

**Technická a certifikační specifikace****DI CRYPTO JAVA CARD****EEPROM paměť**

Čip: 80kB, využitelnost: 67kB

**Typ karty**

Hybridní

**Formát**

ID-1

**Standardy**Java Card 2.2.2., GP 2.1.1  
SCP01/SCP02 / SCP03 OT  
ISO 7816 (1-9)**Kryptografický algoritmus**AES-128/192/256bits, DES, 3DES,  
RSA od 512 do 2048 bitů**Standard bezkontaktního rozhraní**MIFARE ISO/IEC14443-2  
MIFARE ISO/IEC 14443 Type A (MIFARE 1 KB)**Délka RSA klíče**

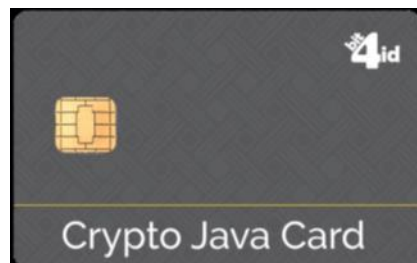
Do 2048 bitů

**Podpora eliptické kryptografie**Diffie-Helman  
160/192/224/256/384/521 bitů**Podpora Secure Messaging****Počet cyklů vložení/vyjmutí karty**

500 tisíc cyklů

**Sériové číslo**

Jedinečné sériové číslo

**Komunikace**

podpora CSP a PKCS#11

**Hash algoritmu**

SHA1, SHA-2, SHA-224, SHA-256, SHA 384, SHA 512

**Vzdálenost účinnosti bezkontaktního čipu**5 – 10 cm  
v závislosti na dané čtečce**Frekvence**

13.56 Mhz

**Podporované operační systémy**

Windows 7 a vyšší, Linux and MAC OS X

**Rychlost přenosu**

106 kb/s

**Magnetický proužek**

High Coercivity Magnetic Stripe (HiCo)

**Komunikační protokol**

T=0, T=1, bezkontaktní

## Certifikace

Čipová karta s kontaktním čipem splňuje podmínky QSCD certifikace.

Certifikace čipu

CC EAL5+,

SO certifikace

CC EAL4+

FIPS 140-2 level 3

Podpora normy

ISO/IEC78161-6,8,9standard,I/Ospeedupto31cycle/etu

ISO/IEC14443TypeA(MIFARE1KB)