

SafeXcel - SafeZone Secure Platform

Complete Secure Platform Solution for Mobile and Consumer Applications

AuthenTec's SafeZone Secure Platform consists of Hardware and Software components that form the foundation of the Secure Platform for mobile communications and consumer electronics appliances where authentication and process encrypted content using standard protocols are required. This set of components provide a low cost, low power and small footprint IP solution for providing system and platform integrity, and symmetric cryptographic acceleration services to applications. The key features of Secure Platform are Secure Boot, Secure Storage, Secure Execution, Hardware Root of Trust, Secure Communication, and Secure Asset Store.

SafeXcel-IP-123 Crypto Module

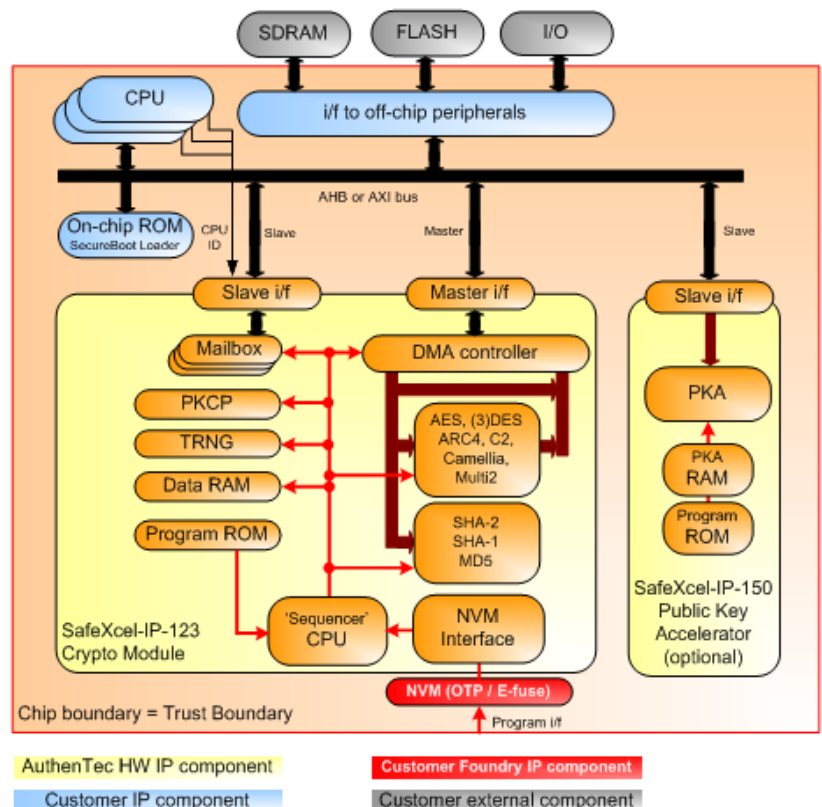
The core of the product is the SafeXcel-IP-123 Crypto Module that provides a closed execution environment with a security boundary and hardware crypto engines (MD5, SHA1, SHA2, AES, DES, 3DES, ARC4, TRNG, and optionally Camellia, C2, and MULTI2). The SafeXcel-IP-123 hardware Crypto Module adds security benefits compared to a software only solution. The hardware solution provides privileged access to the Non Volatile Memory where the secrets (root of trust) are stored as well as key generation using the embedded True Random Number Generator.

Key Features

- Low cost, low-power, and small footprint IP
- Internal storage and management for protection and management of sensitive keys and assets
- Encryption engines to offload computational intensive symmetric algorithms: AES, DES, 3DES, ARC4, Camellia, C2 and Multi2
- Hash engine to offload computational intensive hash algorithms: MD5, SHA-1 and SHA-2
- True random number generator (TRNG) including ANSI X9.31 AES-post-processing.
- Easy to integrate AHB or AXI interface for common embedded processors
- Embedded EIP-141 DMA controller for high speed symmetric crypto and hash data transfer
- Root of Trust as true hardware interface to on chip non-volatile memory
- Optional EIP-150 Public Key Accelerator

Inside the Crypto Module, key material and other cryptographic secrets can be protected against disclosure, modification and unintended use, while this material can be used by the hardware crypto engines. The Crypto Module has an embedded processor that runs its firmware that is stored in ROM.

SafeZone Secure Platform Hardware Components:
EIP-123 Crypto Module & EIP-150 Public Key Accelerator



The Crypto Module can provide cryptographic services to multiple applications simultaneously, with all applications running on one host or a variety of hosts like CPUs and DSPs. The SafeZone software modules are designed to run on these hosts.

