



## Erős azonosítás és titkosított adattárolás egy eszközön

A hagyományos felhasználónév/jelszó alapú azonosítás nem határozza meg egyértelműen a felhasználót, hiszen akár idegen személlyel is megoszthatóak a bejelentkezéshez szükséges adatok. Az erős azonosítás azonban úgynevezett kétfaktoros azonosításra épül, ahol nem elegendő ismerni a felhasználó nevét és jelszavát, hanem birtokolni kell magát az azonosító eszközt is. Bevezetésével az alkalmazás, hálózati és távoli elérések sokkal biztonságosabbá tehetőek, illetve megvalósítható a single-sign-on hozzáférési elv, ahol a felhasználó egy eszközzel lesz képes elérni a vállalat összes erőforrását.

Az adatokat tartalmazó USB alapú hordozók elvesztésének, lopásának kockázata igen jelentős. Számos nemzetközi tanulmány mutat rá az eszközzel együtt elveszített adatok illetéktelen kézbe kerülésének veszélyeire, amelyek a vállalat jó hírnevének és az ügyfelek bizalmának elvesztésétől egészen a komoly kártérítési perekig és bírságokig terjedhetnek. A legfontosabb szabványok és ajánlások, mint a Sarbanes - Oxley (SOX), PCI vagy a HIPAA is rendelkezéseket vagy elvárásokat tesznek az érzékeny adatok megóvása érdekében.

A Gemalto olyan eszközt ad a biztonsági szakemberek kezébe, amely segítséget nyújt a két funkció, az erős azonosítás és a titkosított adattárolás egy eszközön történő, egyszerű és költséghatékony megvalósításához.

### Smart Enterprise Guardian (SEG)

A Smart Enterprise Guardian egy személyi, chipkártyás azonosító- és egy titkosított, USB adattároló integrációja. A szabványos, USB kulcs méretű eszközön tárolhatóak az erős azonosításhoz szükséges tanúsítványok és hitelesítő adatok, mely lehetőséget biztosít a hagyományos PKI szolgáltatások igénybe vételére, az azonosításon túl például elektronikus aláírásra, dokumentumok vagy fájlok titkosítására.

A Smart Enterprise Guardian rendelkezik egy nagykapacitású flash tárolóval is, így pendrive-ként képes a hitelesítő adatoktól szeparáltan, titkosítottan tárolni a felhasználók bizalmas dokumentumait és állományait.

Az eszköz a Gemalto .NET technológiájának köszönhetően maximálisan együttműködik a Microsoft infrastruktúrákkal, mert a Windows operációs rendszerek tartalmazzák a működéséhez szükséges drivereket. Még az erős azonosítás használatához sem kell megszemélyesítő és middleware alkalmazást telepíteni a munkaállomásokra, így a Smart Enterprise Guardian a legkényelmesebben használható és legegyszerűbben integrálható hordozható személyi biztonsági eszköz (PPSD).

A Smart Enterprise Guardian használata nem igényel külön oktatást. Egyszerű és magától érthető kezelhetősége nagyban segíti a bevezetési folyamatokat és a felhasználók részéről az eszköz elfogadását.



## A Smart Enterprise Guardian legfontosabb funkciói és jellemzői

- A kliens oldalon nincs szükség megszemélyesítő alkalmazás vagy driver telepítésére,
- Alkalmos tanúsítvány alapú erős azonosításra, elektronikus aláírásra és dokumentum titkosításra,
- Képes egyszer használatos, dinamikus jelszavak (OTP) generálására,
- Együttműködik a Microsoft Identity Lifecycle Manager-rel,
- 256 bites AES titkosítással védi a felhasználó dokumentumait és állományait,
- Transzparens, a felhasználó számára láthatatlan titkosítási folyamatokat biztosít.

## A Smart Enterprise Guardian előnyei

### Egyszerű integráció és adminisztráció

A Gemalto .NET technológiája lehetővé teszi, hogy az integráció a legkevesebb változtatást igényelje a hálózatban. A Microsoft rendszerek tartalmazzák az eszköz működéséhez szükséges meghajtókat, így nincs szükség megszemélyesítő alkalmazások telepítésére.

A Smart Enterprise Guardian a nagy és közepes vállalatok mellett a kisvállalatok és egyéni felhasználók igényeit is egyszerűen tudja kiszolgálni. A nagyvállalatok komplex rendszerében a Smart Enterprise Guardian együtt tud működni a Microsoft Identity Lifecycle Manager smartcard-menedzsment eszközzel, míg a kisebb vállalatok és egyéni felhasználók részére a Gemalto Allynsis Device Administration vagy Token Lifecycle Manager megoldása biztosítja az eszközök kiadását, visszavonását és menedzsmentjét.

### Együttműködés más alkalmazásokkal

A Smart Enterprise Guardian tökéletesen együttműködik a Microsoft Windows domain logon és az Office dokumentum-aláírási és e-mail titkosítási szolgáltatásaival. Használatával erős azonosításhoz köthető a titkosított fájlrendszerek használata (EFS), tartalmaz egy egyszeri és dinamikus jelszó (OTP) generátor funkciót, amely megfelel az Open Authentication szabványoknak.

Mivel a SEG eszköz egy Gemalto .NET smartkártyára épül, ezért a Microsoft operációs rendszerek alapértelmezetten támogatják használatukat. A Microsoft Base Smart Card kriptográfiai szolgáltatás (Base CSP) elérhető a Windows Vista és Windows XP rendszereken, ezért a használatukhoz nincs szükség megszemélyesítő alkalmazás telepítésére.

A Smart Enterprise Guardian együttműködik a legnagyobb vállalati hozzáférés-szabályozó rendszerekkel is, integrálható a Microsoft Forefront, Citrix Access Gateway™, Citrix Password Manager™ és Lumension Security Certified Sanctuary Device™ eszközökkel.

### Titkosított adattárolás

A 256 bites AES kódolással titkosított adatterületen tárolt dokumentumokhoz és fájlokhoz csak a felhasználó férhet hozzá. A titkosítási folyamat láthatatlanul, az eszközre másolás közben történik meg, így nem igényel felhasználói beavatkozást.

Az Ön viszonteladója: