

Fizikai beléptetés és követés

Vizuális azonosítás

A Gemalto smartcard-alapú eszközök a kártyák egyedi grafikai arculata alapján lehetővé teszik a vizuális azonosítást. A céges arculatnak megfelelően nyomtatott kártyatest kiegészíthető sorszámmal, névvel, biztonsági színkóddal és színes fényképpel, mely az élőerős őrség számára elősegíti a felhasználó felismerését.

Elektronikus azonosítás, beléptetés és követés

Az elektronikus beléptetés biztosítja a szervezet központosított, kapu- vagy zónarendszerű fizikai beléptető rendszerének a jogosultságok szerinti működtetését, a belépések naplózását, illetéktelen belépési kísérlet esetén pedig az őrség azonnali riasztását. A Gemalto intelligens smartcard eszközei contact vagy contactless (proximity kártyás) módokon képesek együttműködni a beléptető rendszerekkel, így bármely meglévő vagy újonnan kiépítendő megoldáshoz könnyedén hozzáilleszthetők, lehetőséget biztosítva a munkatársak épületen belüli mozgásának szabályozásához és követéséhez.

Logikai beléptetés és hozzáférés-védelem

Tanúsítvány-alapú és biometrikus belépés (login)

A smartcard alapú logikai beléptetés a megszokott felhasználónév/jelszó megadása helyett a kártyán tárolt tanúsítvány segítségével és egy személyi PIN kód megadásával történik. Háromfaktorú azonosítás esetén szükséges az ujjlenyomat megadása is, melyhez a biometriai adatok a kártyán titkosítva tárolódnak, és csak a sikeres azonosítás után történik meg a belépés a számítógépbe.

Védett intra- és extranet-oldalak elérése

Gemalto smartcard személyi azonosítóeszközök használatával biztonságosabbá tehető a vállalati intra- és extranet oldalak elérése. A Gemalto eszközei a tanúsítvány-alapú belépést és dinamikusan generált, egyszer használatos jelszavak (OTP) használatát egyaránt lehetővé teszik.

Távoli bejelentkezés, VPN, Citrix

Erős azonosítás használatával lehetőség van olyan hálózatokon hiteles és biztonságos kommunikáció megvalósítására, ahol a környezet egyébként nem megbízható. A Gemalto smartcard és token eszközeinek segítségével tanúsítvány-alapú vagy egyszer használatos, akár SMS jelszavas (OTP) VPN és Citrix kapcsolatok építhetők ki, és megvalósítható a biztonságos távmunka.

OWA – Outlook Web Access

A Gemalto smartcard vagy token eszközeinek segítségével biztonságossá tehető az Outlook webes elérése, hiszen erős azonosítás, tanúsítvány vagy egyszer használatos (akár SMS alapú) jelszó (OTP) használata mellett szavatolható, hogy csak az illetékes és engedélyezett személyek férhessenek hozzá a rendszerhez.



Integrált alkalmazási lehetőségek

HR menedzsment, munkaidő nyilvántartás

Az elektronikus beléptető vagy kapu- és zónarendszerek használatával leegyszerűsíthető a munkaidő-nyilvántartás. A beléptető és a nyilvántartó rendszer integrációja biztosítani tudja a munkáltató számára a pontos és gyors munkaidő-elszámolás lehetőségét, mert a munkavállalók épületen belüli mozgása, illetve az érkezések és távozások időpontja is naplózható és követhető.

Titkosított adattárolás

A Gemalto Smart Enterprise Guardian (SEG) és Smart Guardian (SG) megoldásai a smart card technológiát és a biztonságos adattárolási funkciókat ötvözik. Az adatszivárgásra érzékeny vállalatok számára kifejlesztett eszköz segítségével megvalósíthatók az erős azonosítás és a logikai beléptetés folyamatai, de emellett az azonosítóeszköz egy titkosított területen tárolja a felhasználó adatait és állományait, így egy esetleges eszköz elvesztés sem okoz adatszivárgást.

Elektronikus aláírás és hitelesítés

A Gemalto smart card és token eszközeivel egyszerűen megvalósítható az elektronikus dokumentumok és adatok európai és magyar elektronikus aláírási jogszabályokban rögzített követelményeknek megfelelő hitelesítése.

E-banking, elektronikus fizetőeszközök

Az elektronikus banki szolgáltatások, az Interneten keresztül elérhető elektronikus kereskedelmi rendszerek rendkívül népszerű és felhasználóbarát szolgáltatást nyújtanak. A Gemalto smart card és OTP azonosító eszközei biztosítani tudják az ügyfelek magas biztonsági szintű azonosítását, védelmét, a tranzakciós műveletek biztonságos elvégzését és hitelesítését.

Diszkitkosítás (full disc encryption)

A laptopok diszkterületeinek titkosítása megakadályozza az adatok idegen kézbe jutását az eszközök elvesztése esetén is. Az adatokhoz való hozzáférést –a titkosító szoftvert kiegészítendő- smart card és token eszközök használatához köthetjük, így a felhasználó csak a megfelelő azonosító eszköz birtokában tudja elindítani a számítógépét.

Elektronikus igazolványok

A smartcard eszközök alkalmasak elektronikus igazolványként történő használatra. Mivel az elektronikus igazolvány megfelel a legmagasabb biztonsági elvárásoknak is, felhasználható állampolgári azonosító okmányként, szervezet-tagsági igazolványként, de akár alkalmazható előfizetői vagy klubtagsági azonosítóként is.

Single-sign on megoldás

A Gemalto smartcard vagy token eszköz minden esetben biztonságosan azonosítja annak használóját, ezért az eszköz tulajdonosa minden azonosítást igénylő fizikai és logikai folyamatba egységes módon léphet be. Ugyanazzal az eszközzel képes a fizikai belépésre, hálózatba történő bejelentkezésre, fájlok titkosítására és dekódolására, alkalmazások használatára vagy akár a távmunkára is.

Az Ön viszonteladója: