

Termékleírás és használati útmutató az e-Szignó szolgáltatás kiegészítő termékeihez

1. Chipkártya - CosmopolIC

1.1 Általános leírás

Az e-Szignó aláíró kulcsok biztonságos tárolásához ajánlott Oberthur Kártya Rendszerek terméke a CosmopolIC – egy rendkívül fejlett – a biztonsági, fizetési és elektronikus kereskedelmi (e-commerce) alkalmazásokra kialakított – fix vagy mobil multifunkciós platform, amely gyors hozzáférést biztosít a fizetés virtuális és valós világához. A platform bővítésével ez a Java alapú többfunkciós kártya számos e-commerce és m-commerce, valamint fizetési alkalmazás számára nyitja meg az utat, nagyobb kényelmet biztosítva egy rendkívül biztonságos környezetben.

A memória (ROM és EEPROM) jobb kezelésével a CosmopolIC több helyet biztosít e-commerce, m-commerce, fizetés (debit, credit), hálózati hozzáférés, pay-TV és több más alkalmazás számára, beleértve a WAP-ot is. A hozzáférhető memória ilyen mértékű megnövekedése egy nagy előrelépés a Java technológia alapú smart kártyák terén, és további bővítést tesz lehetővé az azonosítási és fizetési alkalmazások számára a multifunkciós kártyákon.

A CosmopolIC kártyát kifejezetten az igazán biztonságos elektronikus kereskedelem két alapszükségletének kielégítésére, a fizetésre és a hálózati rendszerek biztonságos hozzáféréséhez szükséges azonosítás céljára hozták létre. Továbbá ez az első olyan Java technológia alapú multifunkciós platform, amely összekapcsolja a pénzmozgatás fizikai és virtuális világát.

A legfrissebb Open Platform technológia lehetővé teszi, hogy több alkalmazás is aktív legyen ugyanabban az időpillanatban. A CosmopolIC használata esetén egy WAP-os futtatás indítása mellett egy másik alkalmazást is el lehet indítani. CosmopolIC valóságos digitális ID-t biztosít a mobil-kereskedelem (m-commerce) számára és támogatja a WAP protokollt is. Terminál független, bármilyen Internet elérésre alkalmas eszközön keresztül használható, akár TV, set-top-box, PC, mobiltelefon, PDA. Működőképes többféle különböző hálózaton: kábel, szatellit, GSM, banki rendszerek, stb. A CosmopolIC chipkártya minősített eszköz. (EAL4+: nagyon fejlett biztonsági szint)

1.2 Műszaki jellemzők

	CosmopolIC
CPU	8 bit
Társ-processzor	RSA, DES
Memória (ROM)	96k-ig
Memória (EEPROM)	64k-ig
Protokoll	T = 0 / T = 1
Tulajdonságok	JavaCard 2.1, Open Platform 2.0, Hitelesítés szolgáltatások, EMV Debit-Credit alkalmazások, WAP, ISO File Rendszer
Titkosítási algoritmus	RSA 2048 bit, RSA kulcs generálás, DSA, DES, 3-DES, SHA-1, MD-5RC2, RC5
Standard	ISO 7816, EMV, WAP
Biztonsági értékelés	EAL 4+

1.3 Használati útmutató

Az e-Szignó szolgáltatáshoz megrendelt chipkártyán a tárolt privát kulcs biztonságáról PIN kód gondoskodik, amelyet a kártyához mellékelt PIN borítékban találhatunk meg. Amennyiben a megrendelt chipkártya még nem tartalmaz bizalmas adatokat - pl. a T-Com internetes áruházából megrendelt kártyák esetén - a kártya PIN kódja: 9999. Ezt a kódot javasolt e-Szignó tanúsítványigénylést megelőzően megváltoztatni az e-Szignó chipkártya telepítő szoftver segítségével. A PIN kód gondoskodik arról, hogy a chipkártyát illetéktelen személyek ne tudják használni, ezért a személyes kódot fokozott figyelemmel kell védeni. Tilos a privát kulcs illetéktelen felhasználását megakadályozó PIN-kódot a privát kulcs hordozójával egy helyen tartani, illetve mindig a megfelelő védelemmel ellátva, biztonságosan kell tárolni.

