

Secusmart Security Card Version 1.0 official datasheet

Hardware crypto component

Smart card controller

NXP SmartMX P5CT072 secure PKI crypto controller
 - Highspeed AES co-processor (128bit parallel processing AES engine)
 - PKI co-processor (Elliptic Curve Cryptography)
 - Random number generator in hardware, FIPS140-2 compliant
 TCOS 3.0

Card operating system
 Security Application in EEPROM
 Certification

BOS-Digital end-to-end encryption application v.3.4
 Common Criteria EAL5+

End-to-end voice encryption

- Symmetric voice encryption with 128bit AES
- Authenticated key exchange with Elliptic Curve Diffie-Hellman
- Fast key exchange <4s

Certificate-based user authentication

- Public key infrastructure based on BOS-Digital 3.4
- Trustcenter: Secusmart Root CA hosted by T-Systems
- Elliptic Curve Certificates

PIN protection

- Electronic seal (Zero-PIN)
- 4 digit PIN-Code

Compliant with Nokia S60 phones

- Operating system Symbian 9.2
- User interface Nokia S60 version 3.1
- Supported phones Nokia Eseries / Nseries

Symbian Signed Client Software

Communication

- Bearer type GSM CSD
- Voice codec GSM-AMR
- Round trip delay 900ms
- Call set-up time <5s (same as GSM voice calls)

Power consumption

- Power saving IDLE mode unmeasureable
- low-power active-mode < 9mW

MicroSD-card

- Flash storage

