MICROSEC
Számítástechnikai Fejlesztő Kft.

FELHASZNÁLÓI ÚTMUTATÓ

BIZTONSÁGOS ALÁÍRÁS LÉTREHOZÓ ESZKÖZ (BALE)

GEMALTO CHIPKÁRTYA

2011. október 5.

MICROSEC SZÁMÍTÁSTECHNIKAI FEJLESZTŐ KFT.

1022 BUDAPEST, MARCZIBÁNYI TÉR 9.

TARTALOMJEGYZÉK

1 A FELHASZNÁLÓI CSOMAG TARTALMA

Az aláíró kártya átvételekor az alábbiakat kellett megkapnia:

- Biztonságos aláírás létrehozó eszköz (BALE),
- PUK levél.

1.1 A BALE kártyatípus azonosítása

A MICROSEC által a felhasználók részére biztosított biztonságos aláírás létrehozó eszköz egy bankkártya méretű, beültetett intelligens chipet tartalmazó PVC kártya.

A MICROSEC az eltérő felhasználói igények és a folyamatosan erősödő kriptográfiai követelmények kielégítése érdekében többféle aláíró eszközt is forgalmaz. Az egységes kinézet érdekében a MICROSEC azonos grafikával hozza forgalomba a kártya alapú BALE eszközeit. Az egyes kártyatípusok beazonosítása vizuálisan az alábbi azonosító információk felhasználásával lehetséges:

- A kártya előlapján (chipes oldal) a chip kontaktus alakja gyártónként eltérő. A Gemalto chip kontaktus alakja a Földgömbre emlékeztető, erősen lekerekített sarkú, 6 kontaktust tartalmaz az alábbi ábra szerint:

- A kártya hátoldalán a jobb felső sarokban egy kártyatípusonként eltérő rövid azonosító található a fenti ábra szerint, ami a Gemalto kártya esetén „eSG”.

1.2 A PUK levél

A felhasználónak a kártya átvételekor lezárt borítékban kell kapnia egy személyre szóló PUK levelet. A PUK levél felbontása előtt győződjön meg a boríték sértetlenségéről, sérült borítékot ne vegyen át!

A PUK levél a felhasználó személyes adatai mellett a kártya telepítéséhez és használatához

szükséges információkat is tartalmazza.

A PUK levél tartalmazza a TRANSPORT állapot feloldásához szükséges PUK kódot is, ami egy véletlenül generált, egyedi, 8 számjegyből álló azonosító szám. A PUK kód egy korszerű, biztonságos védelemmel ellátva egy lehúzható öntapadós átlátszó fóliára nyomtatva található a PUK levél alsó harmadán. A PUk kód a fólia eltávolítása nélkül nem olvasható, a fólia eltávolítása után az eltávolítás ténye egyértelműen látszik a címkén.

A levélen található útmutató alapján ellenőrizze, hogy a címkét még nem távolították el a levélről! A címke sérülése esetén a kártyáját ne használja! A problémát haladéktalanul jelezze ügyfélszolgálatunknak, a sérült címkéjű levelet a kártyával együtt minél előbb juttassa vissza a MICROSEC-nek.

Az átlátszó fóliát a sárga fülnél fogva óvatosan távolítsa el a levélről. A PUK kód az eltávolított fólián található, ezért azt ne dobja el, ne gyűrje össze, vigyázzon sértetlenségére. Az eltávolított fóliát egy fehér alapra helyezve a fólián olvashatóvá válik a speciális karakterekkel, halványan nyomtatott PUK kód.

A PUK címkét ragassza vissza a levélre, és/vagy a kapott PUK kódot írja fel jól olvashatóan a PUK levélre! A levélen található titkos kódokra a későbbiekben még szüksége lehet a kártya letiltása vagy blokkolt PIN feloldása esetén (lásd később).

A kártya aktiválása után a PUK levelet tartsa a kártyától elkülönülten egy biztonságos helyen!

2 A GEMALTO KÁRTYA HASZNÁLATBA VÉTELE

A kártya használatba vételéhez Önnek az alábbi feladatokat kell elvégeznie:

- PC/SC szabványt támogató kártyaolvasó üzembe helyezése (lásd 2.1 fejezet),
- .NET Framework 2.0 csomag telepítése,
- Gemalto kártyameghajtó programok telepítése (lásd 2.2 fejezet),
- e-Szignó kártyakezelő alkalmazás telepítése (lásd 2.4 fejezet),
- TRANSPORT mód feloldása (lásd 2.5 fejezet).

2.1 PC/SC szabványt támogató kártyaolvasó üzembe helyezése

A BALE kártya használatához szükséges egy PC/SC szabvány szerint működő chipkártya olvasó eszköz. A BALE kártya az alábbi kártyaolvasó eszközök használatát támogatja:

- tetszőleges PC/SC szabványnak megfelelő kártyaolvasó biztonságos PIN bevitel nélküli használatra (pl. Omnikey CardMan 3121),
- SCM Microsystems SPR532 és SPR332 kártyaolvasó kiemelt biztonságú PIN bevitelre az olvasó billentyűzetén,
- Omnikey CardMan 3621 kártyaolvasó kiemelt biztonságú PIN bevitelre az olvasó billentyűzetén.

Az olvasók a megfelelő meghajtó programokkal és telepítési útmutatókkal együtt beszerezhetők a MICROSEC Kft-nél.

2.2 .NET Framework 2.0 keretrendszer telepítése,

A Gemalto kártya meghajtó programok működéséhez szükség van az alábbi környezetek valamelyikének telepítésére:

- .NET Framework 2.0,
- .NET Framework 3.0 vagy
- .NET Framework 3.5.

A Windows XP utáni operációs rendszerek (Windows Vista, Windows 7, Windows 2003 server) megfelelő telepítés esetén tartalmazzák a keretrendszer 3.0 vagy 3.5 verzióját, így ezeknél általában nem szükséges a környezet telepítése. A Windows XP operációs rendszer nem tartalmaz semmilyen keretrendszert, így ilyen esetben, ha eddig nem volt, akkor most szükséges valamelyik támogatott csomag telepítése.

Figyelem!

A .NET Framework 4.0 nem kompatibilis a korábbi verziókkal, a Gemalto kártya meghajtó programok a 4.0 verzióval nem működnek. Ha Önnek a .NET Framewrok 4.0 van telepítve a számítógépén, akkor e mellé telepíteni szükséges valamelyik korábbi támogatott környezet, pl. a .NET Framework 2.0 verzióját is az elérhető legújabb javító csomaggal.

A .NET Framework 2.0 környezet ingyenesen letölthető például az alábbi helyről:

> Újraterjeszthető csomag a Microsoft .NET-keretrendszer 2.0-s verziójához (x86)
>
> http://www.microsoft.com/downloads/hu-hu/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5

A csomag telepítése során kövesse a megadott oldalon található részletes telepítési útmutató előírásait.

A letöltendő csomag pontos elérhetősége eltérhet a megadottól a használt számítógép konfiguráció függvényében.

2.3 A Gemalto kártya meghajtó programjainak telepítése

Amennyiben a számítógépén telepítve van a Gemalto Classic Client (vagy korábbi nevén Gemplus GemSafe Libraries) bármely verziójú programcsomagja, az új meghajtó program telepítése előtt kérjük, hogy távolítsa el azt a gépéről és indítsa újra számítógépét.

