StealthKey

Key Management Engine With an SP 800-90 Random Bit Generator

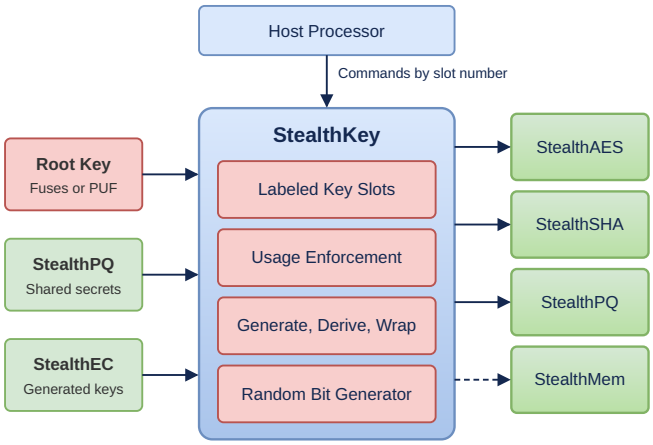
Hardware key management for every cryptographic core in your system. Keys are generated, derived and wrapped inside the core, and software manages them by slot number without ever reading them.

Up to 258,000/s	32	SP 800-90A
256-Bit Key Derivations	Labeled Key Slots	DRBG With SP 800-90B Health Tests

All major FPGAs and ASICs. **AMD** Versal, UltraScale+, UltraScale and 7 Series · **Microchip** PolarFire, PolarFire SoC, SmartFusion 2 and IGLOO2 · **Altera** Agilex, Arria 10, Stratix 10 and Cyclone 10 · RTL optimized for ASIC implementation

Key Features

- **Secure Key Storage**
Labeled key slots that no bus can read
- **On-Chip Key Generation**
AES-256 DRBG with an on-chip entropy source
- **Key Derivation**
SP 800-108, SP 800-56C and HKDF functions
- **Key Wrapping**
AES key wrap that protects each key and its label
- **Direct Key Delivery**
Dedicated key ports into your cryptographic cores
- **Usage Enforcement**
The label of each key limits how it can be used
- **Configurable Alarm Response**
Each alarm input can erase all keys or report only
- **Designed for FIPS 140-3 Modules**
Self-tests, a life cycle and zeroization
- **Simple Integration**
AXI4-Lite host interface with interrupt
- **NIST ACVTS Ready**
ACVP harness and validation support as an option



Applications

Encryption Keys
- Encrypted flash
- Device-bound firmware
- Device-bound AI models
- Sealed key storage

Post-Quantum Systems
- ML-KEM shared secrets
- Session key derivation
- Key seed delivery
- Key hierarchies

Device Identity
- Secure provisioning
- Root keys from a PUF
- Root keys from fuses
- Signing key generation

Message Authentication
- HMAC and CMAC tags
- Boot measurements
- Protocol messages
- FIPS 140-3 modules

StealthKey Product Overview

Technical Specifications

Random Bits	CTR_DRBG with AES-256 (SP 800-90A), with an on-chip entropy source and SP 800-90B health tests
Key Derivation	SP 800-108 counter and feedback modes, HKDF, and SP 800-56C one-step and two-step derivation
Key Wrap	KW and KWP (SP 800-38F)
MAC and Hash	CMAC, HMAC-SHA-2, and SHA-256, SHA-384 and SHA-512
Key Storage	32 labeled key slots of up to 64 bytes, configurable from 4 to 256
Interfaces	AXI4-Lite host interface, with key, import, seed and alarm ports
Software	StealthAPI library and Linux driver
Deliverables	Verilog or VHDL RTL, test suite with NIST ACVP vectors, C header and documentation

Countermeasure Configuration

The countermeasure configuration masks every key from end to end and runs AES on the masked StealthAES engine. StealthAES's countermeasures are tested beyond 1 billion traces with TVLA. This configuration offers the AES-based algorithms, which are CMAC, key wrap, the CMAC-based key derivations and the random bit generator.

Area and Performance

	AMD Versal AI Edge	Microchip PolarFire SoC	Altera Agilex 5
All Algorithms			
Maximum Frequency	210 MHz	120 MHz	145 MHz
Logic	22122 LUT6	43784 4LUT	15985 ALM
Flip-Flops	18216	19692	25217
Block RAM	21 RAMB36	40 LSRAM	40 M20K
Without SHA-2 and HMAC			
Maximum Frequency	210 MHz	120 MHz	140 MHz
Logic	16695 LUT6	31797 4LUT	10969 ALM
Flip-Flops	12991	14528	18646
Block RAM	21 RAMB36	40 LSRAM	40 M20K
Countermeasure Configuration			
Maximum Frequency	195 MHz	105 MHz	145 MHz
Logic	28860 LUT6	57441 4LUT	19550 ALM
Flip-Flops	26506	28372	29571
Block RAM	30 RAMB36	58 LSRAM	54 M20K

Post-place-and-route results for the core alone on a mid-range device of each family; results vary with device, tools and design.

At 210 MHz, the core completes up to 196,000 key wraps, 203,000 key unwraps and 258,000 256-bit key derivations per second. Rates scale with the clock frequency of each family.

Ready to Protect Your Keys in Hardware?

info@stealthcores.com | www.stealthcores.com | © 2026 StealthCores

Rev. 2026.1.0