

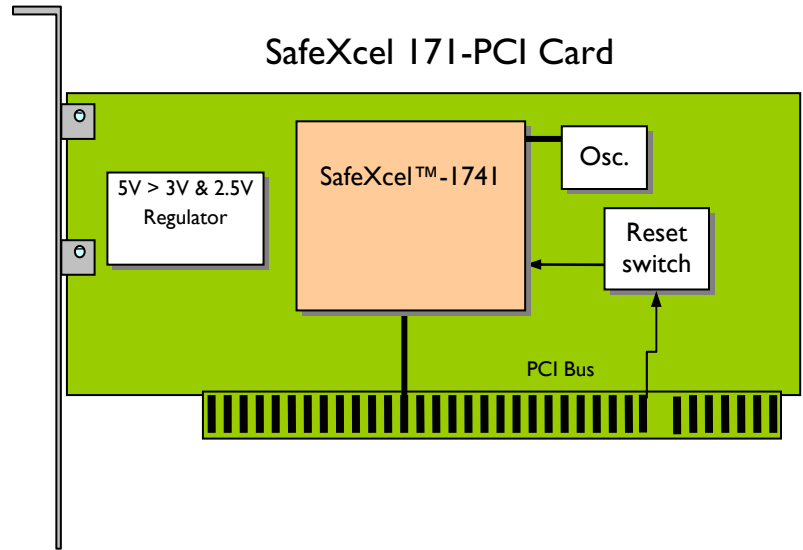


## Software Developer's Kit

SafeNet offers a Developer's Kit which contains 'C' header files, sample applications, Test code and PCI drivers for Win NT/2000, Linux, and VxWorks to assist the software developer in producing applications. Contact SafeNet, Inc. for more information.

## Applications

- Broadband access devices (xDSL, Cable Modem, NIC)
- SOHO router
- Set-top box / Internet appliances
- Wireless (Bluetooth, 802.11x, 2.5G/3G)



## Specifications

### IPSec Throughput

- 290 Mbps sustained ESP (AES, MD5, 1500 byte packets)
- 260 Mbps sustained ESP (3-DES, SHA-1, 1500 byte packets)
- 90 Mbps sustained ESP (3-DES, SHA-1, 64 byte packets)

### Symmetric Encryption Block

- 1056 Mbps Single-DES
- 352 Mbps Triple-DES
- 845 Mbps AES
- Supports all modes: ECB; CBC; OFB;
- 1, 8, 64-bit CFB(DES), 128-bit CFB(AES)
- Multi-mode Padding support
- Implements IPsec ESP transforms

### Hash Block

- Hardware-based MD-5 and SHA-1
- 520 Mbps MD-5
- 417 Mbps SHA-1
- Implements IPsec AH and HMAC
- Includes mutable bit handler for AH, including IPv4 option and IPv6 extension headers

### Public Key Accelerator

- Accelerator for math-intensive public key operations up to 2048-bit modulus size
- Diffie-Hellman negotiate: 5.1ms (1024-bit modulus, 180 exponent)
- RSA 1024-bit sign: 8.4ms
- RSA 1024-bit verify: .85ms
- DSA Sign: 8.9ms, DSA Verify: 20.5ms

### Protocol Support

- Full IPsec transforms including ESP, AH and bundled header/trailer processing
- Basic Encrypt, Decrypt, Hash and HMAC operations

### Random Number Generator

- Hardware-based Non-deterministic Random Number Generator
- Can generate session keys, IV's, public and private key seeds, etc.
- Up to 1 Mbit of Random Data per sec.

### CGX Library

- Advanced cryptographic library, with Integrated Key Management support
- Targeted to Host processor.

#### Symmetric Algorithms

- DES/3DES (hardware accelerated)
- AES Rijndael
- ARC4, ARC5

#### Hash Algorithms

- SHA-1 (hardware accelerated)
- MD5 (hardware accelerated)
- RIPEMD-128
- RIPEMD-160

#### Compression Algorithm

- Deflate

#### Protocol Support

- IPsec ESP & AH (hardware accelerated)
- IPsec IKE (hardware accelerated)
- IPcomp
- SSL, WTLS

### PCI Interface

- 32-bit 3.3V or 5V bus interface
- 66 MHz max bus speed
- PCI v2.2 Compliant
- Bus Master and Target Capability

### Environment

- Operating Temperature: 0 – 70°C
- Storage Temperature: 0 – 85°C
- Operating Humidity: 10 – 90% RH

### Electrical

- PCI Voltage: 5V ±10%
- PCI Bus Signaling: 3.3V or 5V
- Power Consumption: 1W typical

### Mechanical

- Standard PCI 'short' card
- 17.5 cm x 10.7 cm
- 6.875" x 4.2"

Also available: PCI mini card

- 12 cm x 5.1 cm
- 4.75" x 2"

Distributors and resellers located worldwide.



Corporate: 4690 Millennium Drive, Belcamp, MD 21017, USA Tel: 410.931.7500 or 800.533.3958 eMail: info@safenet-inc.com

Australia +61 3 9882 8322  
Brazil +55 11 6121 6455  
China +86 10 8266 3936  
Finland +358 20 500 7800  
France +33 1 41 43 29 00  
Germany +49 18 03 72 46 26 9  
Hong Kong +852 3157 7111

India +91 11 2691 7538  
Japan +81 3 5719 2731  
Japan (Tokyo) +81 3 5719 2731  
Korea +82 31 705 8212  
Mexico +52 55 5575 1441  
Netherlands +31 73 658 1900  
Singapore (1) +65 6274 2794

Singapore (2) +65 6297 6196  
Taiwan +886 2 6630 9388  
UK +44 1932 579200  
UK (Basingstoke) +44 1256 345900  
U.S. (Massachusetts) +1 978.539.4800  
U.S. (New Jersey) +1 201.333.3400  
U.S. (Virginia) +1 703.279.4500

U.S. (Irvine, California) +1 949.450.7300  
U.S. (Santa Clara, California) +1 408.855.6000  
U.S. (Torrance, California) +1 310.533.8100