Két faktoros azonosítás USB alapon

Az **eToken** egy olyan USB eszköz, amely adatvédelmi célokra lett kifejlesztve. Rendkívül könnyen telepíthető és használható IT biztonsági megoldás. A vállalati dolgozó kap egy olyan kézzel fogható hardveres eszközt amelyet mindig magánál hord, nyakába akaszthatja és segítségével biztonsági műveleteket tud elvégezni. A PKI technológia használatával lehetőségük van olyan hálózatokon hiteles és biztonságos kommunikáció megvalósítására, ahol a környezet egyébként nem biztonságos. Segítségével megvalósítható a bizalmas és titkosított információkhoz történő hozzáférés a felhasználók pontos azonosítása által.

Nagy **előnye** az eszköznek, hogy

- használatához csak a számítógép USB portjába kell helyezni és nincs szükség kártyaolvasóra.
- nagy mennyiségű jelszó, digitális tanúsítvány helyezhető el az eszközön. Ezek segítségével lehetőség van tanúsítvány alapú VPN (virtuális magánhálózat) elérésre.
- laptopok védelmére is használható, mivel a két-faktoros azonosítást az együttesen érvényesülő két feltétel - birtoklás (eToken) és tudás (eToken jelszó) - kizárólagos teljesülésével valósítja meg.
- típustól függően lehetőség van pendrive-ként is használni vagy manuálisan kódot generálni az eszközön a még biztonságosabb használat érdekében.
- amint kihúzzuk a számítógépből, nem lehet hozzáférni a rajta lévő adatokhoz, mivel a Windowsba való visszalépéshez kéri az eToken jelszavát.

Lehetőség van arra, hogy az eszköz segítségével bejelentkezzünk Windows környezetbe, különböző alkalmazásokba, és webes oldalakra biztonságosan tanúsítvány alapon. Mikor bejelentkezünk az első alkalommal, megjegyzi a kívánt jelszavakat és rárija magára az eszközre, majd a későbbiekben már nem lesz szükség ezeknek a beírására. A belépéshez szükséges tanúsítványok és jelszavak közvetlenül az eTokenre kerülnek. Így nincs lehetőség arra, hogy illetéktelen kezekbe kerüljenek a személyes adatok.

Token Management

Abban az esetben ha nagyobb felhasználói létszámmal rendelkezünk, szükség van egy olyan menedzsment eszközre, amely a használatban lévő biztonsági eszközök ellenőrzését és kezelését végzi. Mikor feltelepítjük, létrehozunk egy Token Policy-t az Active Directory-ban, amely segít abban, hogy az egyes felhasználói csoportokba tartozó emberek milyen beállításokkal kapják meg az eToken eszközöket. Ez a Policy meghatározza, hogy melyik felhasználó mihez férhet hozzá, milyen jogosultságokkal rendelkezik a vállalaton belül.

Az eToken fontosabb felhasználási területei:

- ✓ Titkosított kommunikáció, elektronikus levelezés
- ✓ Biztonságos web hozzáférés, eBusiness tranzakciók
- ✓ Biztonságos kulcsgenerálás
- ✓ Számítógéphez való hozzáférés, bejelentkezés
- ✓ Bizalmas vállalati dokumentumok aláírása és/vagy titkosítása
- ✓ Webes alkalmazások elérése,
- ✓ Biztonságos távoli elérés (RAS)
- ✓ Tanúsítvány alapú VPN(virtuális magánhálózat) elérés
- ✓ Nem PKI kompatibilis alkalmazások esetén a jelszó biztonságos tárolása
- ✓ SSL VPN, IPsec VPN