Immunity HSM

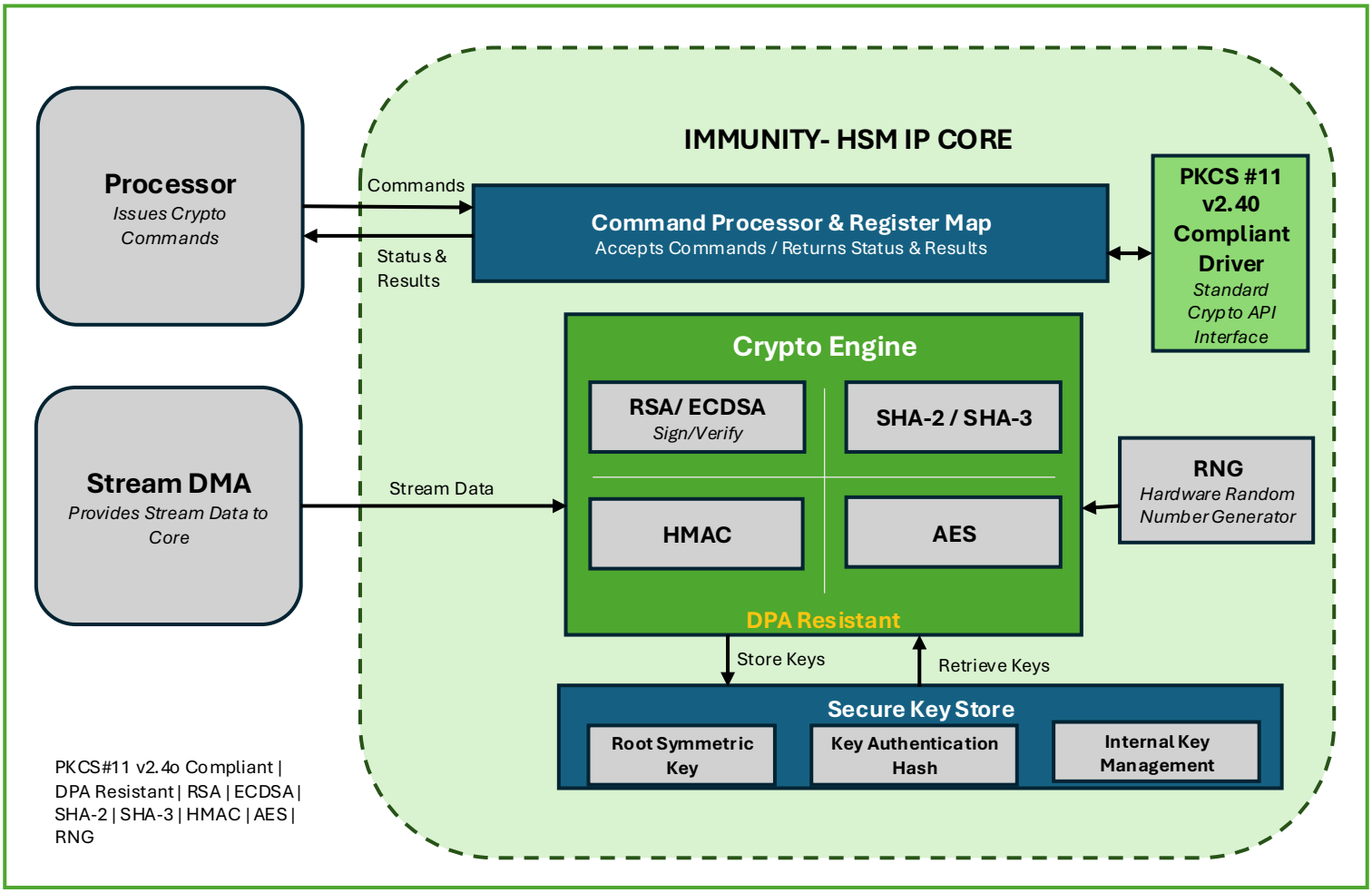
Hardware Security Module IP Core

Overview

Key management is a headache. The Immunity™-HSM IP Core is a hardware security module that provides crypto processing and key management for embedded defense solutions. Immunity-HSM safeguards and manages digital keys, enabling strong authentication and cryptographic operations without exposing sensitive key material.

The IP Core accepts commands from the processor for supported cryptographic functions. Stream data is provided via a Stream DMA or similar device. The core returns status and results to the processor via its core register map, delivering a clean and secure hardware-software interface for cryptographic operations.

Immunity-HSM consolidates a wide suite of DPA-resistant cryptographic functions- including asymmetric signing, hashing, MAC generation, random number generation, and symmetric encryption- into a single, manageable IP core.



Contact Idaho Scientific for more information

info@idahoscientific.com | www.idahoscientific.com

GENERAL DYNAMICS
Mission Systems

IDAHO SCIENTIFIC

Benefits

Benefit	Description
Low Risk	Used in FPGAs on Defense Programs. NIST-approved with proven side channel resistance.
Simple to Integrate	Drag-and-drop design delivered with reference designs and test benches using common interface IP.
Set and Forget	No annual maintenance contracts. Implementation of future updates is optional.
Trusted US DoW Supplier	Developed and supported by cleared US engineers who answer emails, take phone calls, and can travel to ensure smooth integration.

Features

Feature	Detail
Standard Compliance	PKCS#11 v2.40 Compliant Driver
Key Management	Secure Key Store, Root Symmetric Key, Key Authentication HASH
RSA	Sign/Verify and OAEP Encrypt/ Decrypt, max 4096-bit key
ECDSA	Sign/Verify, NIST secpXXXr1 curves: 224, 256, 384, 521-bit
SHA-2	SHA 224, 256, 384, 512, 512/224, 512/256
SHA-3	SHA3 224, 256, 384, 512
HMAC	HMAC 224, 256, 384, 512, 512/224, 512/256
Random Number Generator	Hardware based RNG
AES	Encrypt/Decrypt for ECB, CTR, CBC, GCM modes; 128 and 256-bit key sizes
DPA Resistance	All cryptographic functions include DPA- resistant countermeasures

Deliverables

Xilinx IP_XACT Package	Product Documentation
Example Designs	Simulation Testbench
Technical Support	Maintenance Updates

✓ ***Comprehensive*** ✓ ***DPA Resistant*** ✓ ***Standard Compliant***

©2026 General Dynamics. All rights reserved. General Dynamics reserves the right to make changes in its products and specifications at anytime and without notice. All trademarks indicated as such herein are trademarks of General Dynamics. All other product and service names are the property of their respective owners. ®Reg. U.S. Pat. and Tim. Off.