StealthEC

ECDSA and ECDH Elliptic-Curve Cryptography Engine

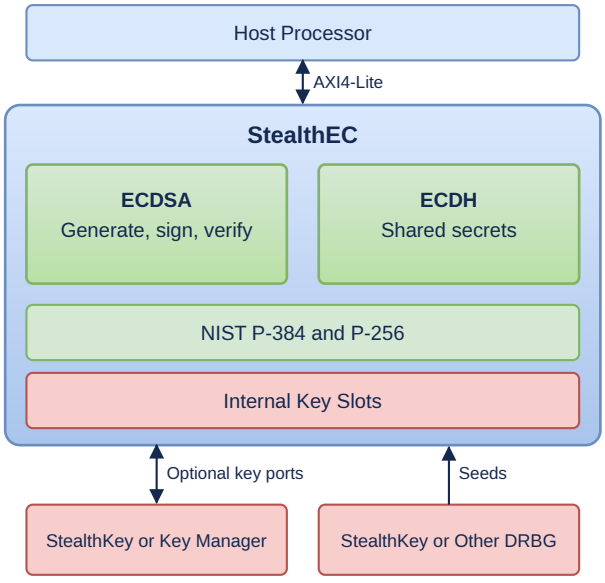
Full offload of ECDSA and ECDH on the NIST P-384 and P-256 curves in a compact design. Private keys remain in secure internal key slots behind a simple AXI4-Lite interface.

545	1430 LUT6	FIPS 186-5
P-384 Signatures per Second	Complete Standalone Core	ECDSA With SP 800-56A ECDH

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

- **Full ECDSA Offload**
Key generation, signing, and verification
- **ECDH Key Agreement**
Shared secrets with public-key validation
- **NIST P-384 and P-256**
Curve selected for each operation
- **Secure Key Storage**
Private keys held in internal key slots
- **Software Support**
Bare-metal and Linux, OpenSSL and wolfSSL
- **Compact Design**
Low logic count on every FPGA family
- **Simple Integration**
AXI4-Lite host interface with interrupt
- **Fault Detection**
Point results verified before any output
- **Zeroization**
Keys and working data cleared on command
- **Countermeasure Option**
Masked key storage and lockout on a fault



Applications

Secure Boot
- Image authentication
- Firmware updates
- Root of trust
- Code signing

Secure Networking
- TLS 1.3
- IPsec IKEv2
- MACsec key agreement
- Secure channels

Device Identity
- Device attestation
- Public-key infrastructure
- Secure provisioning
- Hardware security modules

Post-Quantum Migration
- Hybrid key exchange
- Classical and ML-KEM
- CNSA 1.0 systems
- Long-lived deployments

StealthEC Product Overview

Technical Specifications

Signatures	ECDSA key generation, signing, and verification (FIPS 186-5)
Key Agreement	ECDH shared-secret computation with public-key validation (SP 800-56A)
Curves	NIST P-384 and P-256 (SP 800-186)
Public Keys	Full validation, with compressed public keys supported in hardware
Key Storage	Up to 16 internal key slots
Interfaces	AXI4-Lite host interface, with optional key ports for StealthKey

Area and Performance

Complete Standalone Core	AMD Versal AI Edge	Microchip PolarFire SoC	Altera Agilex 5
Maximum Frequency	435 MHz	190 MHz	220 MHz
Logic	1430 LUT6	3959 4LUT	1321 ALM
DSP Blocks	28	38	26
P-384 operations per second			
Sign	545	189	284
Verify	531	185	277
Shared Secret	622	218	324
P-256 operations per second			
Sign	884	310	454
Verify	860	303	441
Shared Secret	1,000	355	513
Countermeasure configuration			
Maximum Frequency	405 MHz	185 MHz	225 MHz
Logic	1485 LUT6	4108 4LUT	1394 ALM
P-384 Sign, per second	344	125	197
P-384 Verify, per second	494	180	283
P-384 Shared Secret, per second	377	138	215

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

Why Choose StealthCores?

Expert Support
Decades of cryptographic implementation experience with dedicated integration support and comprehensive documentation.

Optimal Performance
A compact design that delivers fast elliptic-curve operations on every major FPGA family.

Flexible Integration
A complete standalone core, with optional key ports for StealthKey and a configuration for P-384 alone.

Standards Compliance
NIST standards verified implementation ensuring reliable and trusted security for commercial and defense applications.

Ready to Secure Your Systems?

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

Rev. 2026.1.0