MICROSEC
Számítástechnikai Fejlesztő Kft.

FELHASZNÁLÓI ÚTMUTATÓ

BIZTONSÁGOS ALÁÍRÁS LÉTREHOZÓ ESZKÖZ (BALE)

BIT4ID CHIPKÁRTYA

2011. március 9.

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 blokk alakja gyártónként eltérő. A Bit4id chip kontaktus blokk alakja enyhén lekerekített sarkú, 6 db téglalap alakú valódi kontaktust tartalmaz az alábbi ábra szerint:

- A kártya hátoldalán a jobb felső sarokban egy kártyatípusonként eltérő azonosító található az alábbi ábra szerint, ami a Bit4id kártya esetén „eSB”.

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.

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

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

2 A BIT4ID KÁRTYA HASZNÁLATBA VÉTELE

A kártya használatba vételéhez Önnek az alábbi feladatokat kell elvégeznie:

- PC/SC szabványt támogató kártyaolvasó üzembe helyezése (lásd 2.1 fejezet)
- Bit4id kártyameghajtó programok telepítése (lásd 2.2 fejezet)
- e-Szignó kártyakezelő alkalmazás telepítése (lásd 2.3 fejezet)
- Transport mód feloldása (lásd 2.4 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 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 A Bit4id kártya meghajtó programjainak telepítése

Amennyiben a számítógépén telepítve van a Bit4id kártya bármely korábbi 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=eSB

A telepítő csomagnak több verziója létezik a használt operációs rendszertől függően.

Operációs rendszer	Telepítő csomag
Microsoft Windows XP, Windows 2003 szerver operációs rendszerekhez	Bit4IDSetupXP-32bit.msi
Microsoft Windows Vista, Windows 7 32 bites operációs rendszerekhez	Bit4IDSetupVista-32bit.msi
Microsoft Windows Vista, Windows 7 64 bites operációs rendszerekhez	Bit4IDSetupVista-32bit.msi Bit4IDSetupVista-64bit.msi

Figyelem!

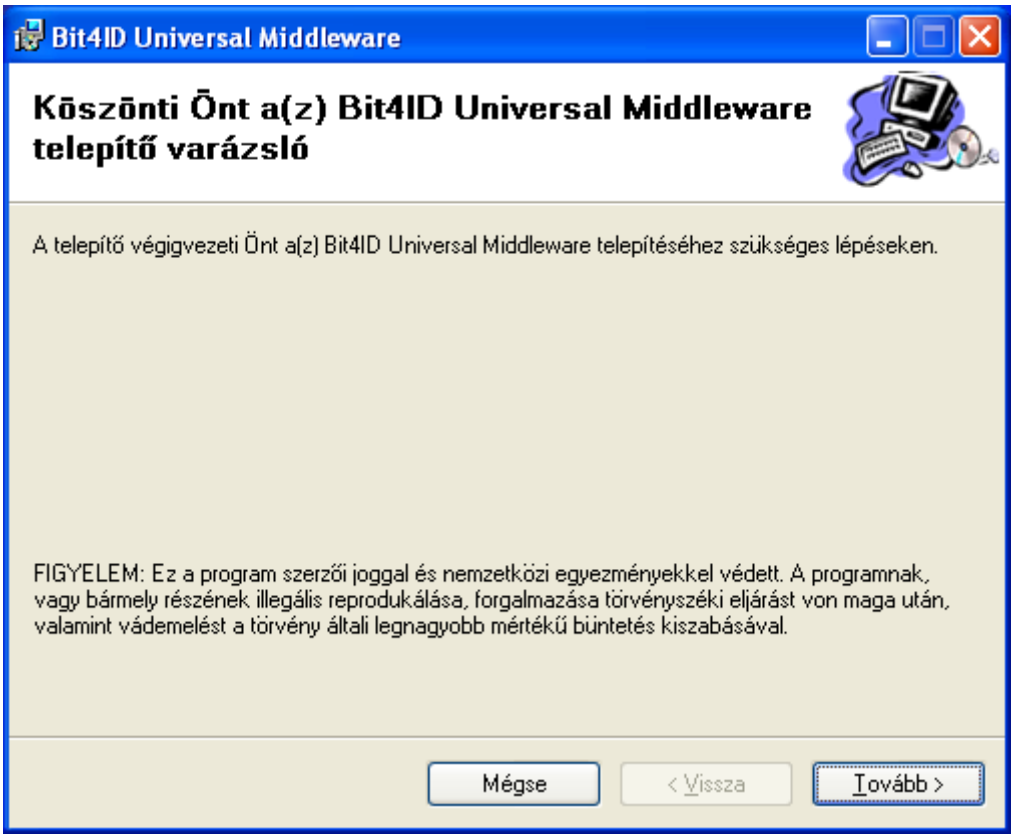
A 64 bites Windows operációs rendszereken futtatott 32 bites alkalmazások nem működnek a 64 bites kártya meghajtó komponensekkel.

A 64 bites Windows operációs rendszereken telepíteni kell a 32 bites és a 64 bites csomagot is.

- A megfelelő telepítő csomag(ok) kiválasztása és letöltése után indítsa el a telepítő programot.

A telepítő csomagot a MICROSEC elektronikus aláírással látta el a visszaélések megakadályozása érdekében. A futtatás elején megjelenik egy biztonsági figyelmeztető ablak.

