

THALES



SafeSign Crypto Module

www.thalesgroup.com/esecurity

Technical Specifications

PROGRAMMING INTERFACES

Interface Type	Industry Standard PKCS#11 v2.01
Cryptographic Functions	DES and triple-DES key generation, encryption and decryption DES and triple-DES MAC generation and verification RSA key pair generation, signature and verification (512 to 2048 bits) DSA key pair generation, signature and verification (512 and 1024 bit) HMAC signature and validation (160 bits) Secure Socket Layer (SSL) v3 key generation and derivation mechanisms MD5 and SHA-1 message digest Certificated storage within Tamper-resistant memory Hardware-based random number generator
Specialised functions	MasterCard CAP and Visa DPA Token Authentication including Thales PSM, WatchWord and Vasco
Operating Systems	Microsoft Windows NT 4.0, 2000, XP and 2003 RedHat Linux 7 or 8 or equivalent kernel SUN Solaris 8 and 9

DEVICE SECURITY

Physical Security	Tamper evident chassis Tamper detection envelope surrounds cryptographic module Motion detection, temperature sensitive device and protection against voltage, chemical and penetration attacks
Security Certification	Security sub-system validated FIPS 140-1 level 4 Security sub-system under validation to FIPS 140-2 level 4 FIPS 140-2 Level 2 compliant tamper evidence detection

DEVICE SPECIFICATIONS

Communications Interfaces	Doubled 10BaseT Ethernet Smart card reader with integral PIN Pad RS232 auxiliary management port accessible from front or back of unit
Regulatory	CE, FCC, UL
Power	Auto-Sensing 110-240V AC/50-60 Hz Internal Power Supply
Environmental	Operating Temperature: -5°C to 40°C (23°F to 100°F) Storage Temperature: -10°C to 60°C (15°F to 140°F) Relative Humidity: 10% to 90% at 25°C (77°F) Non-Condensing Barometric Pressure: 780 to 1100 mBar
Physical Specifications	H 88mm (3.47") x W 482mm (18.8") x D 243.70mm (9.66") 2U x 19" rackable unit

EUROPE, MIDDLE EAST, AFRICA

Meadow View House, Crendon Industrial Estate, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, UK
Tel: +44 (0)1844 201800, Fax: +44 (0)1844 208550, e-mail: emea.sales@thales-esecurity.com

AMERICAS

2200 N. Commerce Parkway, Suite 200, Weston, Florida 33326, USA. Tel: +1 888 744 4976, +1 954 888 6200, Fax: +1 954 888 6211, e-mail: sales@thalesesec.com

ASIA PACIFIC

Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road, Central, Hong Kong, PRC. Tel: +852 2815 8633, Fax: +852 2815 8141, e-mail: asia.sales@thales-esecurity.com

