INTRINSIC ID®

Product Brief: QuiddiKey HW RoT IP

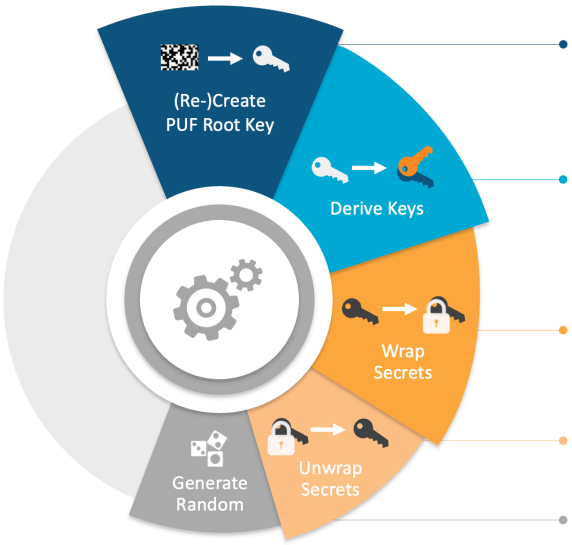
psacertified™
level three RoT component

QuiddiKey X00 Hardware Root-of-Trust IP

Intrinsic ID QuiddiKey enables device manufacturers and designers to secure their products with internally generated, device-unique cryptographic keys without the need for adding costly, security-dedicated silicon.

Intrinsic ID QuiddiKey® is a hardware IP solution that enables device manufacturers and designers to secure their products with internally generated, device-unique cryptographic keys without the need for adding costly, security-dedicated silicon. QuiddiKey uses the inherently random start-up values of SRAM as a physical unclonable function (PUF), which generates the entropy required for a strong hardware root of trust. QuiddiKey IP can be applied easily to almost any chip – from tiny microcontrollers (MCUs) to high-performance systems-on-chip (SoCs).

SRAM is a standard component available upon initial release of any process technology; because it uses SRAM as a PUF source, Quiddikey IP can be used with any foundry and process-node technology. Cryptographic algorithms in QuiddiKey are compliant to the relevant NIST standards and its security functionality has been certified with NIST CAVP and PSA Certified/SESIP evaluations. Furthermore, QuiddiKey has been deployed and proven in hundreds of millions of devices certified by EMVCo, Visa, CC EAL6+, PSA, ioXt, and governments across the globe.



Creates secure root key. Uses start-up values of SRAM to create a device-unique root key. Re-creates this root key each time it is accessed – the key is never stored

Derives wrapping keys to protect other functions. Provisions strong, independent, device-unique keys from the PUF root key to secure separate functions, making it easy for various players in the supply chain to add on security for their functions

Wraps secrets and adds authentication tags. Encrypts secret keys and data and adds authentication tags. Wrapped secrets are bound to the device and can be stored in unprotected NVM.

Checks tags and unwraps secrets. Verifies authentication tags for wrapped secrets and decrypts the content for use.

Generates Random Numbers: Uses the noise in the SRAM PUF as a NIST-compliant entropy source.

QuiddiKey Hardware IP

Applications

- Secure Key Storage
- Authentication
- Flexible Key Provisioning
- Anti-Counterfeiting
- IP Binding
- Supply Chain Protection
- Chiplet Security

Certifications

- PSA Certified Level 3 RoT Component
- SESIP Level 3
- NIST CAVP
- ISO/IEC 20897-compliant PUF
- Supports FIPS 140-3
- QuiddiKey enabled products have been certified by EMVCo, Visa, CC EAL6+, PSA, and ioXt
- DoD and EU governments qualified

Features

- Uses standard SRAM start-up values as a PUF to create a hardware root of trust
- Eliminates target for physical attacks: root key is never stored, but re-created from the PUF each time it is needed
- Supports fault detection and reporting
- Includes countermeasures against side-channel and fault-injection attacks
- Offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device
- Binds keys to the device by ensuring that keys can only be recreated and accessed on the device on which they have been created
- Eases integration with custom driver API

