



SMART CARD ADAPTER

D'Crypt's Smart Card Adapter is a card-neutral OEM reader module that operates with various types of contactless smart cards. The Smart Card Adapter comprises a FIPS140-2 Level 3 certified cryptographic core and integrates interfaces to contactless A, B, and C cards. The adapter can be integrated with LCD and casing as a payment or loyalty terminal, or be integrated into ATMs or vending machines. With all keys stored in the cryptographic core, additional security devices like SAMs are no longer necessary.

Technical Specifications*

Configuration

- Processor – ARM-based processing core
- Main Memory – 4MB Flash ROM and 80KB SRAM

Electrical

- Power source – +5V ±5% DC, 400mA max.
- Meets 47 CFR FCC Part 15C

Contactless Smart Card Interface

- Supports ISO14443A/B and ISO 18092
 - Operating frequency: 13.56MHz
 - Free-Space Operating Distance: up to 3.5cm from board's top surface¹

Connections / Peripheral Interfaces

- EIAJ RC-5320A std Ø5mm DC power jack
- EIA561 (DCE) Host Interface
 - Max baud rate of 460.8Kbps
 - Interfaces directly to PoS and other devices.
- LCD Interface
 - Supports standard 8-bit bus addressable display
- Matrix Keypad Interface
 - Up to 3x5 keypad supported
- Audio Interface
 - PWM output for driving integrated buzzer
- Configuration and Key Loading Interface
 - 3-wire TTL-serial port operating at 115.2Kbps
- Two-pin Molex connector to power indication LED

Security

- Secure micro O/S
- BiST (Built-in Self-Test)
- 256-bit factory-programmed un-erasable Factory ID
- 256-bit one-time programmable User ID
- 32-character one-time programmable Serial Number
- UTC clock
- Code loading verification
- Tamper Resistant and Evident construction
- Cryptographic core certified to FIPS 140-2 Level 3 (Certificate No. 637)

Cryptography

- Algorithms supported:

| Algorithm (Mode) | Key Length |
|-----------------------------------|---------------|
| DES (ECB, CBC, CFB64, OFB64) | 64 |
| TDEA (ECB, CBC, CFB64, OFB64) | 128, 192 |
| AES (ECB, CBC, CFB128, OFB128) | 128, 192, 256 |
| RSA (Encrypt/Decrypt/Sign/Verify) | 512 – 2048 |
| HMAC-SHA-1 | 80 – 160 |
| SHA-1 | – |
| PRNG (ANSI X9.31-compliant) | 128 |

- All cryptographic algorithms are FIPS-approved and are operated in FIPS-approved modes
- CRYPTO OFFICER and multiple user roles
- Identity-based challenge-response authentication
- Key Management
 - Comprehensive key-management framework customizable through key profiles
 - APIs reference keys through opaque handles
 - Encrypted key entry (loading) and exit (archival)
 - Key generation using FIPS-approved RNG
- Application loaded and verified with 2048-bit RSA signature
- Application Partition
 - Dedicated application partition with separate code, stack, and data space

Application Development

- Linux/GNU based software development environment
- Supports Windows 2K/NT/XP and Linux

Environment

- Operating temperature: +5°C to +60°C
- Storage temperature: 0°C to +80°C
- Humidity: maximum 85% non-condensing

Module Size (dimensions in mm)

- 55 x 60 x 42 mm (Depth x Width x Height)

*Specifications subject to change without notice

¹ Centre of Contactless Smart Card (CSC) shall be aligned to the center of the antenna and the CSC shall be parallel to the Antenna plane. CSC detection range is the distance between the top surface of Antenna and the surface of the CSC.

Another quality product by:
D'Crypt Pte Ltd
 20 Ayer Rajah Crescent, #08-08 Singapore 139964
 DID: +65 6773 9016 FAX: +65 6873 0796
 URL: <http://www.d-crypt.com> Email: marketing@d-crypt.com

SMART CARD ADAPTER

Mechanical Drawing