A MICROSEC egy önálló telepítő csomag formájában biztosítja a kártya használatához szükséges meghajtó programokat. Az aktuális legfrissebb meghajtó csomagok az alábbi oldalról tölthetők le:

> http://srv.e-szigno.hu/menu/index.php?lap=eSG

A telepítő csomag a Gemalto által fejlesztett Classic Client 6.1 Patch1 meghajtókat tartalmazza a MICROSEC által összeállított konfigurációban. A telepítő csomagnak két verziója létezik a 32 illetve a 64 bites Windows operációs rendszerekhez:

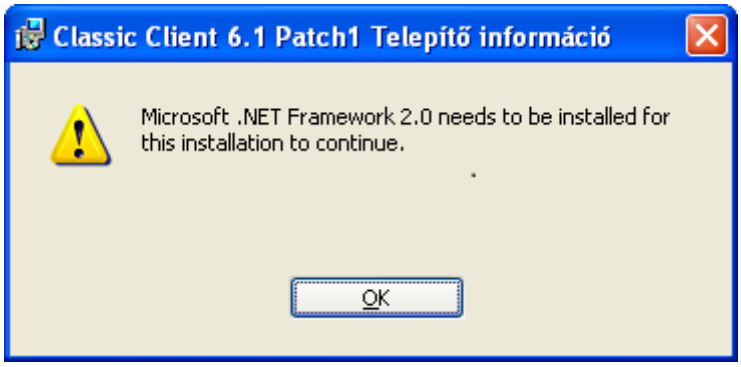
> Classic_Client_32_User_setup.msi
>
> Classic_Client_64_User_setup.msi

A támogatott operációs rendszerek:

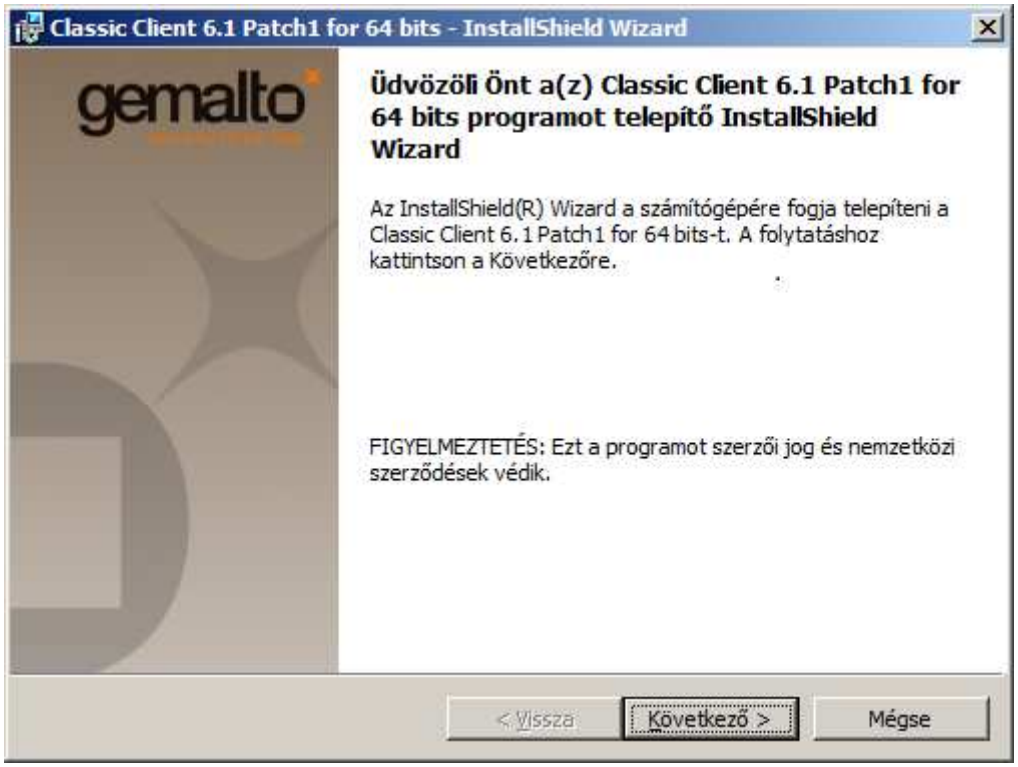
> Microsoft Windows XP, Windows Vista, Windows 7, Windows 2003 server.

A megfelelő telepítő csomag (32 bites vagy 64 bites) kiválasztása és letöltése után indítsa el a telepítő programot.

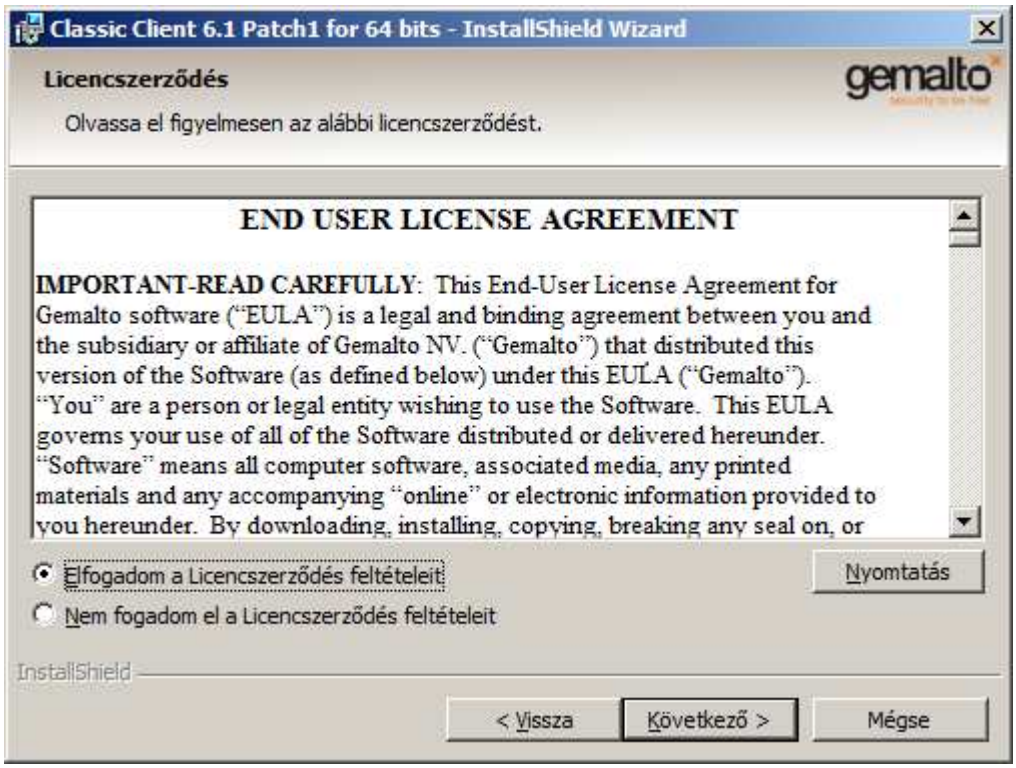
Amennyiben a számítógépen nincs telepítve a .NET Framework 2.0 verziója, a telepítő az alábbi üzenetet írja ki:



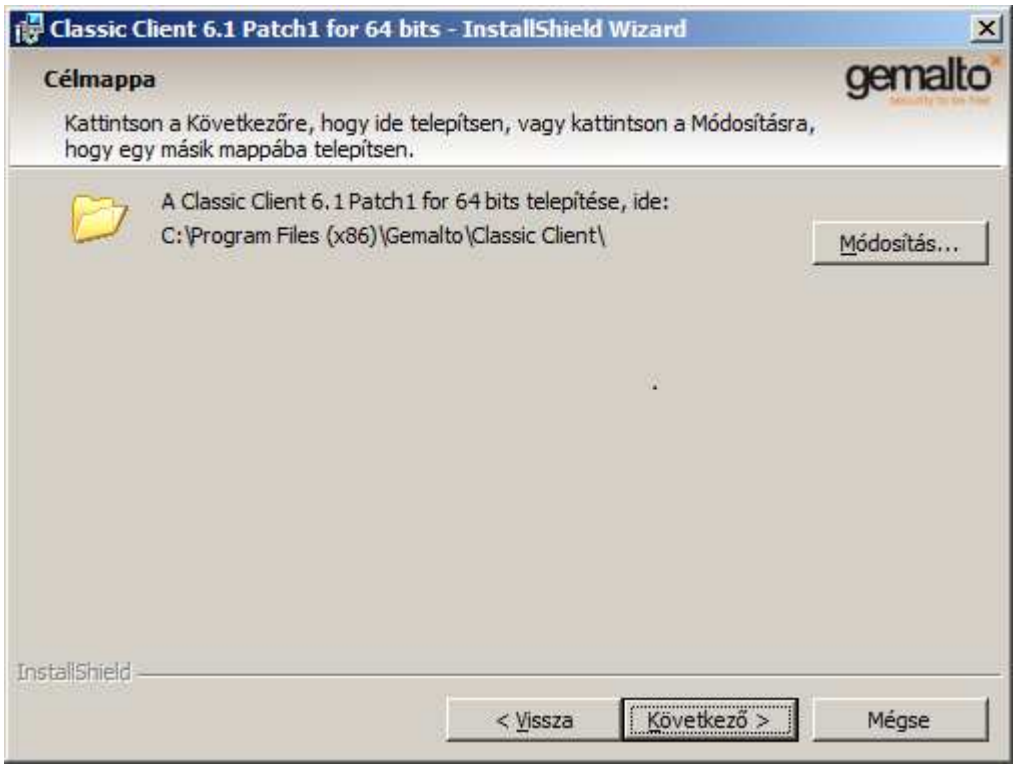
Az üzenet nyugtázása után a telepítő program leáll. Telepítse a hiányolt programot (lásd 2.2), majd indítsa újra a meghajtó program telepítését.



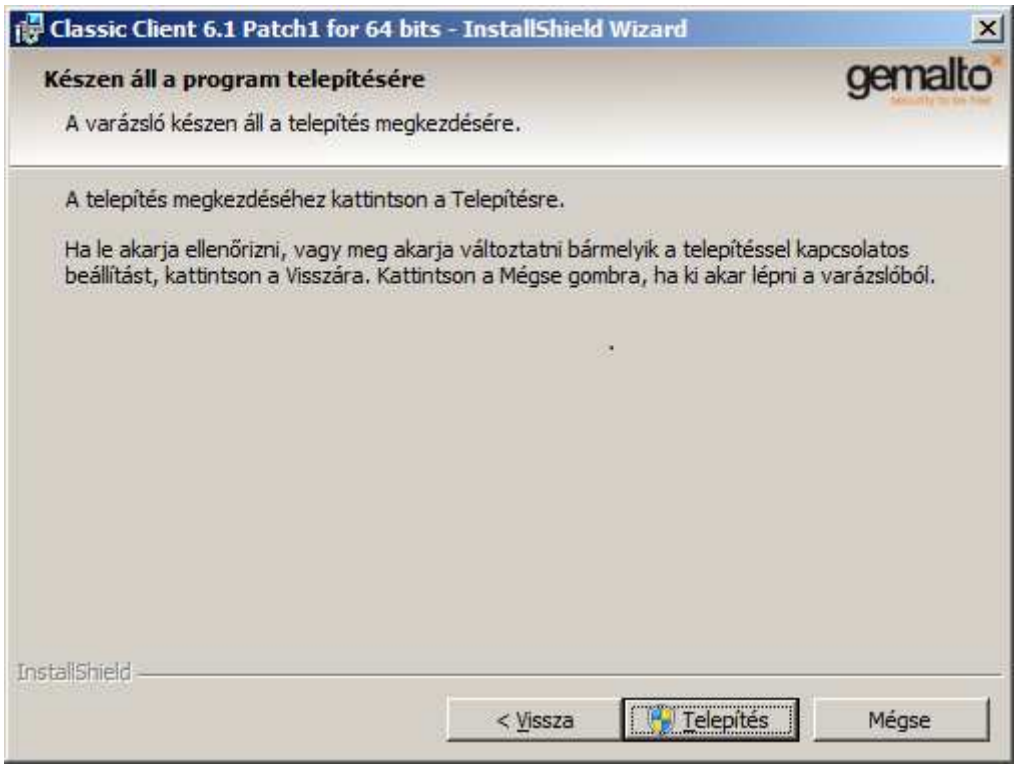
A megjelenő beköszönő ablak információinak elolvasása után kattintson a **<Következő>** gombra!



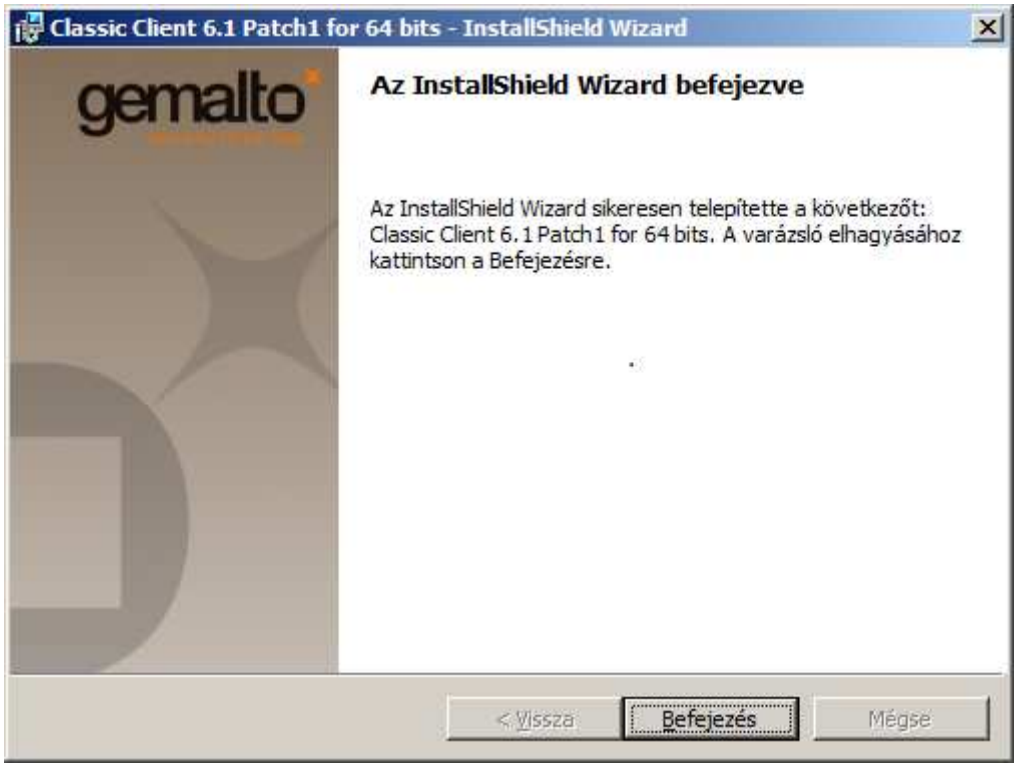
A megjelenő ablakban elolvashatja a program használatának jogi feltételeit, igény esetén ki is nyomtathatja azt. A továbblépéshez válassza ki az **<Elfogadom a Licenszerződés feltételeit>** opciót majd kattintson a **<Következő>** gombra!