Telepítés

A chipkártyát a használat előtt fel kell telepíteni a számítógépre. A telepítést az „e-Szignó chipkártya telepítő v 3.0” program elindításával tudjuk elvégezni. A telepítő program a T-Systems honlapjáról (www.t-systems.hu) az e-Szignó oldalain található Kapcsolódó termékek menüpontból tölthető le. A program lépéseit végigkövetve a telepítés egyszerűen elvégezhető.

Chipkártya használata aláíró kulcs generálásához Tanúsítvány igényléshez

Tanúsítvány igénylés a T-Systems honlap e-Szignó oldalain kezdeményezhető az ott található elektronikus igénylőlap kitöltésével és elküldésével. Az elküldés során legenerálódik a Aláíró kulcspárja is, amely történhet a böngésző program által (alapesetben), vagy az e-Szignó chipkártya által, de ez utóbbihoz az szükséges, hogy az igénylés megkezdése előtt a chipkártyánkat és kártyaolvasónkat telepítsük a számítógépünkre. Amennyiben a telepítést sikeresen elvégeztük, az elektronikus igénylőlapon a "Kripto-modul kiválasztása kulcsgeneráláshoz" című alatti legördülő menüben megjelenik a chipkártyának megfelelő modul neve (OCS Cryptographic Service Provider Library v4.0).

Ezt a modult kiválasztva és a chipkártyát behelyezve a kártyaolvasóba az elektronikus tanúsítvány-igénylőlap elküldését követően a chipkártya le fogja generálni az aláíró kulcspárt. A generálás során a számítógép kérni fogja a kártyájához tartozó numerikus PIN kódot is, melyet a billentyűzet segítségével kell megadni.

Chipkártya használata Tanúsítvány letöltéséhez

A Tanúsítvány igénylés elfogadása után a Tanúsítvány letölthető a T-Systems honlap e-Szignó oldalairól. A Tanúsítvány letöltése csak arra az eszközre (chipkártyára) lehetséges, ahonnan az igénylés feladásra került, ezért ügyeljünk arra, hogy a letöltéskor is csatlakoztatva legyen a kártyaolvasó, valamint a chipkártya a kártyaolvasóban legyen. A letöltés során a számítógép kérni fogja a kártyájához tartozó numerikus PIN kódot is, melyet a billentyűzet segítségével kell megadni.

Chipkártya használata aláírásához

Azokban az alkalmazásokban, amelyekben a kártyáján lévő privát kulcs felhasználásra kerül (pl. Outlook levelező programban e-mail elektronikus aláírására) a kártyaolvasó valamint a chipkártya használata nélkülözhetetlen; az aláírás pillanatában (jellemzően az aláírás ikonra történő kattintást követően) a számítógépe kérni fogja a kártyájához tartozó numerikus PIN kódot is, melyet a billentyűzet segítségével kell megadni.

A chipkártyák használata során felmerült kérdéseivel kérjük, keressé fel ügyfélszolgálatunkat:

e-Szignó ügyfélszolgálat
1476 Budapest, Pf.: 227
E-mail: eszigno.fokozott@telekom.hu
Tel.: 06 80 20 40 40
Fax.: 06 1 447 4451

2. Kártyaolvasók - Oberthur OCR 136 és 150

2.1 Általános leírás

Az e-Szignó chipkártyákhoz használatos OCR 136 és OCR 150 az Oberthur cég kártyaolvasó családjának legfrissebb tagjai. A két típus közötti különbség a csatlakoztatás módjában van: az OCR 136 típus a számítógép soros ill. PS2 portjára, míg az OCR150 típus a számítógép USB portjára csatlakoztatható. A kártyaolvasók oldalán található ragasztó csíkkal könnyen rögzíthetők PC-hez.

