INTRINSIC ID®

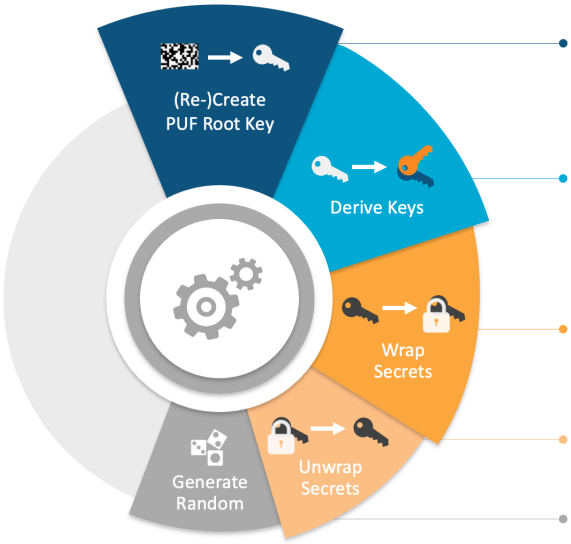
Product Brief: QuiddiKey HW RoT IP

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 (RoT). The QuiddiKey IP is agnostic to foundry and process node and has been protecting millions of ASIC/SoC/MCU and FPGA-based devices for more than a decade with no known breach or failure. QuiddiKey has been proven in devices certified by EMVCo, Visa, CC EAL6+, PSA, ioXt, and governments across the globe.

The QuiddiKey X00 RoT IP family serves various markets such as IoT, datacenter/HPC, and automotive. QuiddiKey 100 can be applied easily to almost any chip – even the tiniest microcontrollers. QuiddiKey 300 is the world's first RoT IP to receive a SESIP and PSA Certified Level 3 certification. QuiddiKey 400, tailored to the automotive industry, has been developed following an ISO 26262 functional-safety-compliant flow, and meets the ISO 26262 Automotive Safety Integrity Level (ASIL) B fault metric.



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.

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
- Meets ISO 26262 ASIL B fault metric
- ASIL D for systematics failures
- 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, SESIP)
- Integrates easily and scales with all fabs and technology nodes
- 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.

psacertified™
level three RoT component

SESIP™

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

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

essential for security-critical IoT market verticals, such as healthcare, critical infrastructures, and smart consumer products as outlined in the US Cyber Mark Program.

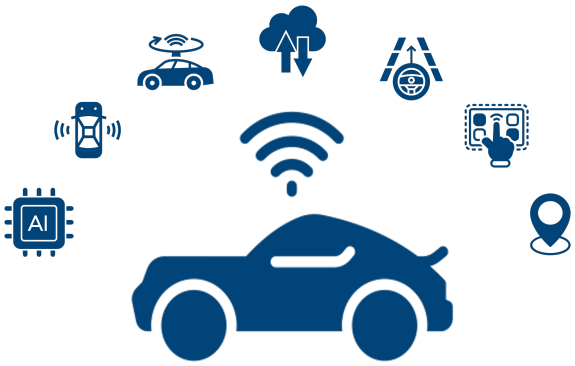
QuiddiKey 300 is available in off-the-shelf configurations with size ranging between 51k and 81k gates.

QuiddiKey 400

Anything that is connected to the internet is at risk, and connected vehicles are no exception. Every connected electronic component represents a potential entry point for malicious intrusion – into the component itself, or onto the network to which it is connected. RoT technology is becoming an essential requirement for components in autonomous vehicles which now need to adhere to the industry standard ISO/SAE 21434 to ensure the vehicle fleet is secure by design.

QuiddiKey 400 has been developed following an ISO 26262 functional-safety-compliant flow, and meets the ISO 26262 Automotive Safety Integrity Level (ASIL) B fault metric. Just like QuiddiKey 300, QuiddiKey 400 includes substantial protection against both software and hardware attacks to deny adversaries access to any key material or data, even on unmanned autonomous vehicles.

QuiddiKey 400 is available in off-the-shelf configurations with size ranging between 115k and 165k gates.



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)
- ISO 26262 documentation (ASIL B/D metrics)

Markets

- Internet of things
- Secure transactions
- Datacenter/HPC
- Automotive
- Aerospace & defense

QuiddiKey	100	300	400
Generate device keys and random values	✓	✓	✓
Wrap and unwrap secrets	(✓)	(✓)	(✓)
Size (k gates)	39-64	51-81	115-165
AC size (bytes)	1000	580 / 852	788
Security strength (bits)	256	256	256
Maximum key length (bits)	4096	4096	4096
Time to root key (k cycles)	49-68	45-69	77-95
SRAM required for PUF (kB)	2-4	4-6	16
Interface	APB	APB or TileLink-UL	APB or TileLink-UL
Masked key output		✓	✓
Logic BIST	(✓)	(✓)	(✓)
SRAM health checks	✓	✓	✓
SRAM anti-aging	✓	✓	✓
PUF monitoring	✓	✓	✓
Countermeasures against side-channel and fault-injection attacks	✓	✓	✓
Tamper-evident: supports fault detection and reporting		✓	✓
Tamper-resilient: supports fault correction (SRAM)		✓	✓
Tamper-resilient: supports fault correction (logic)			✓
Meets ISO 26262 ASIL D for systematic failures		✓	✓
Meets ISO 26262 ASIL B fault metric			✓
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

© 2023 Intrinsic ID, Inc. Intrinsic ID is a trademark of Intrinsic ID, B.V. All names herein are trademarks. All other trademarks are the property of their respective owners.