INTRINSIC ID®

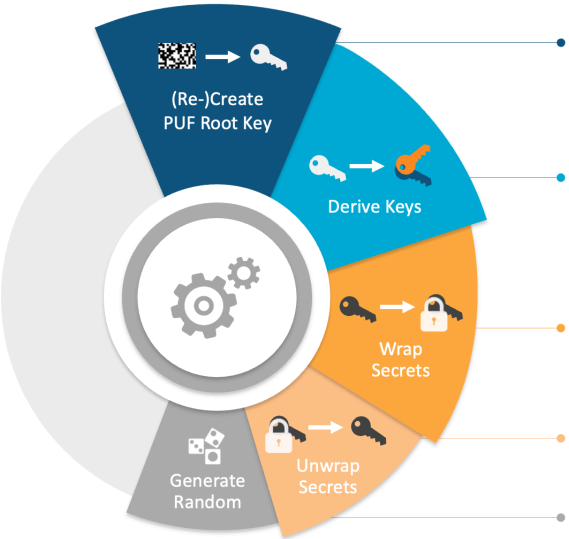
Product Brief: QuiddiKey 100

QuiddiKey 100 Hardware IP

QuiddiKey 100 is a RoT solution that can be applied easily to almost any chip, even the tiniest microcontrollers without the need for adding costly, security-dedicated silicon.

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 a physical unclonable function or 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. 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 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 100 Hardware IP

Applications

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

Certifications

- 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
- Offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device
- Eliminates target for physical attacks: root key is never stored, but re-created from the PUF each time it is needed
- Binds keys to the device so they can only be recreated and accessed on the device on which they have been created on
- Eases integration with custom driver API

	QuiddiKey 100 v1.0
Generate device keys and random values	✓
Wrap and unwrap secrets	(✓)
Size (k gates)	39-64
AC size (bytes)	1000
Security strength (bits)	256
Maximum key length (bits)	4096
Time to root key (k cycles)	49-68
SRAM required for PUF (kB)	2-4
Interface	APB
Logic BIST	(✓)
SRAM health checks	✓
SRAM anti-aging	✓
PUF monitoring	✓
Attack countermeasures	✓
NIST CAVP certification (DRBG, AES, KDF)	(✓)
NIST SP 800-90 compliant	(✓)

(✓) Features are optional

Benefits

- 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
- Remains secure post quantum computing

QuiddiKey 100 Configurations

QuiddiKey 100 is available in off-the-shelf configurations with size ranging between 39k and 64k gates. Configurations differ according to functionality, performance and compliance.

Operational Range

QuiddiKey has been embedded on MCU/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)