



ACOS5-EVO

Cryptographic Smart Card with
ECC and RSA support

ACOS5-EVO, the latest addition to the ACOS5 Series, is cryptographic smart card module from ACS especially designed for Public Key-based applications.

The ACOS5-EVO offers additional cryptographic algorithms which includes ECC on top of the existing RSA support. It also includes additional support for SHA224, SHA312 and SHA512 on top of the existing SHA1 and SHA256 support. For symmetric algorithms, DES/3DES and AES are included and for MAC, CMAC using 3DES and AES are included.

It is a high speed card with extended APDU support and is fully compliant with ISO 7816 parts 1, 2, 3, 4, 8 and 9 as well as other international standards for PKI smart cards such as FIPS 140-2 (US Federal Information Processing Standards) Level 3 and CC EAL 5+ (chip level).



Standard Features

Smart Card Features		Certifications/Compliance	
T=0, T=1	✓	ISO 7816 Parts 1-4	✓
Extended APDU	✓	ISO 7816 Parts 8, 9	✓
192 KB Memory	✓	Common Criteria EAL5+ Certified (Chip Level)	✓
Anti-Tearing	✓	FIPS 140-2 Level 3 Compliant	✓
Cryptographic Capabilities		Customization	
ECC: P-224/P-256/P-384/P-521		PVC/PET/ABS	✓
RSA: up to 4096 bits		Hi-co/Lo-co Magnetic Stripe	✓
DES/3DES: 56/112/168-bits (ECB, CBC)		Color Printing	✓
AES: 128/192/256 bits (ECB, CBC)		Signature Panel/Barcode	✓
Hash: SHA1, SHA224, SHA256, SHA384, SHA512			
MAC: CMAC (3DES, AES), CBC-MAC (DES/3DES, AES)			
Secure Messaging			
Mutual Authentication			

Typical Applications

- ✓ Public Key Infrastructure (PKI)
- ✓ Digital Signature
- ✓ e-Government
- ✓ Network Security
- ✓ Access Control
- ✓ Blockchain Applications