300

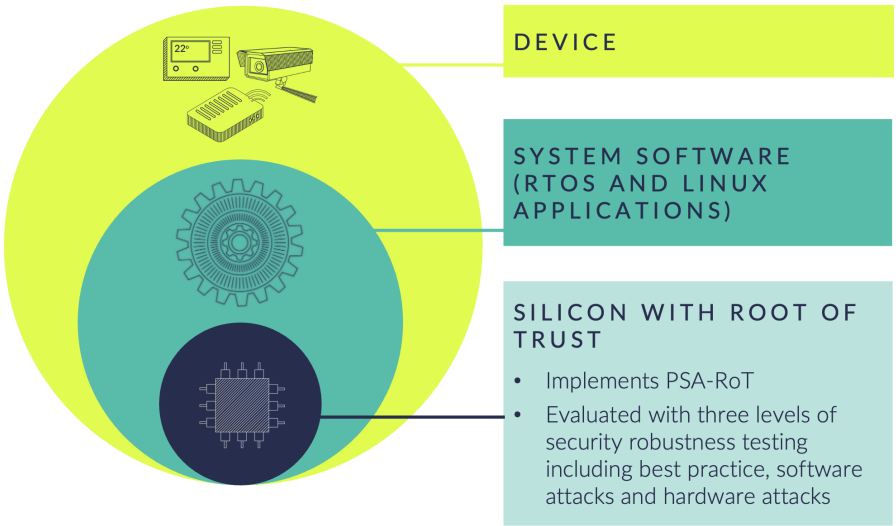
psacertified™
level three RoT component

QuiddiKey 300 Hardware RoT IP

QuiddiKey 300 is the world's first IP solution to be awarded "PSA Certified Level 3 RoT Component."

Digital trust is critical for the continued success of the IoT, so security, reliability, and privacy are top concerns. New legislations are driving improved security practices as well as an increased sense of urgency. 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, a physical unclonable function or PUF-based root-of-trust (RoT) security solution, 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 Hardware IP

Applications

- Secure Key Storage
- Authentication
- Flexible Key Provisioning
- Anti-Counterfeiting
- Anti-Reverse Engineering
- 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

SRAM PUF Benefits

- No sensitive key material present on device
- High protection against invasive attacks
- Deployed in over 500 million production devices over more than a decade

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
- 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

QuiddiKey 300	v1.0
Generate device keys and random values	✓
Wrap and unwrap secrets	(✓)
Size (k gates)	51-81
AC size (bytes)	580 / 852
Security strength (bits)	256
Maximum key length (bits)	4096
Time to root key (k cycles)	45-69
SRAM required for PUF (kB)	4-6
Interface	APB or TileLink-UL
Masked key output	✓
Logic BIST	(✓)
SRAM health checks	✓
SRAM anti-aging	✓
PUF monitoring	✓
Fault detection and reporting	✓
Attack countermeasures	✓
NIST CAVP certification (DRBG, AES, KDF)	(✓)
NIST SP 800-90 compliant	(✓)

(✓) Features are optional

Benefits

- Certified as an 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
- 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 post quantum computing

QuiddiKey Configurations

QuiddiKey 300 is available in off-the-shelf configurations with size ranging between 51k and 81k gates. Configurations differ according to functionality, performance and compliance, enabling options customized to the needs of your application.

Operational Range

QuiddiKey has been embedded on SoC/ASICs in a diverse set of foundry/process node combinations. 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)

INTRINSIC ID

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