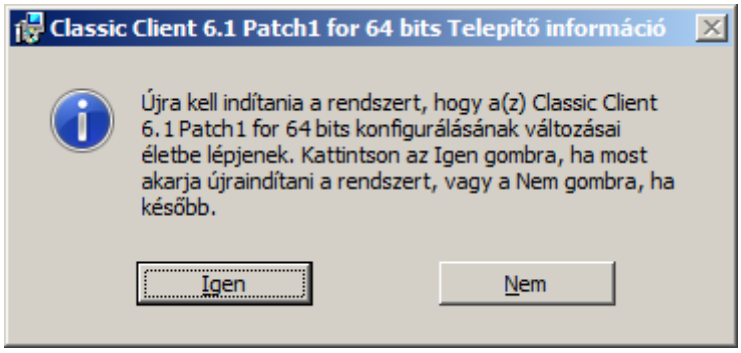
A megjelenő ablakban kiválaszthatja a program telepítésének mappáját. Amennyiben lehetséges, fogadja el a program által felkínált helyet, majd kattintson a **<Következő>** gombra!



Ha módosítani szeretné a telepítés paramétereit, itt még megteheti a **<Vissza>** gombra kattintva. A paraméterek elfogadása esetén kattintson a **<Telepítés>** gombra!



A sikeres telepítés végén általában 1 percen belül meglátja a fenti információs ablakot. A telepítés befejezéséhez kattintson a **<Befejezés>** gombra!



A telepített beállítások csak a rendszer újraindítása után lesznek érvényesek. Ha most szeretné használni a kártyáját, kattintson az **<Igen>** gombra a rendszer azonnali újraindításához, ellenkező esetben választhatja a **<Nem>** lehetőséget is.

2.4 Az e-Szignó kártyakezelő alkalmazás telepítése

Az e-Szignó kártyakezelő alkalmazás telepítésével és használatával kapcsolatos részletes információkat tartalmazó dokumentum elektronikus formában letölthető az alábbi linkről:

http://srv.e-szigno.hu/menu/index.php?lap=eSG

A felhasználói útmutató alapján telepítse számítógépére az e-Szignó kártyakezelő alkalmazást, majd indítsa újra a számítógépét.

2.5 A kártya aktiválása

Az aláíró kulcsok védelme érdekében a MICROSEC által kibocsátott kártya TRANSPORT módban van, ami megakadályozza a kártya illetéktelen használatát. A TRANSPORT módban lévő chipkártyával nem állítható elő minősített elektronikus aláírás.

A TRANSPORT állapotra az e-Szignó kártyakezelő alkalmazás minden esetben figyelmezteti a felhasználót a kártya olvasóba helyezése után. A TRANSPORT állapot a kártyakezelő alkalmazás segítségével oldható fel.

A kártya aktiválása során az alábbi műveleteket kell elvégezni:

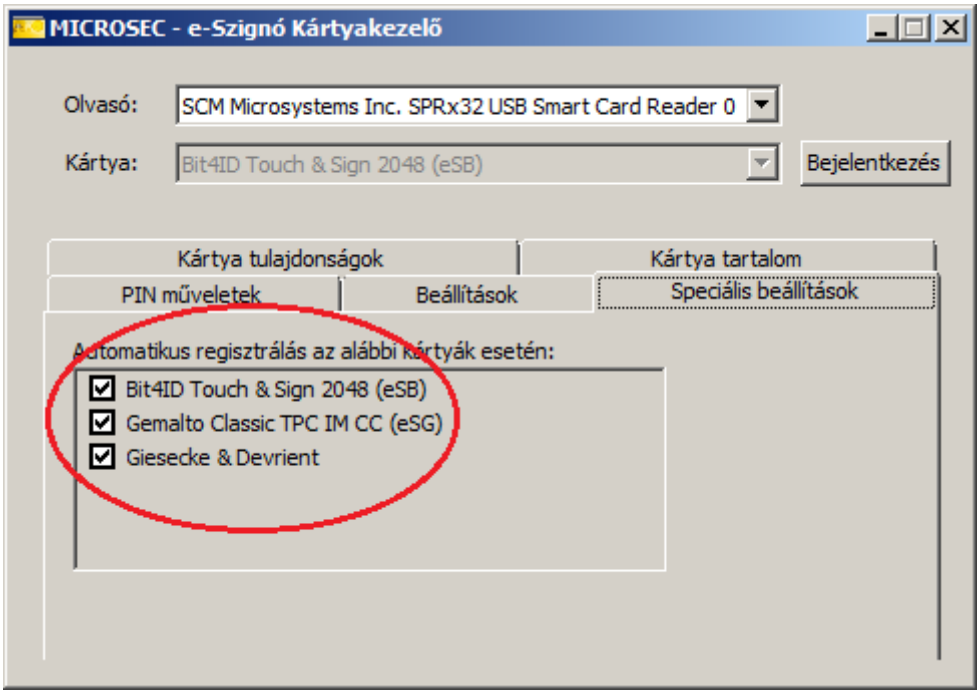
- TRANSPORT mód feloldása
- Felhasználói PIN kód beállítása.

A kényelmesebb használat érdekében az e-Szignó kártyakezelő alkalmazás a két műveletet összevontan, a felhasználó felé egy műveletnek látszóan végzi el.

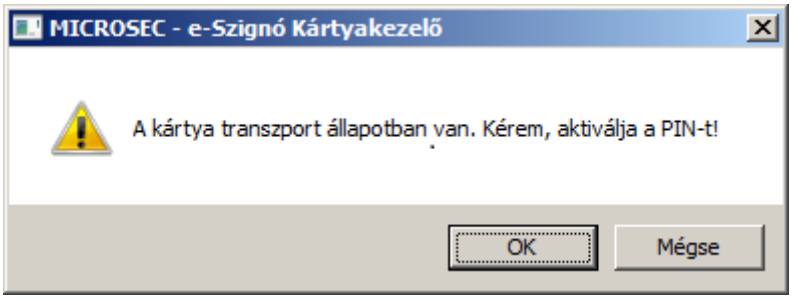
2.5.1 A TRANSPORT állapot feloldása

A kártya aktiválásához az e-Szignó kártyakezelő programnak futnia kell (kis sárga téglalap ikon jelzi a tálca értesítési területén).

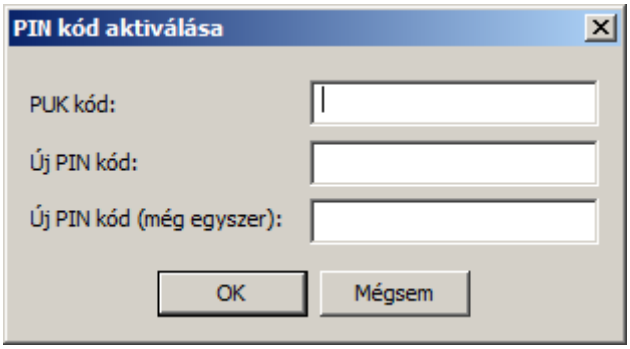
Az e-Szignó kártyakezelő alkalmazásban a **[Speciális beállítások]** panelen aktívnak kell lennie a **'Gemalto Classic TPC IM CC (eSG)'** kártya figyelése funkciónak:



A TRANSPORT állapotban lévő Gemalto kártya kártyaolvasóba helyezése után az e-Szignó kártyakezelő alkalmazás kiolvassa a kártya adatait és megjelenik az alábbi tájékoztató üzenet:

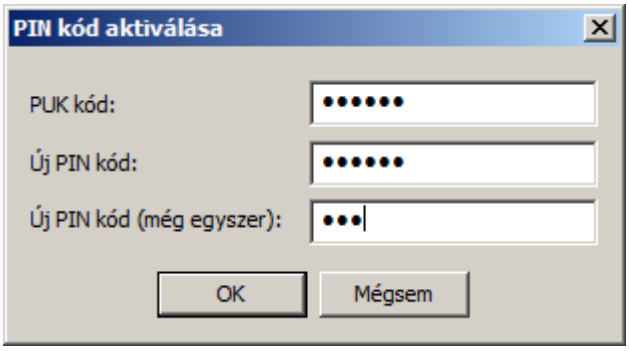


A **<Mégse>** gombra kattintva a kártya nem kerül aktiválásra, így továbbra is TRANSPORT állapotban marad. Az **<OK>** gombra kattintva megjelenik a képernyőn a kártya (PIN kód) aktiváló ablak:



Az ablakban található 3 mezőben rendre meg kell adni a PUK levélen kapott 8 számjegyű PUK kódot, majd alatta a felhasználó által választott PIN kódot kétszer egyezően.