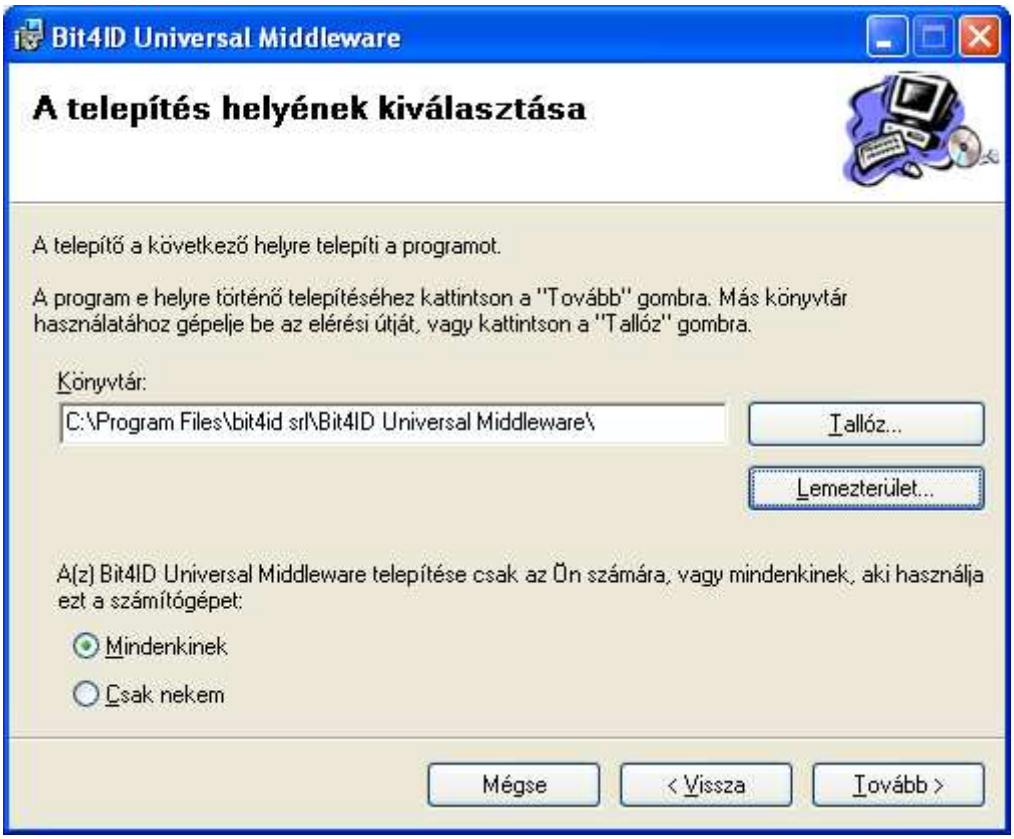
Amennyiben meggyőződött arról, hogy valóban a MICROSEC oldalról letöltött telepítő programot indította el, az ablak információinak elolvasása után kattintson a **<Futtatás>** gombra.



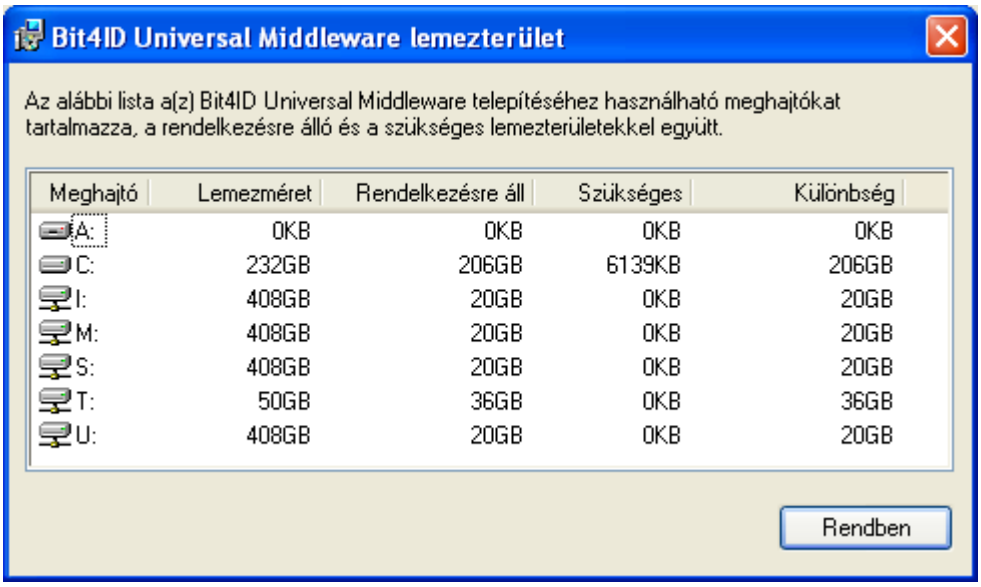
A megjelenő beköszönő ablak információinak elolvasása után a feltételek elfogadása esetén

kattintson a **<Tovább>** gombra!

A megjelenő ablakban kiválaszthatja a program telepítésének mappáját. Amennyiben lehetséges, fogadja el a program által felkínált helyet.

