

Podporované OS

- Microsoft Windows 2000, 2003,
 - XP a Vista
- Apple Mac OS 10.4.6 (Tiger)

Šifrovací API

- PKCS #11 v2.01
- Microsoft CryptoAPI (CAPI) 2.0
 - Microsoft PC/SC
 - Apple Native PC/SC

Délka šifrovacích klíčů

- RSA 512 až 2048 bit

Šifrovací funkce & Algoritmy

Asymetrické klíče

- RSA

Symetrické klíče

- DES, 3DES

Elektronický podpis

- RSA, DSA

Hashovací funkce

- SHA-1

Výměna klíčů

- RSA
- Diffie-Hellman
- Vytváření klíčů na kartě
- DES hardwarový koprocesor pro bezpečné vytváření klíčů na kartě

Paměť EEPROM

- Kapacita 32K

Odpovídá

- FIPS 140-2 úroveň
 - ISO 7816
 - GSC-IS v2.1

Čipová karta model 330i

Finanční instituce a jejich klienti, kteří vytvořili Identrus systém pro zabezpečení B2B e-obchodu, využívají výhody použití čipové karty model 330i. Tento model plně podporuje Identrus. Identrus elektronické podpisy používají podepisovací klíče Identrus a jsou umístěné na čipové kartě. Ověření PINu je pro každou transakci taktéž prováděno na kartě. Model 330i obsahuje 6 odblokovacích PINů pro zjednodušení obnovení ztracených hesel a podporuje bezpečné zobrazení klíče pro rychlou personalizaci.



Vlastnosti:

- Čipová karta dle standardu ISO-7816.
- Plně odpovídá specifikaci Identrus čipové karty.
- Schváleno pro FIPS 140-2 úroveň 2.
- Šifrovací koprocesor pro urychlení.
- SCCOS operační systém čipové karty 32K je uložen v paměti ROM.
- 32K EEPROM pro bezpečné uložení klíčů, hesel, certifikátů a dat.
- Digitální podpisy Identrus používající podpisový klíč – umístění na kartě pro každou operaci.
- Ověření PINu pro každou operaci se uskutečňuje přímo na čipové kartě.
- Až 6 odblokovacích PINů pro zjednodušení obnovy ztracených hesel.
- Bezpečné zobrazení klíče pro rychlou personalizaci.
- Hardwarový koprocesor DES pro šifrování tajného klíče.
- Hardware a software má ochranu proti různým útokům.
- Funkce veřejného klíče (public key):
 - ◇ Generování DSA klíče (klíče o délce 1024-bitů).
 - ◇ Generování RSA klíče (klíče o délce 1024-bitů a 2048-bitů).
 - ◇ RSA/DSA klíče pro elektronický podpis.
 - ◇ Možnost výměny RSA klíčů.
 - ◇ Možnost výměny Diffie-Hellman klíče.
 - ◇ SHA-1.
 - ◇ Možnost šifrovat/dešifrovat pomocí unikátního klíče DES/3DES.

Standardy	ISO-7816- 2, 3, 4; PKCS #1; PKCS #11
Napájení	Maximálně 10mA
EEPROM	32K, neomezené čtecí cykly; zápis/mazání 100 000
Provozní teplota	-25°C to 70°C
Podporované čtečky	Sériové, USB, PCMCIA, Express Card a všechny čtečky podporující PS/SC protokoly
Operační systémy	Windows 95, 98, NT, 2000, XP, Vista

