

Šifrovací funkce na kartě

- RSA podpis/dešifrování 1024-2048
 - 3DES
- DSA podpis/ověření 1024
- SHA-1 hashovací funkce
 - AES128, 192, 256
- Diffie-Hellman výměna klíčů

Vylepšený šifrovací koprocessor pro urychlení

64K EEPROM pro bezpečné uložení

- Klíčů
- Hesel
- Certifikátů
- Aplikačních programů
- Dat

Možnost odblokování PIN uživatelem

Certifikáty

- FIPS 201
- FIPS 140-2 úroveň 2
- Common Criteria ALE 4 + (zažádáno)
 - RoHS

Šifrovací API

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

Šifrovací API

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

Odpovídá smart kartě formátu ISO 7816

Čipová karta model 400

Čipová karta model 400 – představuje silné šifrovací zařízení s 2faktorovou autentizací. Tato nová karta poskytuje vysokou úroveň bezpečnosti (certifikace FIPS 201, FIPS 140-2). 64K EEPROM paměť nabízí vyšší využití při ukládání privátních klíčů, certifikátů a hesel. Kartou je možno integrovat do mnoha aplikací a s produkty mnoha předních výrobců. Karta pracuje společně s klientským softwarem BSec PK nebo BSec SSO (více informací o tomto SW naleznete v sekci Software) a sériovou, USB, PCMCIA, nebo jinou povolenou PC/SC čtečkou čipových karet.



Vlastnosti:

- Čipová karta dle standardu ISO-7816.
- Schváleno pro FIPS 140-2 úroveň 2.
- Šifrovací koprocessor pro urychlení.
- SCCOS operační systém čipové karty 64K je uložen v paměti ROM.
- 64K EEPROM pro bezpečné uložení klíčů, hesel, certifikátů a dat.
- DES hardwarový koprocessor umožňující šifrování tajných klíčů přímo na kartě.
- 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, (SHA -2 bude podporován do konce r. 2009).
 - ◇ Možnost šifrovat/dešifrovat pomocí unikátního klíče DES/3DES.
 - ◇ Odblokování PINu.

| | |
|--------------------|---|
| 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 |