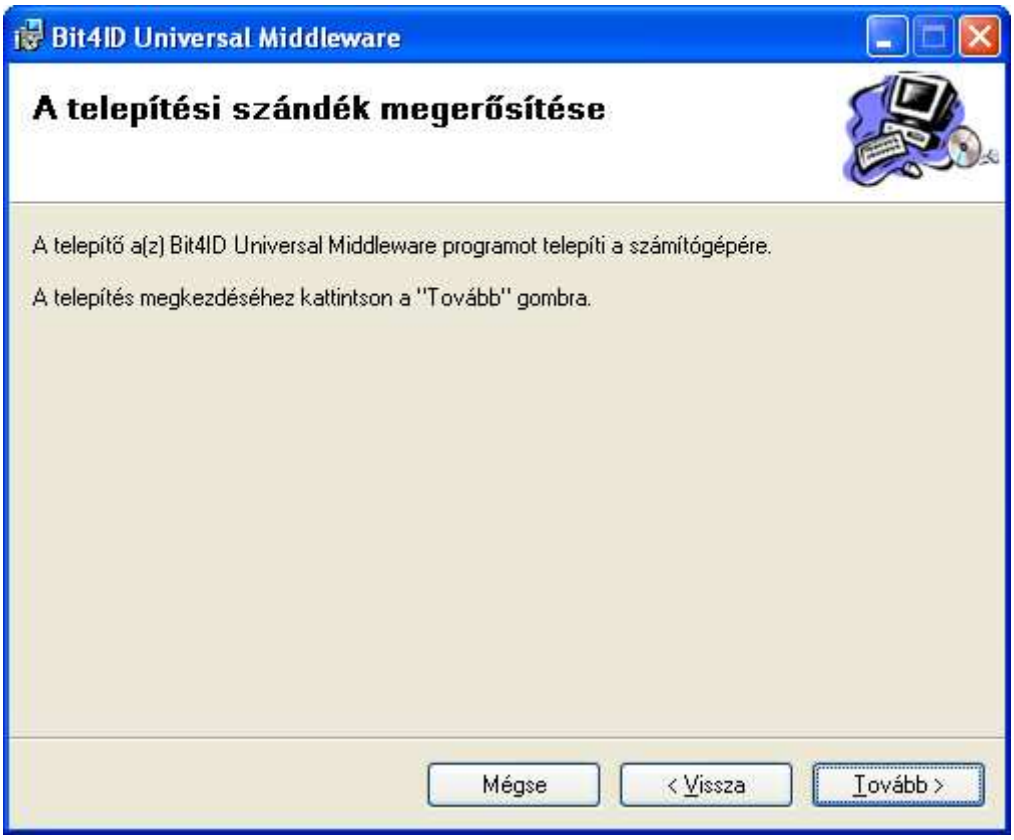


A **<Lemezterület>** gombra kattintva ellenőrizheti, hogy a számítógépén melyik meghajtón áll rendelkezésére a szükséges tároló terület.

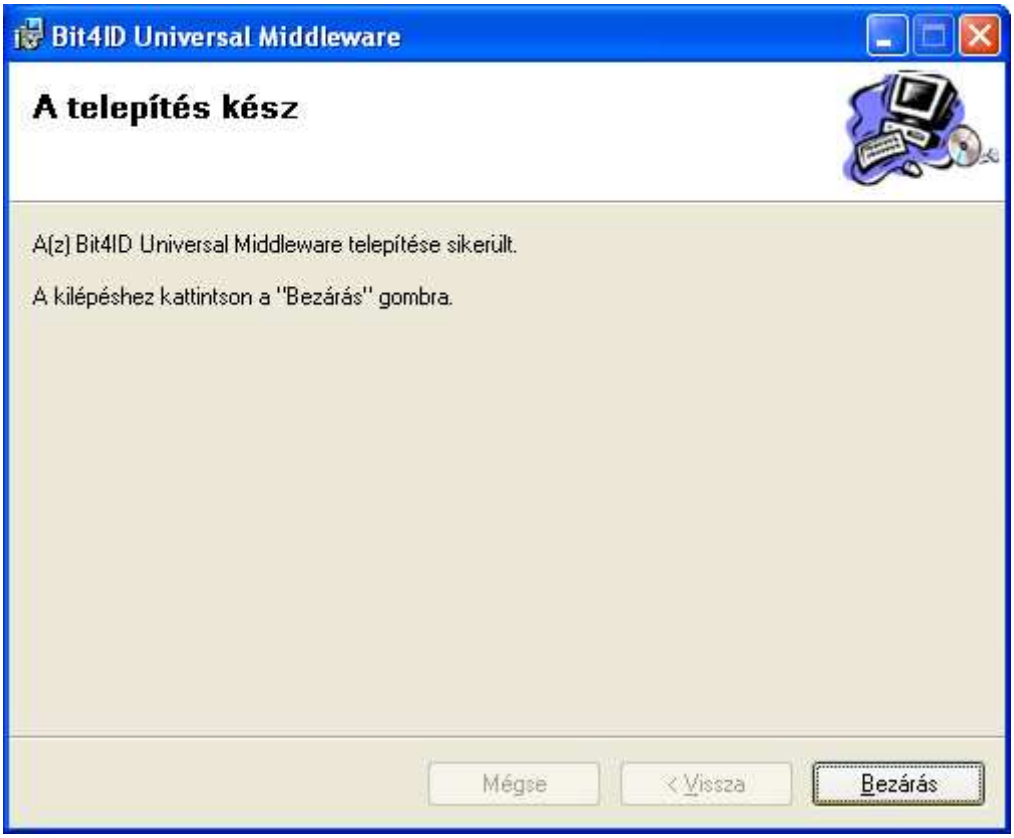


Az információ elolvasása után a beállításokhoz való visszalépéshez kattintson a **<Rendben>** gombra!

