tanúsítványokkal és emelni szeretné az üzleti folyamatok biztonsági szintjét.	Olyan vállalat számára ajánlott, amely az üzleti és IoT folyamatokban sok eszközt, berendezést használ, melyekkel fontos a biztonságos kapcsolat.

NOREG

A MARGARÉTA FUNKCIÓI



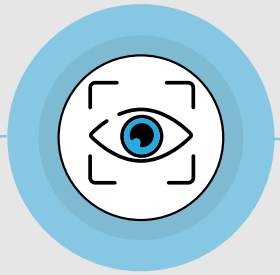
AUTOMATIZÁLÁS

A beépített automatizmusoknak köszönhetően minimalizálható az emberi erőforrás igény, csökken az üzemeltetési költség, a támogatás szükséglet és a hibalehetőségek száma.

HATÉKONYSÁG

A különböző tanúsítványok tárolására elegendő egyetlen kulcshordozó eszköz, ami lehet virtuális vagy fizikai kártya, token, de akár az operációs rendszer tárolója is. Az otthon felejtett eszközök helyettesítése is egyszerű: egy ideiglenes kártya kiadása egyetlen perc.





ÁTLÁTHATÓSÁG

A vállalat külső és belső tanúsítványainak szinkronizált nyilvántartása átláthatóvá teszi, hogy az egyes felhasználók és eszközök milyen tanúsítványokkal rendelkeznek és azok honnan származnak. Riportok alkalmazásával elemzések és statisztikák készíthetők.

KULCS MENEDZSMENT

A titkosító kulcsokat és tanúsítványokat képes biztonságosan archiválni és szükség esetén visszaállítani. Távoli és operátori megújítás is elérhető.





BIZTONSÁG

A kulcsokat és érzékeny adatokat kriptográfiai modul védi, illetve az agent-alapú megvalósítás lehetővé teszi a PKI környezet kritikus elemeinek leválasztását a felhasználók által elérhető zónáktól. Támogatja a négy szem elvű hozzáférést.

INTEGRÁCIÓ

Beépített és egyedi integrációs modulokat is támogat, így az általánosan elterjedt standard megoldásokon túl bármilyen környezetbe illeszthető: legyen szó akár vállalati címtárakról, egyedi IDM interfészről, vagy külső hitelesítésszolgáltató tanúsítványairól.



NOREG

az információbiztonsági technológiák és szolgáltatások **SZAKÉRTŐJE**

20+ év PKI és **10+** év tanúsítványmenedzsment **TAPASZTALAT**

SAJÁT PKI MEGOLDÁSOK és elektronikus aláírás termékek

bizalmi szolgáltatók és vállalati PKI rendszerek kiépítésében és azok **FOLYAMATOS TÁMOGATÁSÁBAN** vesz részt

AKTÍV TAGJA az informatikai biztonsági és nemzetközi PKI szakmai közösségeknek

ÜGYFELEI között megtalálhatók a pénzügyi, távközlési, államigazgatási, ipari és kereskedelmi szektor vezető vállalatai

1118 Budapest, Rétköz u. 5.

+36 1 438 6380

Linkedin