A kódokat a számítógép billentyűzetén kell megadni. A begépelt számjegyek biztonsági okból nem kerülnek megjelenítésre, csak egy '●' karakter jelez egy bevitt számjegyet.

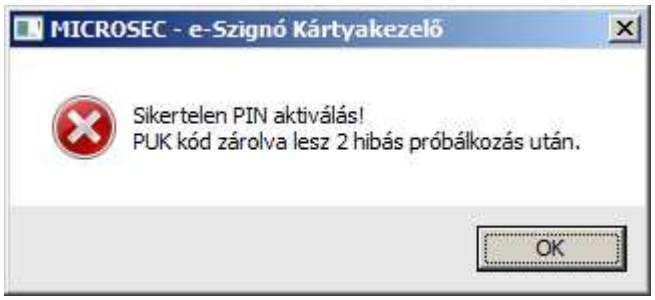


Ha elrontotta bármelyik kód bevitelét, törölje az adott mező tartalmát és kezdje újra a kód bevitelét. A **<Mégsem>** gombra kattintva kiléphet az aktiválás folyamatából és azt későbbre halaszthatja.

A kódok megadása után kattintson az **<OK>** gombra. Amennyiben a PIN kódot nem egyezően adta meg, a program erre figyelmezteti és a kártya nem kerül aktiválásra.

Törölje a PIN kód értékeket mindkét mezőből és adja meg újra.

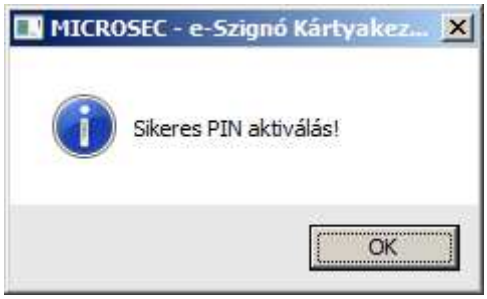
Ha hibásan adta meg a PUK kódot, a program erre figyelmezteti és kiírja a még rendelkezésére álló próbálkozások számát:



Figyelem!

A PUK kód 3-szori ismételt hibás megadása esetén a kártya blokkolt állapotba kerül. A blokkolt kártya nem használható, a blokkolt állapot nem szüntethető meg. A kártya leblokkolásának megelőzése érdekében az utolsó próbálkozás előtt kérjen segítséget, mert valószínű valamit rosszul csinált vagy tévesen olvasta a PUK kódot.

A sikeres kártya aktiválást az alábbi üzenet nyugtázza:



Kattintson az **<OK>** gombra, a program befejezi a kártya aktiválását.

3 A PKCS#11 meghajtó használata (pl. FireFox)

A programok jelentős része a Windows kriptográfiai meghajtó szolgáltatásait használja, ezek használata esetén nincs szükség további komponensek telepítésére illetve beállítására. Más programok a Windows rendszertől független, önálló kriptográfiai könyvtárat használják, ami a PKCS#11 szabvány szerinti felületet biztosít a kriptográfiai funkciók használatához.

Ilyen programok például a Mozilla által fejlesztett FireFox böngésző és ThunderBird levelező rendszer. Ilyen programoknak általában manuális módon meg kell adni a megfelelő konfigurációs felületen, hogy az adott kártya PKCS#11 meghajtó könyvtára hol található.

A Gemalto kártya a meghajtó komponenseket egy önálló könyvtárba helyezi el a számítógépen, amelynek telepítési helyét Ön választhatja meg a telepítés során. Ha Ön elfogadta a program által automatikusan felajánlott könyvtárat, akkor a PKCS#11 meghajtó – a Windows telepítési helyétől függően - általában az alábbi helyen található:

32 bites operációs rendszer esetén: C:\Program Files\Gemalto\Classic Client\BIN\gclib.dll

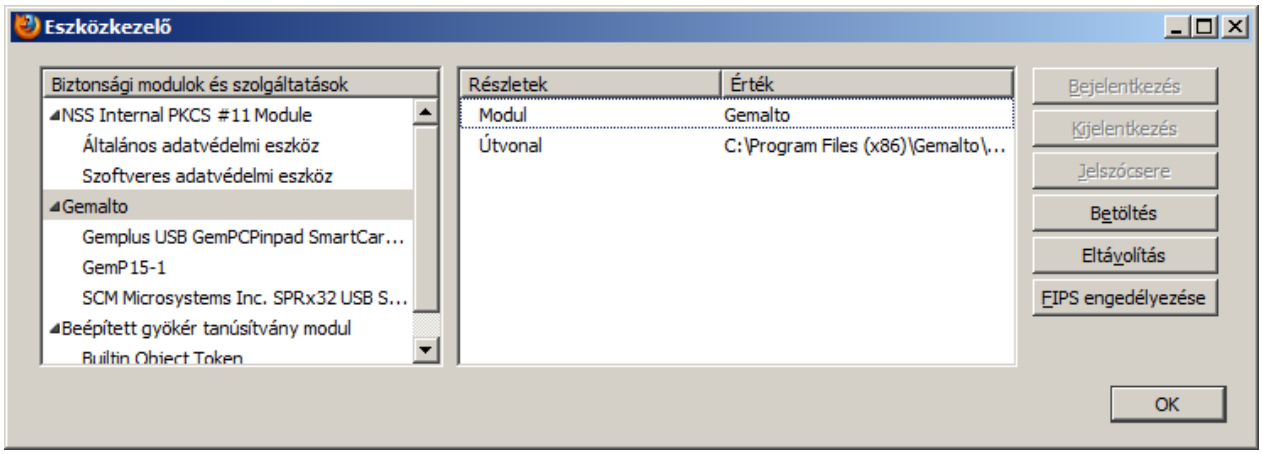
64 bites operációs rendszer esetén: C:\Program Files (x86)\Gemalto\Classic Client\BIN\gclib.dll

FireFox böngésző használatához az alábbi módon állíthatja be a Gemalto kártya használatát:

Válassza ki az alábbi funkciót:

Eszközök > Beállítások > Titkosítás > Adatvédelmi eszközök

A megjelenő ablakban a <**Betöltés>** funkció segítségével vegye fel új modulként a Gemalto kártya meghajtóját. Sikeres felvétel után megjelenik az új modul a listában az alábbi módon:



4 FELHASZNÁLÓ AZONOSÍTÁS – PIN KEZELÉS

Minden kártya tartalmaz egy egyedi PIN (Personal Identification Number = személyi azonosító szám) értéket, amely a kártyán tárolt valamennyi adatot védi.

A kártya minden privát kulccsal végzendő művelet előtt a felhasználó azonosítását igényli (PIN bekérés), és utána csak egyetlen kulcsművelet elvégzését teszi lehetővé.

