GENERAL DYNAMICS Mission Systems | IDAHO SCIENTIFIC

Immunity

Security & Anti-Tamper Core Suite

The Challenge

Instructions and data stored at rest and in transit are vulnerable to attack, introspection, and modification. For defense-grade embedded systems, this is not an acceptable risk.

The Solution

Idaho Scientific's Immunity ™ Product Family is a suite of security and anti-tamper FPGA IP cores designed to help engineers protect embedded hardware and firmware across the full data lifecycle– from memory, to chip-to-chip links, to key management.

Immunity IP Cores encrypt, decrypt, and authenticate information to that it cannot be exposed to anyone but the intended user.

Crypto cores address use cases including:

- Key generation, Exchange & Storage
- Digital Signatures
- Bulk Encryption
- Packet Encryption
- Message Authentication

Why Choose Immunity?

Lower Technical Risk

Simple Integration, reference designs, and technical support from cleared US engineers who specialize in DoD systems security

Proven Performance

NIST certified, Government validated, and operating in Programs of Record

More Flexibility

Features configurable at compile and/or run-time to meet your exact requirements.

Learn More

Idaho Scientific's engineers are cleared US citizens. We answer emails, take phone calls, and travel on-site to ensure your integration succeeds. Get in touch:

info@idahoscientific.com
www.idahoscientific.com

Product	Function	Key Standard
Immunity AES	AES Encryption & Decryption IP Core	FIPS-197, SP800-38A/D
Immunity Chip2Chip	Authenticated Encryption for Xilinx Chip2Chip Links	FIPS 197, SP 800-38D
Immunity IME	Inline Memory Encryption & Authentication	FIPS-197, SP 800-38A/D
Immunity HSM	Hardware Security Module- Crypto Processing & Key Management	PKCS#11 v2.40, FIPS-197

Side Channel Countermeasures

Immunity products ***are available with or without side channel countermeasures*** for protection against Simple Power Analysis (SPA), Differential Power Analysis (DPA), and other SCA techniques

Side channel countermeasure technology is licensed from Cryptography Research Incorporated (CRI), a division of Rambus. Customers receive a sub-license for use and distribution within their products.

PRI-2605-0001