BootProtect

Post-Quantum-Resistant, Owner-Controlled Secure Boot for Fielded FPGAs

Rickert-Areno Engineering, LLC · in partnership with IC-Safety

BootProtect establishes post-quantum (PQ)-resistant, owner-controlled secure boot on commodity FPGAs that are already fielded — with no hardware modification. It pairs Rickert-Areno Engineering's patent-pending **Errantry** secure-boot datapath with IC-Safety's **SiRF physically unclonable function (PUF)**. The result is a fabric-portable capability that lets an installed base of environmentally-qualified, platform-certified hardware meet PQ requirements through reconfiguration alone — years ahead of any silicon refresh, and without the cost or recertification of replacement.

THE PROBLEM

Today's hardware roots of trust are manufacturer-anchored: trust derives from an immutable, vendor-controlled secret — a fused eFuse key, mask ROM, or provisioned PUF helper data — so the customer inherits trust rather than owning it, and that anchor is almost always built on classical cryptography. On fielded FPGAs, the post-quantum-vulnerable asymmetric algorithms (RSA/ECC) that gate secure boot are implemented in hard logic that cannot be replaced through configuration. CNSA 2.0 directs National Security Systems toward PQ-secure algorithms on a 2030–2035 timeline; the only conventional route to compliance on these platforms is silicon replacement — a multi-year effort gated by vendor roadmaps, with recertification cost for hardware that is otherwise perfectly serviceable.

HOW BOOTPROTECT WORKS

BootProtect inverts the trust model. Rather than storing a secret, it re-creates the bitstream decryption key from a design-integrity-conditioned pool of random bits, so there is nothing for an attacker to extract. Because it uses no asymmetric cryptography, it is PQ-resistant by construction — while reproducing the central benefit of asymmetric secure boot: only owner-authorized code runs.

- **Provisioning.** Compatible PUF challenge vectors are combined with SHA2-384/512 hashes of the encrypted bitstream and a self-measurement of the BootProtect bitstream itself, then stored in NVM — binding trust to the owner's design.
- **Enrollment.** The stored value drives the PUF; its response feeds an HKDF (keyed by the bitstream hash, salted by the self-measurement) to produce a 2048-bit pool of random bits (PoRB). The owner's key is XOR-split against the PoRB into a NIST SP 800-152 key split and stored — supporting multiple keys and in-field re-keying.
- **Run-time.** The key is regenerated from the PoRB and used to authenticate and decrypt the original design. Any modification to the protected design changes the PoRB and prevents key re-creation, so unauthorized code cannot complete boot.
- **Teardown.** Once the original design is validated, dynamic partial reconfiguration (DPR) overwrites BootProtect's own region and loads that design — so its steady-state fabric cost approaches zero, and native secure-boot mechanisms remain in place beneath it.

WHY IT IS DIFFERENT

Four classes of solutions exist today, and each leaves a different gap on already-deployed FPGAs. BootProtect sits orthogonal to all of them — the only known solution combining PQ-resistant secure boot with an owner-controlled hardware root of trust on existing FPGAs. Matching it would require an incumbent root-of-trust vendor to surrender the manufacturer-controlled trust anchor its business is built on: a business-model change, not a product update.

Approach	Representative offerings	Gap on already-deployed FPGAs
FPGA-vendor native security	Microchip, AMD/Xilinx, Altera	Classical crypto on the boot chain; PQ roadmaps unannounced or research-only; locked to one vendor's silicon
PQC IP cores	PQShield, Xiphera, PQSecure, Secure-IC	Drop-in ML-KEM / ML-DSA accelerators, but require new silicon; no retrofit path for deployed parts
Hardware RoT / PUF IP	Rambus, Intrinsic ID, PUFsecurity	Trust anchored in manufacturer-provisioned helper data; mostly classical KDF; ASIC-targeted
PQ secure-boot software	wolfBoot, NXP EdgeLock, Crypto4A	PQ algorithms in firmware, but no hardware-anchored root of trust for FPGA platforms
BootProtect	Rickert-Areno Engineering + IC-Safety	Hardware-anchored, owner-controlled, PQ-resistant, and retrofittable on existing FPGAs — across vendors

KEY CAPABILITIES

- **Retrofit, not replace:** deployed on existing FPGAs today, avoiding hardware replacement and recertification while meeting the CNSA 2.0 PQ transition ahead of schedule.
- **Vendor-independent:** a portable VHDL datapath spans Microchip, AMD/Xilinx, and Altera rather than locking to one silicon line.
- **Crypto-agile in the field:** multiple keys can be enrolled, replaced, or rolled after deployment — for example before third-party work or for routine security hygiene — keeping devices fielded far longer.
- **Tamper-evident by design:** integrity conditioning ties the key to the design, so any change to the bitstream breaks key re-creation and blocks boot.
- **Side-channel hardened:** a custom AES engine draws on the PUF as a TRNG to mask emissions; a customizable configuration-lock mechanism governs enrollment.
- **Independently validated primitive:** the SiRF PUF — the hardest-to-port element — is assessed by Sandia National Laboratories on all three target fabrics.

TECHNICAL SPECIFICATIONS

Cryptography	Symmetric 256-bit AES + SHA2-384 / SHA2-512 hashing; no asymmetric primitives — PQ-resistant by construction
Root of trust	Owner-controlled; key regenerated from a design-integrity-conditioned pool of random bits (PoRB), never stored
Key management	NIST SP 800-152 §6.7.5 key split; multiple enrolled keys with in-field re-keying and crypto-agility
FPGA support	Microchip PolarFire (demonstrated); AMD/Xilinx and Altera (portable VHDL datapath); potential Lattice
Deployment	Injected as a bitstream into the existing secure-boot sequence; vacates the fabric via dynamic partial reconfiguration (DPR)
Steady-state footprint	Approaches zero after DPR teardown; estimated ~25–30K 4-input LUTs for the core datapath
Boot-to-handoff	Estimated ~50–60 ms for the core (181 ms in the full RISC-V demonstration build)
Independent validation	SiRF PUF assessed by Sandia National Laboratories across all three target fabrics; thermal and aging tested

Compliance	CMMC Level 2 (self); ITAR / EAR handling; U.S.-owned, woman-owned small business, all work performed in the U.S.

DEPLOYMENT & USE CASES

BootProtect ships as licensable, deployable security IP — a fabric-portable bitstream and provisioning toolchain — with depot and in-field provisioning available as a service. The primary DoD transition target is retrofit of fielded FPGA-based systems whose native secure boot is classical-crypto hard logic, bringing them into PQ-resistance compliance through reconfiguration; Rickert-Areno Engineering is working with the Midwest ME-Commons Consortium (MMEC) to identify adopting technology-refresh programs. The same IP serves critical-infrastructure and supply-chain operators with long-lived FPGA hardware and enables a distinctive “blank-slate” use in which ITAR-restricted designs run securely on commercial systems. The core datapath is also positioned for integration into future ASIC and chiplet root-of-trust blocks.

ABOUT & CONTACT

Rickert-Areno Engineering, LLC is a U.S.-owned, woman-owned small business delivering secure product architectures and licensable hardware-root-of-trust IP to the U.S. Government, the Defense Industrial Base, and critical-infrastructure operators. Errantry and the SiRF PUF were developed independently and self-funded by their respective companies; **IC-Safety** holds exclusive license to the SiRF PUF and is an industry-recognized authority in PUF technology.

Dr. Matthew Areno, Chief Technology Officer · matt@rickertarenoengineering.com · (737) 406-6197
Dr. Jim Plusquellic, CEO, IC-Safety · jimplus@ic-safety.com · (240) 475-1882