A megfelelő beállítások kiválasztása után kattintson a **<Tovább>** gombra!



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



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

A meghajtók aktiválásához nem kell újra indítania a számítógépét, de ha már telepítve van a számítógépén az e-Szignó kártyakezelő alkalmazás, a Bit4ID kártya használatához azt le kell állítania majd újra kell indítania.

2.3 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=eSB

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

2.4 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, az elvégzendő feladatok:

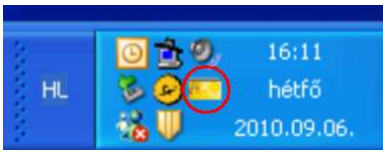
- TRANSPORT állapot feloldása a PUK kód megadásával
- Globál PIN kód megadása a 'Globál PIN kód feloldása' funkcióval

- Aláíró PIN kód megadása az ’Aláíró PIN kód feloldása’ funkcióval

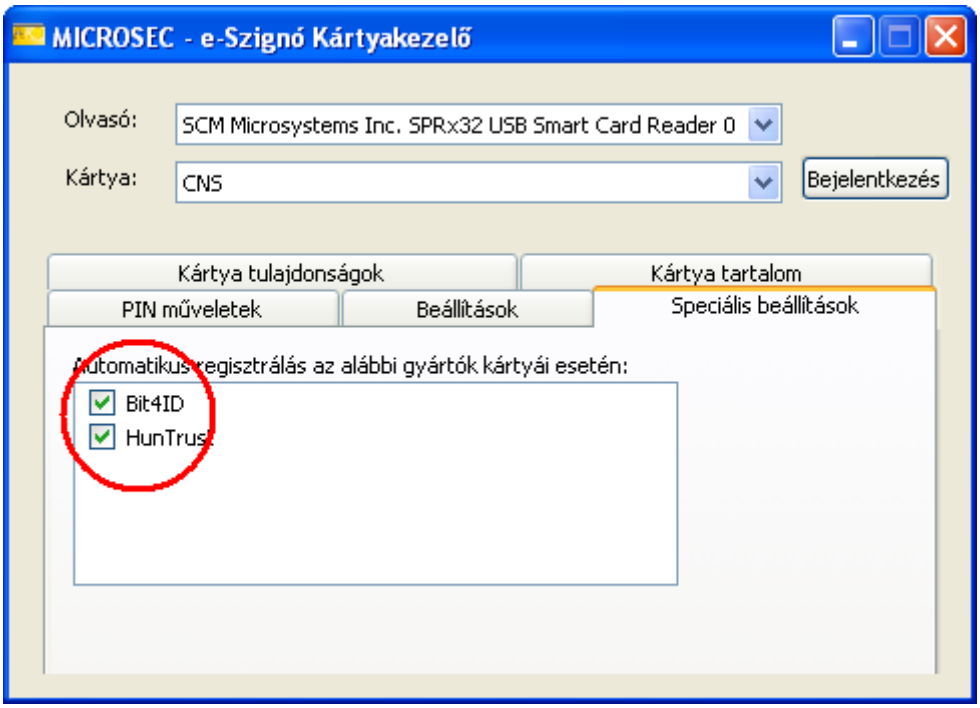
A felhasználás megkönnyítése érdekében a fenti funkciókat az e-Szignó kártyakezelő program automatikusan meghívja egymás után a TRANSPORT állapot észlelése esetén. A felhasználó elvégezheti a feladatokat a programot követve, de ki is léphet a folyamatból és későbbi időpontban, kézzel indítva is elvégezheti az adott feladatot.

2.4.1 A TRANSPORT állapot feloldása

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



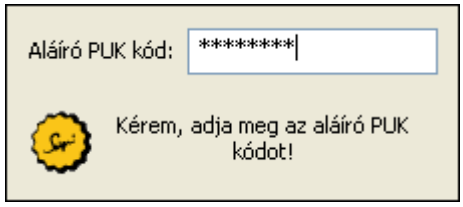
Az e-Szignó kártyakezelő alkalmazásban aktívnak kell lennie a ’Bit4ID’ kártya figyelése funkciónak:



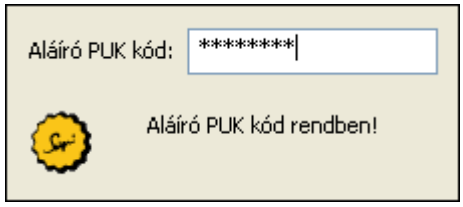
A TRANSPORT állapotban lévő kártya kártyaolvasóba helyezése után az e-Szignó kártyakezelő alkalmazás kiolvassa a kártya adatait és megjelenik az alábbi tájékoztató üzenet:

Az üzenet az <OK> gombra kattintva nyugtázható.