Az olvasók kifejezetten a B2B és B2C alkalmazásokhoz megfelelőek, és számos esetben használhatóak:

- Hozzáférés kontroll hálózatokhoz, távoli szerverekhez, és különböző e-szolgáltatásokhoz
- Elektronikus adatátvitel
- e-tárca tartalmának leolvasása

Az OCR 136 és az OCR 150 teljesen támogatja az Oberthur összes kártyatípusát, valamint az AuthentIC, AuthentIC Lite és Identrus alkalmazásokat is.

Az OCR 136 rendelkezik egy integrált szoftvercsomaggal Win95, 98, 2000, ME, és NT rendszerekhez.

Az OCR 150 szintén rendelkezik integrált szoftvercsomaggal Win98, ME, 2000 és LINUX rendszerekhez. Megjegyzés: A Microsoft Windows NT4 operációs rendszere nem támogatja az USB portot, ezért az ilyen esetekben az OCR 136 típus használata ajánlott (az operációs rendszer cseréjével természetesen az OCR 150 is használható).

2.2 Műszaki jellemzők

	OCR 136	OCR 150
Kapcsolat	RS232	USB
Kábelhossz	180 cm	180 cm
Áramellátás	PS/2	-
Interfész	Soros	USB
Kártya kapcsolati egység		
Smart áramellátás	Max. 60 mA	Max. 60 mA
Smart kártya interfész	ISO 7816	ISO 7816
Állapotjelző	duo-LED	Kérésre duo-LED
Protokollok	Asszinkron: T=0 (115 200 Baud-ig), T=1 (38 400 Baud-ig)	T=0 (9 600 Baud), T=1 (up to 115 200 Baud), T=14, szinkron: 2WBP (SLE4418/28), 3WBP (SLE4432/42)
Meghajtók	PC/SC, CT-API,	PC/SC - W98/2000/ME és Linux
Operációs rendszer	Win95, Win98, NT 4, Win2000/ME	Win98, Win2000/ME
Tanúsítvány	Mondex Level 1	PC/SC, Mondex Level 1
Átviteli sebesség	Átviteli módban PC és kártya között 9600 - 115200 Baud	-
Opciók	Lábazat	Lábazat

2.3 Használati útmutató

Csatlakoztatás. Telepítés

A kártyaolvasókat a használat előtt csatlakoztatni kell, majd fel kell telepíteni a számítógépre. Csatlakoztatás után (típustól függően: OCR136 – soros RS232, PS/2; illetve OCR150 – USB), elvégezhetjük a telepítést, amelyhez a szükséges illesztő programok a T-Systems honlapjáról (www.t-systems.hu) az e-Szignó oldalain található Kapcsolódó termékek menüpontból tölthetők le, tömörített állomány formájában. A kártyaolvasók helyes csatlakoztatása után kigyullad a kártyaolvasón egy zöld jelzőfény, amely a kártyaolvasó áramellátását jelzi.

Használat

A kártyaolvasók feltelepítése után lehetőségünk nyílik intelligens kártyák használatára. Így a Tanúsítványigénylés, Tanúsítvány letöltés valamint elektronikus aláírás funkciókat akkor tudjuk használni, ha a kártyaolvasónkat az adott munkaállomáshoz csatlakoztattuk, és feltelepítettük.

A kártyaolvasó használata során, ha a chipkártyára írás illetve olvasás történik (pl. elektronikus aláírás során), a zöld jelzőfény pirosra vált.

A kártyaolvasók használata során felmerült kérdéseivel kérjük, keresse fel ügyfélszolgálatunkat:

e-Szignó ügyfélszolgálat
1476 Budapest, Pf.: 227
E-mail: eszigno.fokozott@telekom.hu
Tel.: 06 80 20 40 40
Fax.: 06 1 447 4451