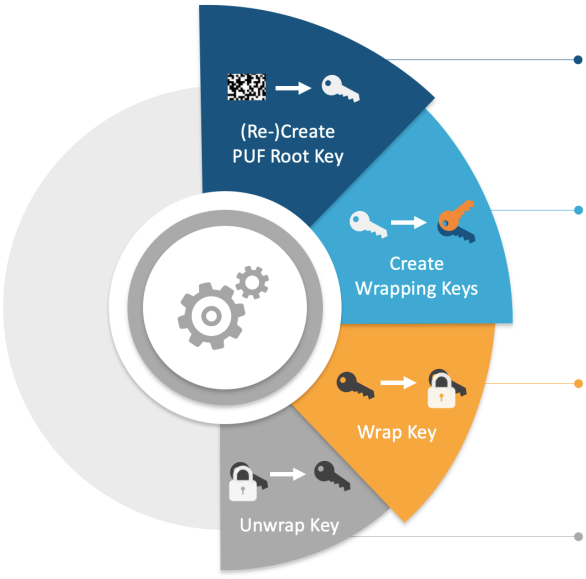
Intrinsic ID QuiddiKey enables device manufacturers and designers to secure their products with internally generated, device-unique cryptographic keys without the need for adding costly, security-dedicated silicon.

QuiddiKey

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. QuiddiKey has been validated for NIST CAVP and 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 wrapping 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 keys 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 keys. Verifies authentication tags for wrapped secrets and decrypts the content for use.

QuiddiKey Hardware IP

Applications

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

Certifications

- NIST CAVP
- Supports FIPS 140-3
- QuiddiKey enabled products have been certified by EMVCo, Visa, CC EAL6+, PSA, and ioXt
- DoD and EU governments qualified

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

Features

- Uses standard SRAM start-up values as a PUF to create a hardware root of trust
- Root key is never stored, but re-created from the PUF each time it is needed
- Offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device
- Keys are bound to the device and can only be recreated and accessed on the device they have been created on
- Configurations can be customized for your application
- Custom driver API for easy integration

QuiddiKey 3.9	Safe	Plus
Generate device keys	✓	✓
Generate random values	✓	✓
Wrap and unwrap secrets		(✓)
Size (k gates)	25	39-64
Security strength (bits)	256	256
Maximum key length (bits)	4096	4096
Time to root key (k cycles)	146	49-68
SRAM required for PUF (kB)	2	2-4
NIST CAVP certification (DRBG, AES, KDF)		(✓)
NIST SP 800-90 compliant		(✓)
Interface	APB	APB
Logic BIST	(✓)	(✓)
SRAM health checks	✓	✓
SRAM anti-aging	✓	✓
Diagnostics	✓	✓
Driver	✓	✓
Attack countermeasures	+	++

(✓) Features are optional

Benefits

- 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
- Highly reliable secure key storage solution in the most advanced technology nodes

QuiddiKey Configurations

QuiddiKey is available in off-the-shelf configurations with size ranging between 25k and 64k gates. Configurations differ according to functionality, performance and compliance, enabling options customized to the needs of your application.

Operational Range

QuiddiKey has been deployed on MCUs/SoCs/ASICs in a diverse set of foundry/process node combinations. SRAM PUF responses across this diverse array have been qualified for use with QuiddiKey in a wide range of operational environments, over years of field operation.

- 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)
- 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)