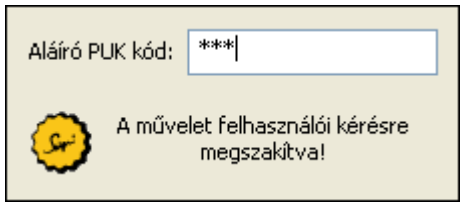
A kártya aktiválásához a kártyaolvasó billentyűzetén meg kell adnia a PUK levélen kapott PUK kódot. A számítógép képernyőjén megjelenő ablakban minden számjegy bevitele után megjelenik egy pont.



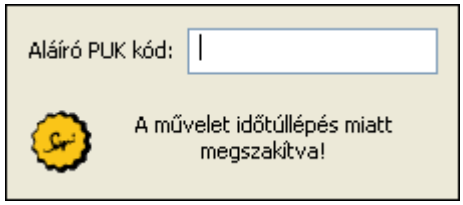
A 8 számjegy bevitele után nyomja meg az olvasón a ZÖLD gombot. Helyes PUK kód megadása esetén a program nyugtázza a PUK kód elfogadását:



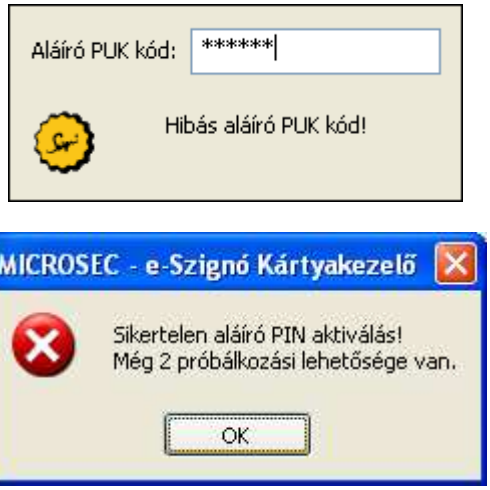
Ha elrontotta a PUK bevitelét, nyomja meg az olvasó PIROS gombját. A megszakított PUK kód bevitelt a kártya nem érzékeli, így nem számít bele a 3 próbálkozásba.



Ha lejár a PUK megadására rendelkezésére álló idő, a program kilép a műveletből:



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 kártya leblokkolásának megelőzése érdekében az utolsó próbálkozás előtt kérjen segítséget, mert valószínű valamit rosszul csinált vagy tévesen olvasta a PUK kódot.

A TRANSPORT állapot feloldása után a felhasználó kiléphet a folyamatból vagy elvégezheti a program által felkínált PIN megadási funkciókat. Bár a kártya már nincs TRANSPORT állapotban, nincs a felhasználó által ismert PIN kódja így nem használható PIN megadást igénylő műveletek elvégzésére.

A felhasználó által kívánt PIN értékek beállítása a globál PIN feloldása és az aláíró PIN feloldása funkciókkal lehetséges (a használatát lásd a 3.4 fejezetben)

3 FELHASZNÁLÓ AZONOSÍTÁS – PIN KEZELÉS

A kártya két független PIN kódot tartalmaz:

- globál PIN kód
- aláíró PIN kód.

A kártya kibocsátáskor nem tartalmaz egyetlen ismert PIN kódot sem. A felhasználó a kártya TRANSPORT módjának feloldása során állíthatja be a saját PIN kódjait a PIN feloldás funkció használatával (lásd 3.4 fejezet). A PIN kódokra az alábbi szabályok érvényesek:

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

A két PIN kód egymástól teljesen független, a felhasználó igénye szerint használható azonos PIN kód, vagy akár eltérő hosszú különböző PIN kód is.

Az egyes PIN kódokat az aktuális megfelelő PIN kód megadása után a felhasználó bármikor megváltoztathatja az e-Szignó kártyakezelő alkalmazás segítségével (lásd 3.5 fejezet).

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

A blokkolt PIN kód feloldása az e-Szignó kártyakezelő alkalmazás segítségével lehetséges (lásd 3.4 fejezet).

3.1 A globál PIN kód

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

A kártya minden új kapcsolat felépítése után a felhasználó egyszeri azonosítását igényli a kulcsok használatához, de utána több műveletet is hajlandó végrehajtani a PIN ismételt megadása nélkül. Ez azt jelenti, hogy pld a globál PIN egyszeri megadása után több visszafejtés művelet is elvégezhető, vagy több fokozott elektronikus aláírás is létrehozható.

3.2 Az aláíró PIN kód

Minden kártya tartalmaz egy önálló aláíró PIN értéket, amely a kártyán tárolt minősített aláíró kulcsokat védi.

A kártya minden egyes minősített aláírás létrehozása előtt a felhasználó azonosítását igényli az aláíró PIN megadásával.

Mivel a minősített aláíró kulcsokat az aláíró PIN és a globál PIN is védi, sorozatos aláírás létrehozásánál egyszer meg kell adni a globál PIN értékét, majd minden egyes aláírás előtt az aláíró PIN értékét is.

3.3 A PUK kód

A globál és az aláíró PIN kódok mindegyike rendelkezik egy saját PUK (PIN Unblock Key = PIN feloldó kulcs) kóddal, azonban ezeket a kártya kibocsátása során az egyszerűbb kezelhetőség érdekében azonos értékűnek állítjuk be, ezt közösen PUK kódnak hívjuk. A PUK kód 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!

