Features

Support of Standards
The SafeXcel-2141 supports many standards used to implement secure systems:

- IPSec - ISAKMP/Oakley negotiations in all modes, IPSec transforms per IETF RFC 2401 through 2412
- FIPS-140-1 - strict U.S. Federal security standard
- X9.17 - International banking key management guideline

OEMs can concentrate on making their security systems unique in the marketplace, while the SafeXcel-2141 assures that expected standards are adhered to.

The DSP core may be programmed using standard Analog Devices software development tools. A SafeXcel Developers Kit is available from SafeNet.

Enables High Throughput VPN.

Integrates into networking and telecommunications equipment to enable high throughput VPNs with strong security

Overview
The SafeXcel™-2141 from SafeNet is the first product in a family of embedded encryption solutions. With sustainable throughput of Triple DES IPSec transforms at OC-3 (155 Mbps) rates, the SafeXcel-2141 offers high performance at reasonable price points. The on-chip SafeNet CGX Library of cryptographic functions simplifies security system development for the OEM designer. In addition, the DSP core of the SafeXcel-2141 is fully programmable by the user, affording the designer a high level of flexibility in customizing and differentiating the final security system.

The SafeXcel-2141 is an enabling technology for the Internet—allowing OEMs to develop the high throughput and highly-secure networking and telecommunications products required to proliferate applications such as eCommerce and Extranets.

SafeNet and Analog Devices (ADI) teamed together to create this new class of security system-on-a-chip. The combination of SafeNet’s patent-pending SecureIP Technology™ with ADI’s IC design expertise made this invention the industry's first DSP-based solution for secure communications.

Safe at High Speeds
The SafeXcel-2141 is a highly integrated “security system on a chip” incorporating a sophisticated, general purpose DSP core, several high-performance cryptographic function blocks, as well as PCI, External Memory and Serial EEPROM interfaces. The SafeXcel-2141 architecture segregates security functions in a kernel separate from standard processing functions. This hardware approach provides an unprecedented level of security for commercial applications. The on-chip bus is automatically isolated to prevent access to sensitive information such as keys.

Hash/Encrypt
The Encrypt Block performs high-speed DES and Triple DES encrypt/decrypt operations. All 4 standard modes of DES are supported: Electronic Code Book (ECB), Cipher Block Chaining (CBC), 64-bit Output Feedback (OFB) and 1-bit, 8-bit and 64-bit Cipher Feedback (CFB). The DES encrypt/decrypt operations execute full 16-round DES in only 4 clock cycles.

The Hash Block is tightly coupled with the Encrypt Block and accelerates one-way hash functions. Both the MD5 and SHA-1 algorithms are supported. Combined operations which chain both hashing and encrypt/decrypt functions significantly reduce the processing time for data which needs both operations. The SafeXcel-2141 can perform parallel execution of both functions from the same source and destination buffers, with an optional offset between operations.

Public Key Acceleration
The Public Key Accelerator module works in concert with the CGX Toolkit firmware to provide full public key services to the host application. The Toolkit provides Macro-level functions to perform Diffie-Hellman Key Agreement, RSA Encrypt or Decrypt, Calculate and Verify Digital Signatures, etc. The hardware accelerator block speeds computation-intensive operations such as large vector arithmetic.

Random Number Generation
The Random Number Generator provides a true, non-deterministic noise source for the purpose of generating keys, Initialization Vectors (IVs), and other random number requirements. The CGX Kernel requests random numbers as needed to perform requested CGX commands such as Gen-Key, and can also directly supply from 1 to 65,535 Random Bytes to a host application via the Random-CGX command.
Technical Specifications

High Throughput
- 3-DES at 214 Mbps
- DES at 640 Mbps
- MD5 at 315 Mbps
- SHA-1 at 253 Mbps
IPSec Transforms Triple-DES, SHA-1 at OC-3 rates (155 Mbps)

Strong Security
- Unencrypted keys never leave the SafeXcel nor reside in unprotected memory
- Facilitates certification FIPS 140-1
- Security functions isolated by DSP-controlled protection circuitry

Fast Development Time
- SafeNet CGX Toolkit and Library of Cryptographic functions embedded on-chip
- ADSP-218X DSP Core is user programmable

Electrical
- Lock rate: 40 MHz
- Voltage: 3.3 V
- Temperature: 0-70° C

Package
- 208-lead Metric Quad
- Flat Pack

Laser Variable Storage

The Laser Variable Storage consists of 256 bits of Tamper-Proof factory-programmed data which is only accessible to the internal function blocks and the Security Kernel and uniquely identifies the SafeXcel-2141. Included in these Laser Variable bits are master key storage and program control to enable or disable SafeXcel-2141 features.

Secure Code Download

Additional security functions may be added to the SafeXcel-2141 through a Secure Download feature. Code may be downloaded into internal DSP memory and given the security privileges of the CGX Toolkit firmware. Additional functions could include new encryption, hash or public key algorithms such as IDEA, RC-4, RIPEMD, or Elliptic Curve.

Fast Development Time

Developing and implementing embedded security systems is a complex issue. The SafeXcel-2141 has simplified this task by incorporating in one chip accelerated performance of critical security algorithms and high-level security functions using the SafeNet CGX Library. The library executes on a high performance, user programmable general purpose DSP Core. Designers concentrate on integrating security into their system in the best and most cost-effective manner, instead of focusing on the development of complex security algorithms or combining these algorithms into industry standard implementations like IPSec. That essential security work is done for the designer by the SafeXcel-2141.

SafeNet CGX Library

The SafeNet CGX Toolkit and Library is programmed into ROM within the DSP Core, rendering it tamper-proof. The Library provides the Application Programming Interface (API) for applications which require security services from the SafeXcel-2141. The applications may be software executing in the ‘User Mode’, or Host software accessing the SafeXcel-2141 via a PCI bus. Forty security commands, called CGX (Crypto-Graphic eXtensions), are provided at the API. The firmware runs under a ‘Protected Mode’ state. This guarantees the security integrity of the system during the execution of security functions, and, for example, prevents disclosure of cryptographic key data or tampering with a security operation.

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 email: info@safenet-inc.com

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
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 26917538