A kártya kibocsátáskor nem tartalmaz ismert PIN kódot. A felhasználó a kártya TRANSPORT módjának feloldása során állíthatja be a saját PIN kódját az alábbi szabályok betartásával:

megadható karakterek	csak számjegyek
PIN minimális hossza	6 számjegy
PIN maximális hossza	8 számjegy

A PIN kódot az aktuális PIN kód megadása után a felhasználó bármikor megváltoztathatja az e-Szignó kártyakezelő alkalmazás segítségével (lásd 4.3 fejezet).

Amennyiben a használat során a PIN kód egymás után 3-szor hibásan kerül megadásra, a kártya blokkolja a PIN kódot és nem engedi a vele védett privát kulcsok használatát.

A blokkolt PIN kód feloldása az e-Szignó kártyakezelő alkalmazás segítségével lehetséges (lásd 4.2 fejezet).

4.1 A PUK kód

A PIN kód rendelkezik egy PUK (PIN Unblock Key = PIN feloldó kulcs) kóddal, amely a kártya megszemélyesítése során véletlenül generált, egyedi, 8 számjegyből álló kód. A PUK kódot a MICROSEC a PUK levélen átadja a felhasználónak. A PUK kódot a MICROSEC biztonsági okokból nem őrzi meg, elvesztése esetén nem pótolható.

A PUK kód megadása szükséges az alábbi műveletek elvégzéséhez:

- kártya feloldása TRANSPORT módból, kezdeti PIN értékek megadása
- blokkolt PIN kód feloldása új PIN kód megadásával.

A PUK kód a felhasználó által nem módosítható.

FIGYELEM!

A PUK kód háromszori ismételt hibás megadása esetén a kártya blokkolja a PUK kódot. A blokkolt PUK kód nem oldható fel.

A PIN és a PUK kód egyidejű blokkolása esetén a kártya a továbbiakban már nem használható.

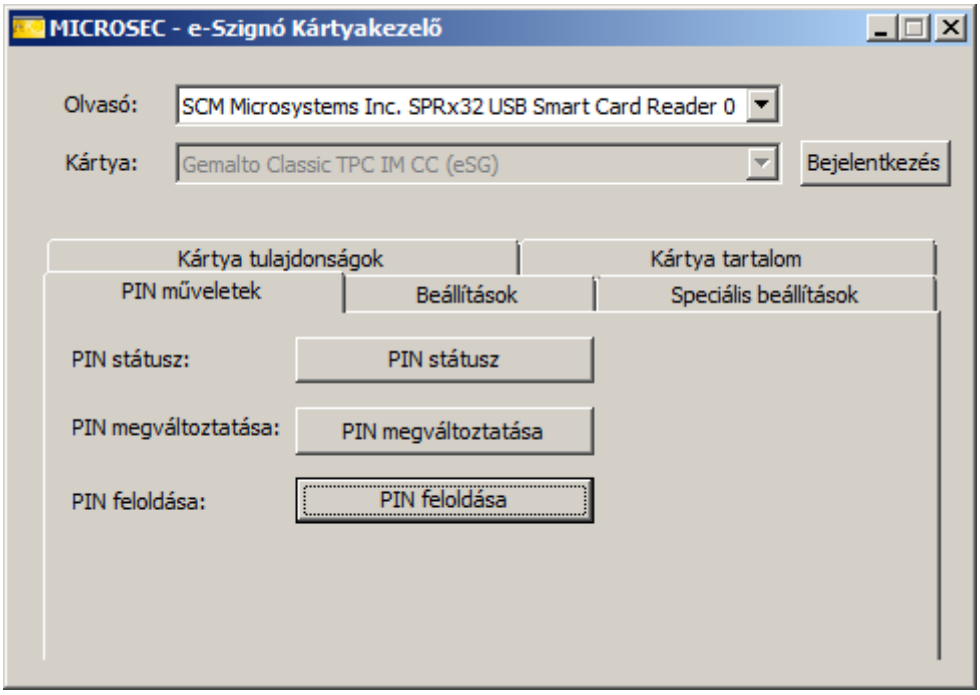
A kártya átvételekor minden felhasználó megkapja a kártyához tartozó PUK kód értékét egy lezárt borítékban. A PUK levelet tartsa biztonságos helyen, hogy illetéktelen személyek ne férhessenek hozzá a titkos azonosító adatokhoz! Kérjük, gondosan őrizze meg a PUK kódot, mert az elvesztett PUK kódot a MICROSEC nem tudja pótolni!

Az elvesztett PUK kód miatt használhatatlanná vált kártya pótlási költsége a felhasználót terheli.

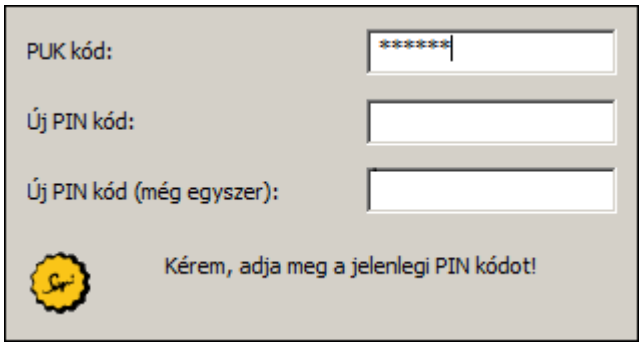
A PIN kódokkal kapcsolatos funkciók használatáról részletes leírás található az e-Szignó kártyakezelő program felhasználói leírásában.

4.2 A blokkolt PIN feloldása

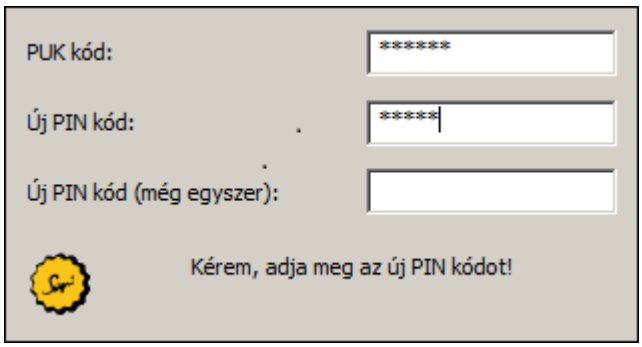
A PIN feloldás indításához kattintson az e-Szignó kártyakezelő program **[PIN műveletek]** paneljén a **<PIN feloldása>** gombra.



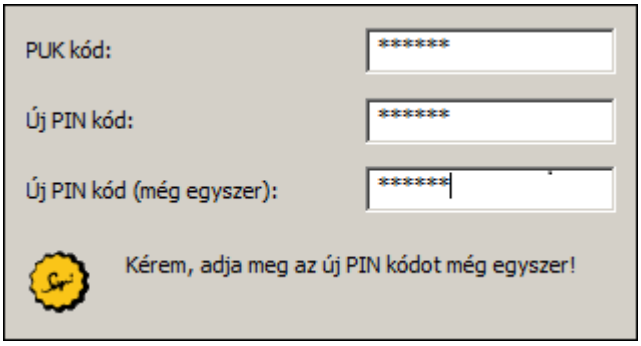
A PIN kód feloldásához először meg kell adni a PUK kódot:



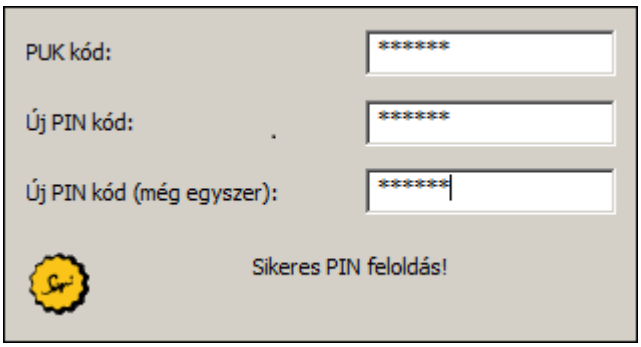
A PUK megadása után meg kell adni a beállítani kívánt PIN kódot.



