

# SnapCrypt



Snapcrypt addresses the requirements for high performance cryptographic cores by offering cryptographic libraries optimized for Texas Instruments DSP and the ARM RISC processors. Snapcrypt features a small memory footprint combined with exceptional efficiency that minimizes the impact on battery life. Snapcrypt provides a complete suite of industry standard cryptographic libraries. These cryptographic libraries enable application developers to easily integrate encryption, hash functions, digital signatures and key exchange mechanisms into embedded systems.

Powered by industry-standard cryptographic algorithms and optimized for mobile applications, Snapcrypt will enable rapid and robust implementation of security applications in embedded systems. Snapcrypt is also FIPS 140-2 level 2 approved.

Snapcrypt provides all popular private and public-key encryption algorithms (including all algorithms required by IPsec standard), such as DES, Triple DES and AES algorithm for symmetric encryption, with key exchange protected by ElGamal and Diffie-Hellman, MD5 and SHA-1 hash functions along with their keyed versions (HMAC), RSA, ECC and DSA for digital signatures. Snapcrypt also supports all known mobile operating systems.

## Key Benefits

- Reduces processing power requirements
- FIPS 140-2 Level 2 Approved
- Optimized for wireless and mobile applications
- Efficient use of computing resources minimizes impact on battery life
- Low footprint design
- Supports TI's eXpressDSP and ARM RISC Processor
- High-performance low performance security
- Ideal for: mobile applications & multimedia applications
- Optimized for Texas Instruments DSP and ARM processors
- High performance & efficiency
- Supports all popular encryption algorithms
- Fast time-to-market
- Supports TI eXpress DSP standard

## Technical Specifications

Supported Platforms	TI DSP C54x; TI DSP C55x; TI DSP C62x; TI DSP C64x; TI OMAP; ARM7; ARM9; ARM10; ARM11; XScale.
Standards Compliance	Supports algorithms as used in government, financial and Internet standards, including all the algorithms required by IPSEC. Compliant with ANSI, FIPS, IETF, PKCS and PacketCable standards.
Key Agreement	Diffie-Hellman; ECDH.
Digital Signatures	RSA; DSA; ECDSA.
Public Key Encryption	RSA; ElGamal
Symmetric Block Ciphers	DES; Triple DES; AES. Support all the FIPS approved modes of operation.
Hash Functions	MD5; All the Secure Hash Algorithms (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512); MMH,
Message Authentication Code (MAC)	HMAC-MD5; HMAC-SHA; MMH-MAC; CCM



**Kane Computing Ltd**  
**7 Theatre Court, London Road,**  
**Northwich, Cheshire, CW9 5HB, UK.**  
**Tel: +44(0)1606 351006**  
**Fax: +44(0)1606 351007/8**  
**Email: [sales@kanecomputing.com](mailto:sales@kanecomputing.com)**  
**Web: [www.kanecomputing.co.uk](http://www.kanecomputing.co.uk)**