A few special cryptographic secrets like the Root Key or Hardware Unique Key (HUK) are programmed into the device Non-Volatile Memory (NVM) during manufacturing. For security reasons, the NVM is only readable by the Crypto Module. CRC is used to verify the integrity of the static assets. The exact data objects to store in NVM can be customized.

The optional SafeXcel-IP-150 Public Key Accelerator provides powerful modular mathematical operations required for Public Key algorithms like RSA and ECDSA, like Modular Exponentiation and Elliptic Curve Cryptography (ECC). The Public Key Accelerator runs Firmware, which is stored in ROM or downloaded into RAM. The Public Key Accelerator provides acceleration but no security like the Crypto Module.

SafeZone Secure Asset Store

The Internal storage and management for protection and handling of sensitive keys and assets is achieved through the Secure Asset Store feature in AuthenTec’s Secure Platform. Protecting the key material from disclosure and modification, allowing key material to be used by the cipher and hash cores inside the Crypto Module, allowing keys to be securely wrapped (AES SIV, RFC5297) and stored in off-chip flash for permanent storage. This will make sure that the secure assets are never exposed outside of the trusted boundary.

SafeZone Secure Boot

AuthenTec’s Secure Platform solution provides complete Secure Boot functionality. Secure Boot is needed to make sure that only the software images from an authorized source are booted, corrupted software images are not booted; and downgrading software images to a version with possibly known security holes is prevented. Software image can also be encrypted preventing software reverse engineering.

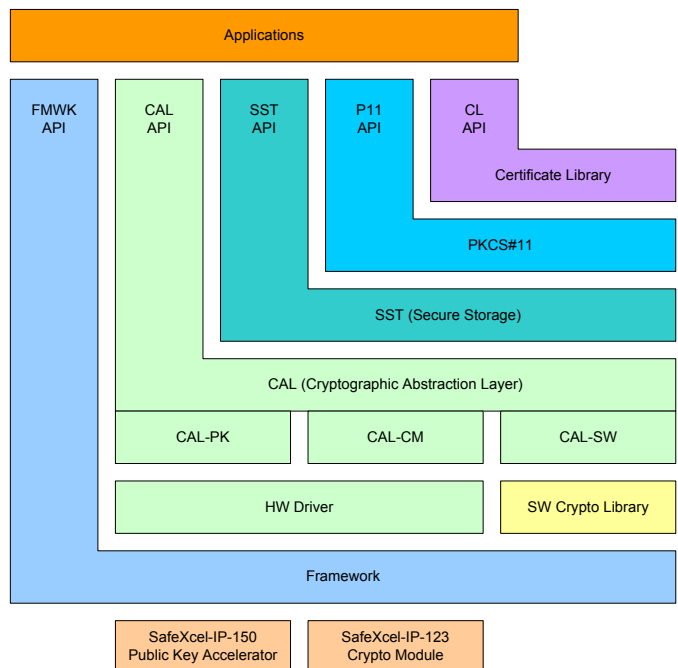
SafeZone Software — Complete Security Solution

To address the difficulties of security integration across hardware, software and application layers, AuthenTec

provides a unique middleware solution - SafeZone Software. SafeZone Software is an integrated security middleware that enables application developers to transparently utilize and easily integrate hardware-based security services. The SafeZone middleware provides the certificate and cryptographic protocols and algorithms essential to applications while ensuring API compatibility and seamless upgradeability to future generations of processors and mobile devices. With SafeZone Software, software developers can take full advantage of sophisticated security mechanisms, and develop robust and future-proof mobile applications that are optimized for the resource-constrained wireless environment. SafeZone Software allows applications to be quickly integrated into an established ecosystem of security solutions, ensuring quick adoption of mobile applications in the marketplace. The software has been designed for resource-constrained environments like mobile phones and to support industry standards like the Open Mobile Alliance DRM, OMTP TR1 Secure Storage and Secure Boot and the PKCS#11 Cryptographic Token Interface Standard.

SafeZone Secure Platform Software Components:

Certificate Library, PKCS#11 Library, Secure Storage Library, Cryptographic Abstraction Layer, Hardware- and Platform Abstraction Framework



Key Features

- PKCS#11 API to applications
- Fully integrated with key protection and usage mechanisms offered by Asset Store
- Comprehensive Cryptographic library
- Secure Boot library
- Secure Storage library
- Digital Certificate library
- Hardware enablement for SafeXcel Trusted/Crypto Module
- Easy adaptation to target hardware and software environment

SafeXcel IP – SafeZone Secure Platform

is available as a complete, tested and ready-to-deploy package. The following are the SafeZone Secure Platform deliverables.