Ellenőrzésképpen még egyszer meg kell adni a beállítani kívánt PIN kódot.



Ha a megadott PUK kód helyes volt és a PIN kód egyezett mindkét esetben, a program elfogadja a megadott PIN kódot és visszaigazolja a PIN feloldás tényét:

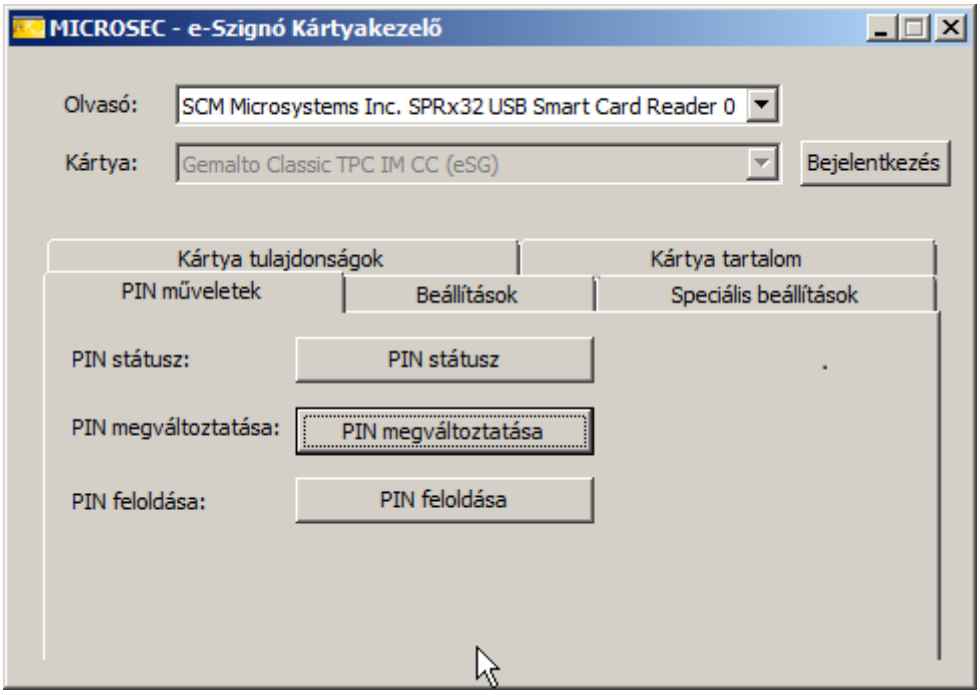


A PIN feloldásnál a PIN értéket akárhányszor meg lehet hibásan adni minden következmény nélkül, de a PUK kód egymást követő háromszori hibás megadása a kártya blokkolását eredményezi.

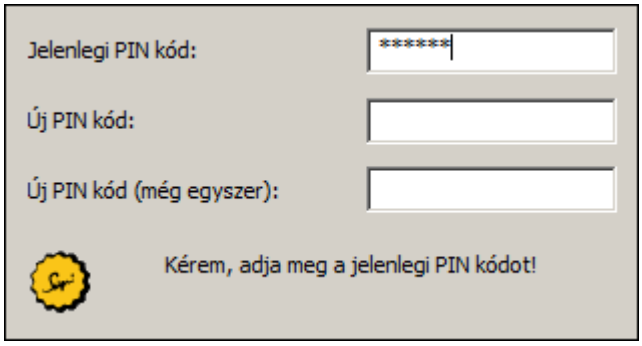
4.3 PIN kód megváltoztatása

A felhasználó bármikor megváltoztathatja az általa ismert PIN kód értékét az e-Szignó kártyakezelő alkalmazás segítségével.

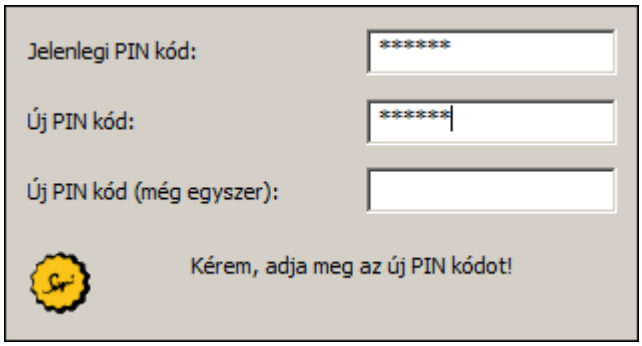
A PIN kód megváltoztatásához kattintson az e-Szignó kártyakezelő program **[PIN műveletek]** paneljén a **<PIN megváltoztatása>** gombra.



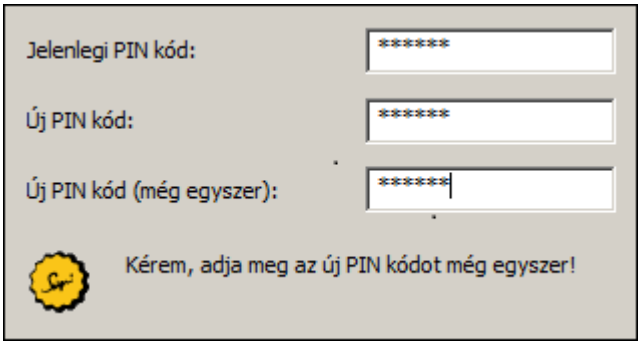
A PIN kód megváltoztatásához először meg kell adni a régi (jelenlegi) PIN kódot:



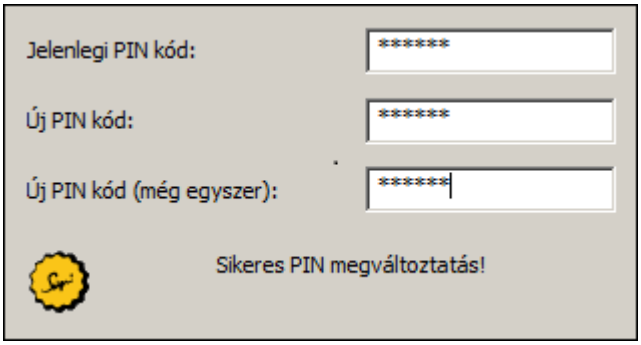
A jelenlegi PIN helyes megadása után meg kell adni a beállítani kívánt új PIN kódot.

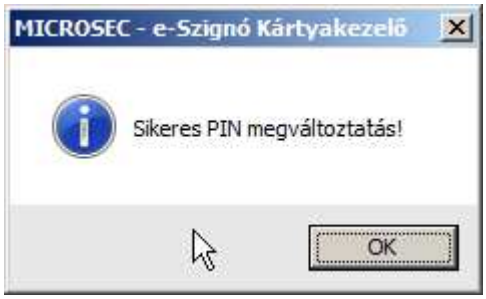


Ellenőrzésképpen még egyszer meg kell adni a beállítani kívánt új PIN kódot.



Ha a megadott régi PIN kód helyes volt és az új PIN kód egyezett mindkét esetben, a program elfogadja a megadott új PIN kódot és visszaigazolja a PIN megváltoztatás tényét:





A régi PIN egymást követő háromszori hibás megadása a PIN kód blokkolását eredményezi. A blokkolt PIN kód a PIN feloldás funkció segítségével aktiválható.

