

Mithril

HAIR-Compliant Boot-Flash Root of Trust — Transparent, Attestation-Bound Encryption for Fielded Platforms

Rickert-Areno Engineering, LLC



Mithril is a HAIR-compliant hardware root of trust (HrOT) that protects a platform’s SPI boot flash — the code a system runs before any software defense exists. The boot image is held encrypted at rest in the flash device; Mithril sits inline on the SPI bus, decrypts it on-the-fly, and re-encrypts the data returned to the host under keys bound to a live platform attestation. It requires no change to the host, the flash device, or the boot software, and stores no static secret. Mithril has been demonstrated inline on an Intel Ice Lake-D platform, which completes bootstrap discovery and loads its boot image through the FPGA. To our knowledge, Mithril is the only HAIR-compliant HrOT solution in existence.

The Problem

A platform’s earliest boot code lives in an external SPI NOR flash that sits outside the host’s security perimeter, where its contents can be read, copied, or altered with inexpensive bus-level tools — exposing proprietary firmware and opening a pre-boot attack surface that host-resident defenses cannot cover, because they have not yet begun to run. Native boot protections are fixed in host silicon: their algorithms, key ownership, and trust anchors cannot be changed after the part ships, and they leave the flash image unprotected on the medium and on the wire. Operators of long-lived, already-fielded systems need confidentiality, integrity, and attestation-bound control over their boot flash without redesigning the platform or replacing silicon.

How It Works

Mithril sits transparently on the SPI path between the host and its boot flash.

- **Boot discovery.** Mithril answers the host’s SFDP descriptor read directly from FPGA fabric, so the platform completes flash discovery at its hardwired bootstrap rate regardless of the flash device’s addressing mode.
- **Attestation.** On power-up, an embedded root of trust performs a mutual platform attestation with the host using the industry-standard SPDm 1.3 protocol before any protected data is served.
- **Key derivation.** Generates key and IV pairs for encryption of SPI transactions using native RNG.
- **At-rest decryption.** The boot image is stored encrypted at rest in the flash device. Mithril decrypts it on-the-fly with AES-256-GCM, generating the keystream ahead of each access so the host is never stalled.
- **In-transit protection.** The data returned to the host is re-encrypted under the session keys and authenticated per transfer with a unique IV.

Why It Is Unique

Mithril is the only HAIR-compliant hardware root of trust combining properties no single fielded solution offers together: keys bound to a live attestation, re-created at run time and never stored; transparent inline protection of the boot flash both at rest and in transit, with no change to the host or its boot software; and delivery as portable FPGA logic that drops onto hardware already in service. Mithril requires no external DDR memory and is instantiated purely in reconfigurable fabric.

Approach

Boot-flash protection is addressed today by several classes of product. None of them combines attestation-bound keys, protection of the image both at rest and in transit, and insertion into a platform that has already shipped.

Approach	Representative offerings	Gap for boot-flash protection
Host-native boot protection	Intel Boot Guard, AMD PSB	Fixed in host silicon — algorithm, key ownership and trust anchor cannot be changed after the part ships; the flash image is left unprotected on the medium and on the wire
FPGA-vendor secure boot	Microchip, AMD/Xilinx, Altera	Protects the FPGA’s own configuration, not the host’s boot flash; nothing sits inline on the host SPI path and the host is not attested

Encrypted SPI flash devices	Winbond, Macronix, Infineon	Requires replacing the flash device, which is not an option on fielded hardware; the key lives in the flash and is not bound to a live platform attestation
Hardware RoT / PUF IP	Rambus, Intrinsic ID, PUFsecurity	Supplies device identity and key storage, not an inline boot-flash datapath; the boot image remains readable at rest on a commodity flash
Discrete TPM	Infineon, Nuvoton, STMicroelectronics	Measures and attests, but sits outside the SPI datapath and cannot keep the boot image confidential or serve it encrypted
Mithril	Rickert-Areno Engineering	Attestation-bound keys derived at run time and never stored; AES-256-GCM confidentiality and integrity both at rest and in transit; transparent inline insertion with no change to the host, the flash device or the boot software