Benefits

- Certified as a RoT component (PSA)
- Offers a higher level of security than traditional key storage in NVM such as secure flash, OTP or e-fuses
- Enables designers to create and store an unlimited number of keys securely in unprotected NVM on/off chip
- Minimizes overhead through optimized hardware design
- Eliminates the need for centralized key management and programming
- Provides a highly reliable secure key storage solution in the most advanced process nodes
- Remains secure in the post-quantum computing era

QuiddiKey 100

The number of connected devices, machines or sensors that are linked with each other over open communication networks on the internet of things (IoT) has exploded. Processes are remotely monitored through networks of smart devices. And every device represents a potential entry point for malicious intrusion – into the device itself, or onto the network to which it's connected. These new security threats pose technology challenges in securing and stabilizing such large systems. In such an environment, root-of-trust (RoT) technology is becoming an essential requirement for every connected device.

QuiddiKey 100 is PUF-based RoT solution that can be applied easily to almost any chip – even the tiniest microcontrollers – without the need for adding costly, security-dedicated silicon. It is available in off-the-shelf configurations with size ranging between 39k and 64k gates.

QuiddiKey 100 can also be integrated as a trust anchor for other crypto libraries, extending the chain of trust beyond just a single device.

QuiddiKey 300

Digital trust is critical for the continued success of the IoT, so security, reliability, and privacy are top concerns. Developers and service providers tasked with demonstrating the security capability of their products are looking for guidance and standardized solutions. One important industry-led effort that can speed up the process and build confidence is PSA Certified.

QuiddiKey 300 is the world's first IP solution to be awarded "PSA Certified Level 3 RoT Component." This certifies that the IP includes substantial protection against both software and hardware attacks. It allows chip designers to fast-track their products for full PSA Level 3 certification and further helps ensure supply chain integrity, chiplet security, and protection against reverse engineering. Certification is essential for security-critical IoT market verticals, such as healthcare, critical infrastructures, and smart consumer products as outlined in the US Cyber Mark Program.

QuiddiKey 300 is available in off-the-shelf configurations with size ranging between 51k and 81k gates.

INTRINSIC ID

www.Intrinsic-ID.com | info@Intrinsic-ID.com

Benefits

- No sensitive key material present on device
- High protection against invasive attacks
- Deployed in hundreds of millions of production devices over more than a decade

Operational Range

QuiddiKey has been embedded on SoC/ASICs in a diverse set of foundry/process node combinations and SRAM PUF responses have been qualified for use with QuiddiKey in a wide range of operational environments.

- All major fabs from 0.35 µm to 5 nm
- Temperature range from -55°C to 150°C
- Voltage supply variation +/- 20%
- Lifetime > 25 years

Deliverables

- RTL netlist (VHDL, Verilog)
- Testbench (UVM, VHDL), C model
- Synopsys Design Compiler® synthesis constraints (tcl)
- QuiddiKey driver (C sources, headers)
- QuiddiKey register description (IP-XACT)
- Datasheet, integration manual and driver documentation
- NIST documentation (SP 800-90A/B)

QuiddiKey	100	300
Generate device keys and random values	✓	✓
Wrap and unwrap secrets	(✓)	(✓)
Size (k gates)	39-64	51-81
AC size (bytes)	1000	580 / 852
Security strength (bits)	256	256
Maximum key length (bits)	4096	4096
Time to root key (k cycles)	49-68	45-69
SRAM required for PUF (kB)	2-4	4-6
Interface	APB	APB or TileLink-UL
Masked key output		✓
Logic BIST	(✓)	(✓)
SRAM health checks	✓	✓
SRAM anti-aging	✓	✓
PUF monitoring	✓	✓
Tamper-evident: supports fault detection and reporting		✓
Countermeasures against side-channel and fault-injection attacks	✓	✓
NIST CAVP certification (DRBG, AES, KDF)	(✓)	(✓)
NIST SP 800-90 compliant	(✓)	(✓)
PSA Certified Level 3 RoT Component		✓

(✓) Features are optional

INTRINSIC ID

www.Intrinsic-ID.com | info@Intrinsic-ID.com