5 A KÁRTYA BEMUTATÁSA

A fejezet műszakilag képzettebb felhasználók számára tartalmaz a kártyával kapcsolatos részletes információkat, a fejezet tartalmának ismerete nem szükséges a kártya normál használatához.

5.1 A kártya rövid ismertetése

A Gemalto Classic TPC (Classic Trusted PKI Card) a MultiApp ID Citizen 72k azonosítóval tanúsított kártya kereskedelmi márkaneve.

A Classic TPC kártyát PKI alapú alkalmazásokban való szabványos felhasználásra tervezték.

A kártya támogatja a szigorúbb követelményeknek megfelelő kriptográfiai algoritmusok használatát az alábbiak szerint:

- RSA aláíró algoritmus használata 2048 bitig,
- onboard kulcs generálás,
- SHA-256 lenyomatképző algoritmus.

A kártya rendelkezik az Egységes Követelményrendszer (Common Criteria) szerint kiállított tanúsítvánnyal, amely alapján az NMHH nyilvántartásba vette Biztonságos Aláírás Létrehozó Eszközként.

A kártya a szabványos Class 1 típusú PC/SC kártyaolvasókon túl együttműködik a MICROSEC által forgalmazott Omnikey CardMan 3621-es, az SCM Microsystems SPR 532-es és SPR332-es valamint a Gemalto PC Pinpad Reader nevű Class 2 típusú pinpades kártyaolvasókkal is. A Class 2 típusú kártyaolvasóknál a PIN értékek megadása megfelelő alkalmazások használata esetén a kártyaolvasók saját billentyűzetén történik, így a PIN értékek nem kerülnek be a számítógépbe.

5.2 A kártya azonosítása

TÍPUS	MULTIAPP ID CITIZEN 72K CLASSIC TPC IM CC
Gyártó	Gemalto / Samsung Electronics
Tanúsítvány kiállítója	Serma Technologies / ANSSI
Tanúsítvány száma	DCSSI-2009/07
Tanúsítvány kelte	2009. április 23.
PP megfelelés	SSCD PP Type 2 v 1.04 SSCD PP Type 3 v 1.05

5.3 Memória

A kártya 68kB EEPROM-ban tárolja a felhasználói objektumokat (kulcsok, tanúsítványok) a PKCS#15 szabványnak megfelelő struktúrában.

A kártya memória az alábbi részekre osztható:

Kulcs konténerek	A kártya előre definiált tároló helyeket foglal le a kriptográfiai (RSA) kulcsok tárolására. A kulcs konténer előre definiált méretű és felhasználhatóságú kulcsok tárolására szolgál.
Privát memória	A felhasználó védett adatainak tárolására szolgáló terület, amihez csak a PIN megadása után lehet hozzáférni. Csak speciális alkalmazások használják, ezért mérete a lehető legkisebbre van állítva (64 bájt).
Publikus memória	A kártya szabadon elérhető memória területe, ezen tároljuk a tanúsítványokat. Az alkalmazott jelenlegi beállításban 32kB.

5.3.1 A kulcs méretek

A kártya forgalmazott konfigurációja az alábbi méretű kulcsok használatát támogatja:

- 1024 bites RSA kulcs
- 2048 bites RSA kulcs

5.3.2 A kulcs típusok

A TPC kártya a felhasználás módja szerint a kulcskonténerek két alapvető típusát különbözteti meg:

- Minősített aláíró RSA kulcs (Digital Signature: DS)
- Általános célú RSA kulcs (Standard / General Purpose: GP)

A Minősített aláíró RSA kulcs konténerek privát kulcsai csak elektronikus aláírás létrehozására használhatók, a titkosítás funkció használata kártya szinten tiltott. A DS privát kulcsokkal való műveletvégzéshez a kártya minden esetben kikényszeríti a Secure messaging használatát. A kártya megszemélyesítése során a MICROSEC valamennyi DS kulcshelyre generál kulcspárt megfelelően biztonságos körülmények között, amelyhez később minősített aláíró tanúsítványt tud kibocsátani. A DS kulcshelyekre a kártyabirtokos biztonsági okból nem telepíthet saját tanúsítványokat.

Az Általános célú RSA kulcs konténer minden kriptográfiai műveletet lehetővé tesz a tárolt kulcsokkal, így itt tetszőleges célú tanúsítvány kulcsai tárolhatók (akár aláíró tanúsítvány kulcsai is). A kulcsok használatához nem jön létre Secure Messaging, így ez nem felel meg a minősített aláírás követelményeinek. de minden más célra felhasználható. A szabad kulcskonténerekbe a kártyabirtokos elhelyezheti a saját tanúsítványaihoz tartozó kulcsokat.

5.3.3 A kártya struktúra

A MICROSEC a TPC kártyát az alábbi memória konfigurációban forgalmazza:

4 db	1024 bites GP általános célú kulcs konténer
3 db	2048 bites DS konténer a minősített aláíró kulcsok részére
9 db	2048 bites GP általános célú kulcs konténer az egyéb kulcsok részére
64 bájt	privát memória, nem használt
32.000 bájt	publikus memória a tanúsítványok tárolására

5.3.4 Objektumok törlése

A TPC kártya szinten nem védi a kártyán tárolt objektumokat, azok bármelyike törölhető. Mivel a tervezett felhasználás során a MICROSEC által felvett objektumokat nem kell törölni, a MICROSEC által biztosított kártyakezelő alkalmazás nem teszi lehetővé a kártyán tárolt objektumok törlését.

Harmadik fél által szállított alkalmazás használata esetén a kártyán tárolt kulcsok kitörlődhetnek. Az aláíró kulcsok kitörlése esetén a felhasználónak új kártyát kell kibocsátani, aminek költsége a felhasználót terheli.

5.3.5 A kártya tartalma

A kártya tartalma az aktuális konfigurációtól, az előfizető által igényelt szolgáltatásoktól függően változhat. Egy teljes konfiguráció az alábbi objektumokat tartalmazza:

Kulcs konténerek:

Sorszám	Kulcs méret	Típus	Felhasználás
1	1024	GP	Régi titkosító tanúsítvány kulcsa G&D kártyáról
2	1024	GP	Szabadon használható a felhasználó által
3	1024	GP	Szabadon használható a felhasználó által
4	1024	GP	Szabadon használható a felhasználó által
5	2048	DS	**<DS3>** on-board generált kulcs a kibocsátott minősített aláíró tanúsítványhoz
6	2048	DS	**<DS4>** on-board generált kulcs későbbi felhasználásra
7	2048	DS	**<DS5>** on-board generált kulcs későbbi felhasználásra
8	2048	GP	**<KP_CH_AUT>** Authentikációs tanúsítvány kulcsa
9	2048	GP	**<KP_CH_ENC>** Új titkosító tanúsítvány kulcsa
10	2048	GP	Szabadon használható a felhasználó által
11	2048	GP	Szabadon használható a felhasználó által
12	2048	GP	Szabadon használható a felhasználó által
13	2048	GP	Szabadon használható a felhasználó által
14	2048	GP	Szabadon használható a felhasználó által
15	2048	GP	Szabadon használható a felhasználó által
16	2048	GP	Szabadon használható a felhasználó által

Memória terület:

Típus	Méret	Tartalom
Private	64 byte	Használaton kívül
Public	32.000 byte	1024 bites régi tikosító tanúsítvány DS3 2048 bites minősített aláíró tanúsítvány KP_CH_AUT 2048 bites authentikációs tanúsítvány KP_CH_ENC 2048 bites új titkosító tanúsítvány Kb 20.000 bájt szabadon felhasználható memória