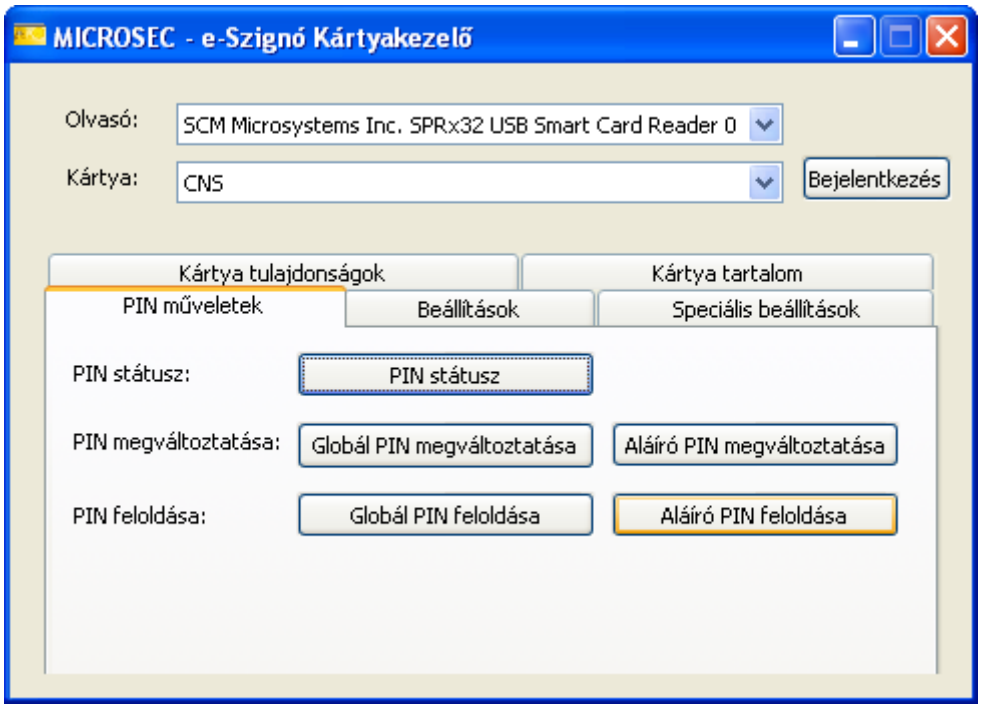
Az elvesztett PUK kód miatt használhatatlanná vált kártya pótlási költsége a felhasználót terheli.

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

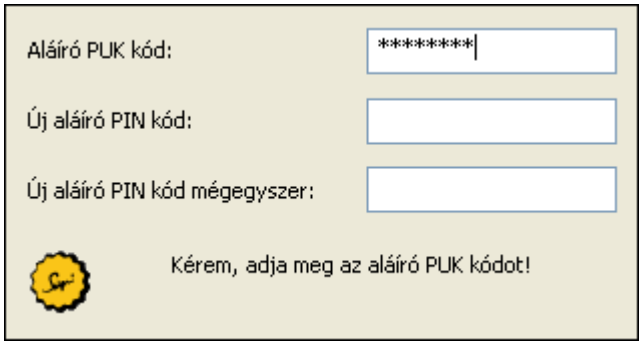
3.4 A PIN inicializálása / blokkolt PIN feloldása

A globál és az aláíró PIN kód feloldása teljesen azonos módon történik, ezért csak az aláíró PIN kód feloldásának menetét mutatjuk be részletesen.

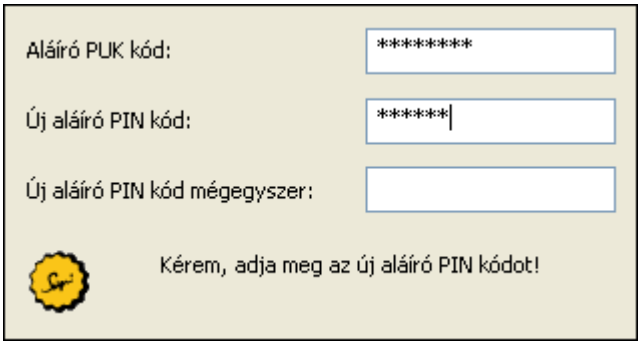
A PIN feloldás kézi indításához kattintson az e-Szignó kártyakezelő program **[PIN műveletek]** paneljén az **<Aláíró PIN feloldása>** gombra.



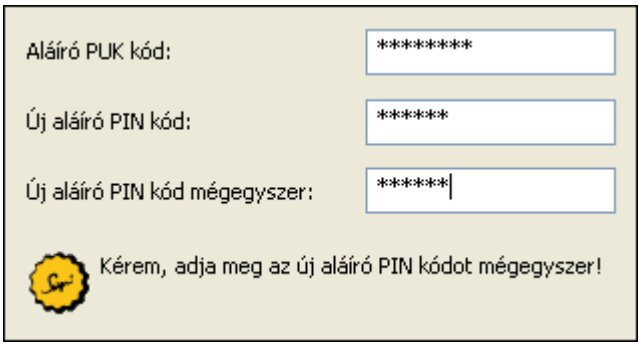
A PIN kód feloldásához először meg kell adni a PUK kódot:



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



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



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

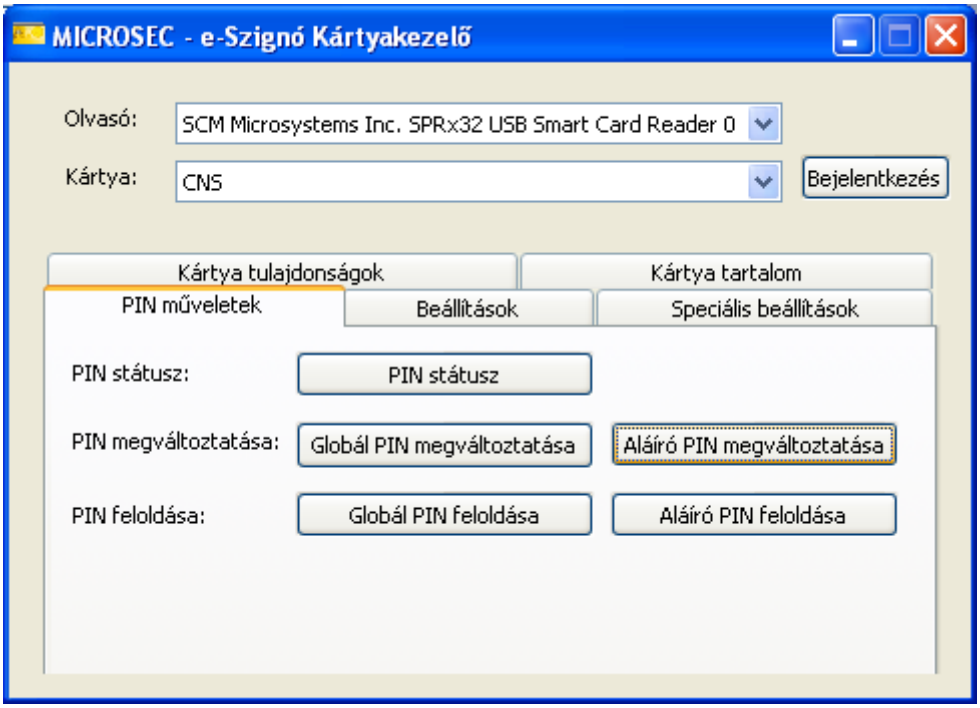
A PIN feloldásnál a PIN értéket akárhányszor meg lehet hibásan adni minden következmény nélkül, de a PUK háromszori hibás megadása a kártya blokkolását eredményezi.

3.5 PIN kód megváltoztatása

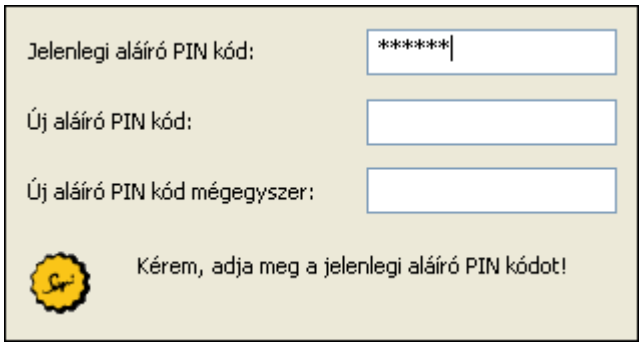
A felhasználó bármikor megváltoztathatja az általa ismert PIN kódok értékét az e-Szignó kártyakezelő alkalmazás segítségével.

A globál és az aláíró PIN kód megváltoztatása teljesen azonos módon történik, ezért csak az aláíró PIN kód megváltoztatásának menetét mutatjuk be részletesen.

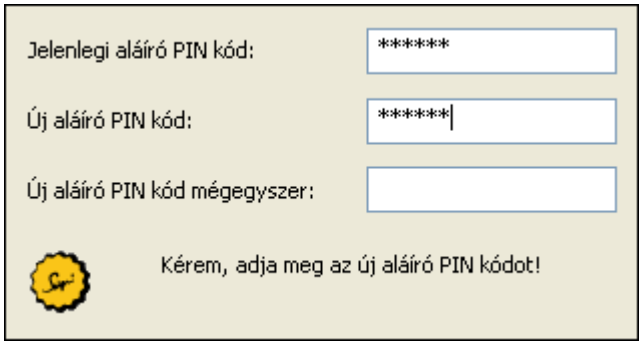
A PIN feloldás kézi indításához kattintson az e-Szignó kártyakezelő program **[PIN műveletek]** paneljén az **<Aláíró PIN megváltoztatása>** gombra.



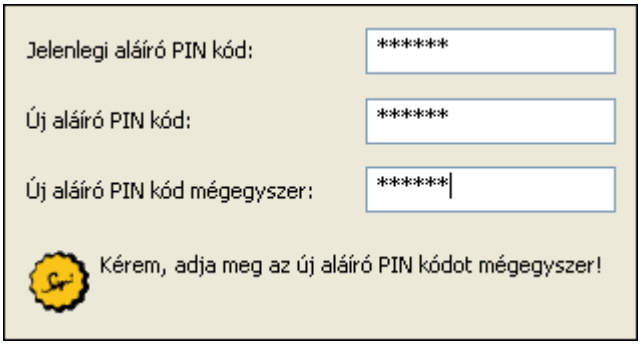
A PIN kód megváltoztatásához először meg kell adni a régi (jelenlegi) PIN kódot:



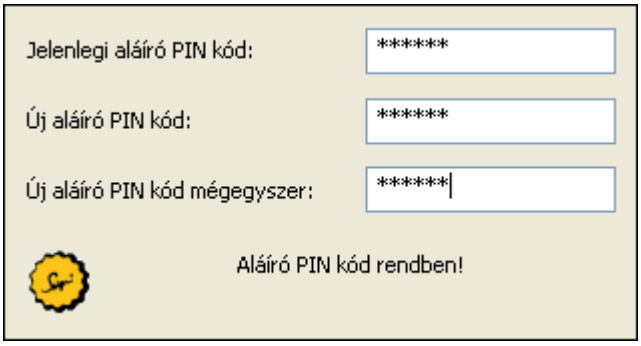
A jelenlegi PIN helyes megadása után meg kell adnia a beállítani kívánt új PIN kódot.



