SECURITY & TRUST

Garmo-Secure-Boot

Security — post-quantum-ready root of trust and secure boot

IP-2084 · Evaluation package · Evaluation / IP scope

Function and architecture

- SHA-256/384/512 and SHA-3 streaming hash
- ECDSA P-384/Ed25519 adapter plus ML-DSA accelerator boundary for hybrid signatures
- Measured boot, DICE-style compound identity and attestation log

Integration summary

Garmo-Secure-Boot integration role: Security — post-quantum-ready root of trust and secure boot. Documented composition: SHA-256/384/512 and SHA-3 streaming hash; ECDSA P-384/Ed25519 adapter plus ML-DSA accelerator boundary for hybrid signatures; Measured boot, DICE-style compound identity and attestation log.

Technical record

Canonical identity	IP-2084
Responsibility	Security — post-quantum-ready root of trust and secure boot
Documented interface architecture	ROM/OTP/eFuse, flash/NVMe stream, crypto accelerator ports, lifecycle/debug, DICE/attestation output
Documented building blocks	SHA-256/384/512 and SHA-3 streaming hash; ECDSA P-384/Ed25519 adapter plus ML-DSA accelerator boundary for hybrid signatures; Measured boot, DICE-style compound identity and attestation log
Delivery boundary	Evaluation / IP scope
Evidence scope	Evaluation package
Architecture targets · not measurements	<10 ms verification target for typical 4 MiB first-stage image with streaming hash; measured boot and recovery.

Delivery and release binding

- Interface version and parameter set
- Clock/reset domains and integration constraints
- Companion memory, PHY and software requirements
- Verification collateral and acceptance criteria

Confirm for the selected release: Node/library binding, Clock/reset limits, Physical and protocol dependencies, Artifact hashes, Acceptance criteria.

Evidence and qualification

Canonical technology and its architecture/integration role are recorded. The offered delivery is confirmed against the exact release before licensing.

No node-port, silicon-performance, standards certification or analog qualification is inherited from a related product.

Canonical status: P0 / REPRESENTATIVE ARCHITECTURE RTL — concrete integration specification and synthesizable RTL shell/representative datapath only; all frequency, throughput, power, area, jitter and standards-superiority figures remain architecture targets until the required evidence hierarchy closes.

Evaluation and licensing

Evaluation: Evaluate an individual IP configuration. Production: Named-design production license. Custom work: Node binding or derivative integration. Rights, pricing, support and acceptance criteria are agreed for the exact scope.

Contact: patrick@garmolabs.com | Product path: /ip/garmo-secure-boot