

In order to make next-generation processors suitable for fast and reliable security processing, chip designers are often faced with two options: designing security features from scratch, which often results in lengthy and expensive design cycles, or licensing silicon-proven semiconductor IP from a trusted security vendor that makes it easy and cost-effective for chip designers to integrate advanced security functionality into various semiconductor designs, such as NPUs, communications processors, and custom ASICs and FPGAs.

AuthenTec provides high-performance, highly integrated security engines that support cryptographic algorithms and protocol-related security operations for a wide range of applications. Silicon-proven and ready-to-use, the SafeXcel™ IP security engines are a reliable security solution for chip designers—delivering quick time-to-market while reducing design cost.

BENEFITS

- Silicon-proven
- High degree of integration
- World-class support
- Easy to integrate
- Modular design
- Reduces time to market
- Supports wide range of applications

Broad Suite of Security Engines

SafeXcel IP solutions enable OEM customers to rapidly implement a wide range of security functions in system-onchip designs, including cryptographic building blocks, VPN packet engines for SSL and IPSec, and content inspection engines.

VPN Packet Engines

SafeXcel IP – Packet Engine

- Highly integrated, lookaside security processor
- Support for IPSec, SSL/TLS/DTLS, MACsec and SRTP packet transforms
- Support for IPv4, IPv6, and Jumbo packets
- Support for DES/3DES, AES, ARC4
- Support for MD5, SHA-1, GMAC, SHA-256/512, AES-XCBC-MAC-96
- Support for Pseudo Random Number Generation, True Random Number Generation, AES-XCBC-MAC-PRF
- Support for AES-GCM (ESP and 802.1ae (MACsec) mode) and AES-CCM (WiMAX and Wi-Fi)
- Support for public key operations (including ECC) SafeXcel IP – Inline Packet Engine
- Highly integrated inline security processor
- Support for IPsec, MACsec and SRTP packet transforms
- Packet classification, flow processing, and firewalling
- Support for IPv4, IPv6 and Jumbo packets
- NAT, NAPT, NAT-T
- Support for DES/3DES, AES
- Support for MD5, SHA-1, HMAC, GMAC, SHA-256/512, AES-XCBC-MAC-96
- Support for Pseudo Random Number Generation, AES-XCBC-MAC-PRF
- Support for AES-GCM (ESP and 802.1ae (MACsec) mode) and AES-CCM (WiMAX and Wi-Fi)

Cryptographic Building Blocks

SafeXcel IP - DES / 3DES Accelerators

SafeXcel IP - AES, AES-GCM and AES-XTS Accelerators

SafeXcel IP - ARC4 Accelerators

SafeXcel IP - MD5/SHA-1/SHA-256/512 Accelerators

SafeXcel IP - True Random Number Generator

SafeXcel IP - Public Key Accelerators

Mobile Security Engines

SafeXcel Trusted Module IP

- Highly integrated module, designed for use in wireless and consumer devices
- Provides trust boundary in order to protect secret information from being compromised
- Small silicon footprint, low power requirements
- Supports hardware acceleration for encryption and hashing functions (DES/3DES, AES, MD5, SHA-1)
- Supports Public-Key Operations
- Supports True Random Number Generation
- Enables emerging mobile applications such as DRM (Digital Rights Management)



Ease of Integration and World-class Support

Years of experience in designing silicon security products made AuthenTec the leading vendor of complete, reliable, and high-quality semiconductor IP products, featuring cost-efficient designs and user-friendly product interfaces. AuthenTec's global presence and expertise in security IP design enables us to provide our customers with world-class OEM support that is unmatched in the industry — supporting your design-in process and ensuring the success of your project.

Complete Hardware/Software Solution

SafeXcel IP is a key component of AuthenTec's fully integrated security systems for OEMs. AuthenTec offers a wide range of security solutions for Telecommunications, SME, SOHO, ODM/OEM and Semiconductor markets with products that include QuickSec software development toolkits, SafeXcel hardware security co-processors and semiconductor IP. This complete suite of integrated security hardware and software products enable vendors to build complete network security.

DELIVERABLES

Synthesizable Verilog RTL source code

- RTL test bench, including test vectors and expected result vectors
- Simulation script
- Synthesis script
- User Documentation : Data Sheet and Developer's Manual

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, FL 32901 USA
+1-321-308-1300

WORLDWIDE REPRESENTATIVES NETWORK
A complete listing of AuthenTec's network of representatives is available at our web site.

For more information about Embedded Security Solutions: embedded@authentec.com
www.authentec.com/embedded