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



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



A PIN feloldásnál az új PIN értéket akárhányszor meg lehet hibásan (a két verziót egymástól eltérően) adni minden következmény nélkül, de a régi PIN háromszori hibás megadása a PIN kód blokkolását eredményezi.

4 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.

4.1 A kártya rövid ismertetése

A Touch&Sign2048 V1.00 egy többfunkciós intelligens kártya termék, amelyet a minősített elektronikus aláírások létrehozásában érintett eszközök által igényelt összes képesség biztosítására terveztek.

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 NHH nyilvántartásba vette Biztonságos Aláírás Létrehozó Eszközként.

A kártya a szabványos PC/SC kártyaolvasókon túl együttműködik a MICROSEC által forgalmazott Omnikey 3621-es és SPR 532-es pinpades kártyaolvasókkal is. A PIN értékek megadása megfelelő alkalmazások használata esetén a kártyaolvasók saját billentyűzetén történik, így a PIN értékek nem kerülnek be a számítógépbe.

4.2 A kártya azonosítása

TÍPUS	TOUCH&SIGN2048 VERSION 1.00
Gyártó	Bit4id / ST Incard S.r.l.
Tanúsítvány kiállítója	Bundesamt für Sicherheit in der Informationstechnik
Tanúsítvány száma	BSI-DSZ-CC-0422-2008
Tanúsítvány kelte	2009. április 9.
PP megfelelés	SSCD PP Type 3

4.3 Memória

A kártya 66kB EEPROM-ban tárolja a felhasználói objektumokat (kulcsok, tanúsítványok).

A kártya memória területe 2 részre van osztva:

- DS a minősített aláíró kulcsok tárolására
- FULLP11 általános célú objektumok tárolására

4.3.1 A DS terület

A kártya a DS objektumok részére elkülönített memória területet használ, 3 db 1024 bites és 3db 2048 bites minősített aláíró kulcs tárolására van lehetőség.

A DS területen létrehozott kulcsokat a kártya megkülönböztetett módon kezeli:

- Külön DS PIN illetve PUK kóddal is védettek
- Az itt tárolt kulcsok csak elektronikus aláírás létrehozására használhatók
- A felhasználó azonosítása után csak egyetlen elektronikus aláírás hozható létre
- A kulcs használatához *secure messaging* kialakítása szükséges a kártya és az alkalmazás között
- A DS terület kulcsai nem importálhatók a kártyára, csak a kártyán generálhatók
- A DS területen tárolt kulcsok nem törölhetők

- A DS terület kulcsai a kártya TRANSPORT állapotában nem használhatók

4.3.2 A FULLP11 terület

A kártya minden más objektuma az általános felhasználású FULLP11 területen tárolódik:

- Általános célú kulcs komponensek
- Minden tanúsítvány

A kártyán tárolható objektumok számát csak a rendelkezésre álló memória mérete korlátozza.

A FULLP11 terület objektumaihoz való hozzáférést a globál PIN szabályozza.

A kártya TRANSPORT módban nem korlátozza a FULLP11 terület kulcsainak használatát, de az e-Szignó kártyakezelő alkalmazás részlegesen kiterjeszti a TRANSPORT mód védelmi hatályát a FULLP11 terület objektumaira is.

4.3.3 A kártya tartalma

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

Rövid név / Címke	Leírás
DS User Private Key3 DS User Public Key3 DS User Certificate3	On-board generált kulcspár a kibocsátott minősített aláíró tanúsítványhoz Minősített aláíró tanúsítvány
DS User Private Key4 DS User Public Key4	On-board generált kulcspár későbbi felhasználásra minősített aláíráshoz
DS User Private Key5 DS User Public Key5	On-board generált kulcspár későbbi felhasználásra minősített aláíráshoz
KP_CH_DS	On-board generált kulcspár későbbi felhasználásra fokozott aláíráshoz
KP_CH_AUT	Authentikációs tanúsítvány kulcspárja Authentikációs tanúsítvány
KP_CH_KE	Titkosító tanúsítvány kulcspárja Titkosító tanúsítvány

A minősített tanúsítványok valamennyi objektumánál (kulcs komponensek és tanúsítvány) a kártyán tárolt címke az alábbi lehet:

DS3, DS4, DS5

Az általunk biztosított alkalmazások az egyes objektumok neveit kiegészítik az objektumra jellemző megnevezéssel, így alakulnak ki a táblázatban felsorolt egyedi megnevezések.

Más alkalmazások használata esetén elképzelhető, hogy a minősített aláíró objektumok a valódi, rövid nevükkel kerülnek felsorolásra.