Key Capabilities

- **Transparent, inline insertion:** no changes to the host processor, the boot flash, or the boot software; non-encrypted traffic passes through unmodified.
- **Attestation-bound keys:** SPDMM 1.3 mutual attestation gates every session; keys are derived live and never stored, so there is no static secret to recover.
- **Confidentiality and integrity, at rest and in transit:** authenticated AES-256-GCM protects the boot image on the medium and re-protects it on the wire.
- **Crypto-agile in the field:** multiple independent key domains and in-field re-keying keep platforms serviceable across long lifecycles.
- **Vendor-portable:** implemented on Microchip and Lattice FPGAs today, with AMD/Xilinx and Altera ports underway.
- **Post-quantum upgrade path:** the root of trust can be made post-quantum-resistant with the BootProtect secure-boot datapath (see the BootProtect Product Brief).

Technical Specifications

Cryptography	AES-256-GCM (NIST SP 800-38D): no asymmetric primitives on the data path. The engine is a standards-conformant reference, replaceable with a customer-supplied or side-channel-hardened engine.
Platform attestation	SPDMM 1.3 mutual attestation (DMTF) gates every session; the host is attested before any protected data is served.
Key management	256-bit session keys derived at run time from the attested key schedule, held in write-only, non-readable registers, and never stored in non-volatile memory. In-field re-keying; session material zeroized after use.
At-rest protection	The boot image stored encrypted at rest and decrypted on-the-fly with AES-256-GCM; keystream generation runs ahead of each access so the host is never stalled.
In-transit protection	Data returned to the host is re-encrypted and authenticated per transfer. Regions are served encrypted as defined by the Intel platform specification.
Host integration	Transparent inline insertion on the SPI NOR path; no modification to the host processor, the flash device, or the boot software. The host sees a standard SPI flash.
FPGA support	Microchip PolarFire and Lattice implemented; AMD/Xilinx and Altera ports underway. Portable HDL datapath — not locked to one silicon line.
Post-quantum option	Upgradeable to post-quantum-resistant secure boot with Rickert-Areno Engineering's Errantry solution (see the BootProtect Product Brief).

Platform Validation

Mithril has been demonstrated inline between an Intel Ice Lake-D host and its boot flash on a Microchip PolarFire MPF300T. With Mithril in the SPI path, the host completes bootstrap discovery — its SFDP descriptor served directly from FPGA fabric — and goes on to load a 6.41 MB boot image in 105,143 sequential fast reads using

four-byte addressing, captured end to end on Rickert-Areno Engineering's own bit-accurate SPI instrument. Transparent inline insertion is therefore established on hardware rather than inferred. The encrypted datapath is validated against known-answer tests whose ciphertext and authentication tags match independent golden vectors exactly; hardware bring-up of the encrypted path is in progress.

Deployment & Use Cases

Mithril ships as licensable, deployable security IP — portable FPGA logic together with the provisioning and attestation firmware — for insertion into the design of new or already-fielded platforms. The primary target is HAIR-compliant protection of host boot flash on long-lived systems: adding confidentiality, integrity, and attestation-bound key control to the pre-boot datapath without redesigning the platform or replacing silicon. Serves defense and critical-infrastructure operators who must keep proprietary or export-controlled boot firmware confidential. Where post-quantum resistance is required, the root of trust integrates with BootProtect.

Licensing

Mithril is offered under a one-time-fee, perpetual license granting unrestricted use and full source-code access.

- **One-time, perpetual license.** A single up-front fee conveys a perpetual, unrestricted-use license with full source-code access — no per-unit royalties or recurring fees.
- **Integrate and ship.** The licensee may use, modify, and embed Mithril within its own products and devices and sell those devices to its customers.
- **No resale as IP.** The license does not permit resale or redistribution of Mithril as a standalone product, or its incorporation into a hardware-root-of-trust IP offering that the licensee in turn licenses or sells to third parties.
- **Documentation under NDA.** The User's Manual and detailed architectural documentation are provided under a non-disclosure agreement.

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.

Dr. Matthew Arenó, Chief Technology Officer · matt@rickertarenoengineering.com · (737) 406-6197

Trevor Hird, Director of Engineering · trevor@rickertarenoengineering.com · (737) 406-5851