

ACOS 3



Functional Specification

Introduction

The purpose of this document is to describe in detail the features and functions of the ACS Smart Card Operating Systems Version 3 (ACOS3) developed by Advanced Card Systems Ltd.

Features

- Full 32/72 Kbytes of EEPROM memory for application data.
- Compliance with ISO 7816 parts 1, 2, 3; supporting the T=0 direct protocol.
- ISO7816-2 compliant 8-contact module.
- High-speed transmission possible (9.6 to 223.2 kbps) with modifiable ATR.
- DES / 3DES and MAC capabilities.
- Five secret codes + issuer code.
- PIN code that can be updated by card holder.
- Key pair for mutual authentication.
- Session key based on random numbers.
- FIPS140-2 compliant hardware-based random number generator.
- Binary files and record files are available for user data storage.
- Secure messaging option ensures transmission of user data is secured against eavesdropping, replay attack and unauthorized modifications.
- Highly secured e-Purse for payment applications.
- Completely backward compatible with ACOS1 / ACOS2 /ACOS3-24/64 cards.

Technical Specifications

The following are the technical properties of the ACOS3 card:

Electrical

- Operating at 5V DC +/-10% (Class A) and 3V DC +/-10% (Class B)
- Maximum supply current: <10 mA
- ESD protection: ≤ 4 KV

EEPROM

- Capacity: ACOS3-32: 32 Kilobytes (32,768 bytes)
ACOS3-72: 72 Kilobytes (73,728 bytes)
- EEPROM endurance: 100K erase/write cycles
- Data retention: 10 years

Environmental

- Operating temperature: -25 °C to +85 °C
- Storage temperature: -40 °C to +125 °C