SafeXcel-IP-123 Crypto Module (EIP-123)

The SafeXcel-IP-123 Crypto Module (EIP-123) is a Hardware IP design. The core of this package is the Verilog source tree of the design. In addition to this source code data base, the package comprises of supporting files as a testbench for verification, synthesis scripts and extensive documentation.

SafeXcel-IP-150 Public Key Accelerator (EIP-150)

The SafeXcel-IP-150 Public Key Accelerator (EIP-150) is a Hardware IP design. The core of this package is the Verilog source tree of the design. In addition to this source code data base, the package comprises of supporting files as a testbench for verification, synthesis scripts and extensive documentation.

SafeZone Secure Platform Middleware

The SafeZone Secure Platform Middleware is packaged as an SDK and supports the EIP-123 and EIP-150 packages. The SafeZone SDK comprises of several components.

SafeZone Secure Boot toolkit

The SafeZone Secure Boot solution provides the toolkit to build Secure Boot solutions.

Gatecount and Performance

The Secure Platform gate count values listed below are NAND equivalents and indicative for generic cell libraries:

EIP-123 Max frequency

- 550 MHz –TSMC 40nm technology
- 375 MHz –TSMC 65nm technology
- 300 MHz –TSMC 90nm technology

EIP-123 Symmetric Crypto Performance @ 200MHz

- 261 Mbps 3DES (168-bit key)
- 1280 Mbps C2 (56-bit key)
- 752 Mbps Multi2 (64-bit key, 32-rounds)
- 492 Mbps AES (128-bit key)
- 1280 Mbps Camellia (128-bit key)

EIP-123 Hash Performance @ 200MHz

- 1575 Mbps MD5
- 1264 Mbps SHA-1
- 1575 Mbps SHA-256

EIP-123 Gate count (TSMC 90nm)

- 135k - 210k gates depending on options

EIP-150b Max frequency

- 600 MHz –TSMC 40nm technology
- 460 MHz –TSMC 65nm technology
- 350 MHz –TSMC 90nm technology

EIP-150b Performance @ 400MHz

- 160 bit DSA: 1900 signs/s
- 180 bit DH: 569 key negotiations/s
- 512 bit RSA: 579 signs/s
- 1024 bit RSA: 98 signs/s
- 2048 bit RSA: 13.6 signs/s
- 4096 bit RSA: 1.86 signs/s

EIP-150b Gate count (TSMC 90nm)

- 27k gates

Security Applications

- M-commerce or Mobile Payments
- Point of Sale
- Digital Rights Management
- Handset data encryption
- Secure Boot
- Secure FOTA
- Secure Device Management
- Secure Storage
- IMEI & SIMLock protection

Benefits

- Complete embedded security solution
- Enables multiple content protection schemes
- Secure Key Management
- Support for hardware-based security
- Maximum application performance
- Small footprint for efficient implementation
- Seamless platform portability
- Fast time to market
- Lower total cost of ownership
- Support for broad range of processors and operating systems
- Minimized deployment risk
- World-class support
- Proven technology
- Trusted Execution Environment for robust security
- Extended battery life
- Protection against side channel attacks

Features

- Asset Store
 - Trusted environment for storing and using assets in a secure way
- Standard Cryptographic Accelerators
 - Public Key Algorithms
 - RSA DSA Diffie-Hellman
 - True Random Number Generation (Entropy based)
 - Enc/Dec: AES, DES, 3DES, ARC4
 - Hash/HMAC: MD5, SHA-1 and SHA2
- Non-Volatile Memory Interface
- Hardware CRC-32 module to perform basic integrity checks on data objects in the internal Data RAM and the NVM
- Embedded Secure DMA controller for high speed symmetric crypto and hash data transfer
- Key Exchange Mechanisms
 - RSAES-KEM
 - AES-WRAP
- Host Interface
 - AXI or AHB interface
 - Streaming interface with embedded FIFO's and DMA support
 - A mailbox forms the SafeZone security barrier that passes commands, status and regular data, but shields sensitive embedded data like keys
- Embedded Storage
 - Mailbox
 - Rootkey storage
 - Volatile key storage
 - Non-volatile key storage
 - Input and output FIFOs in the streaming interface

All of the recommended IP and middleware is available today, silicon proven and provides a solution where all SafeZone software is fully integrated with the SafeXcel hardware. In addition AuthenTec's DRM and IPsec solutions can be added as security applications to run on top of the SafeZone Secure Platform. FPGA prototype and customization services for non-standard products can be provided.

For more information about AuthenTec's Embedded Security Solutions: embedded@authentec.com.