QuiddiKey®

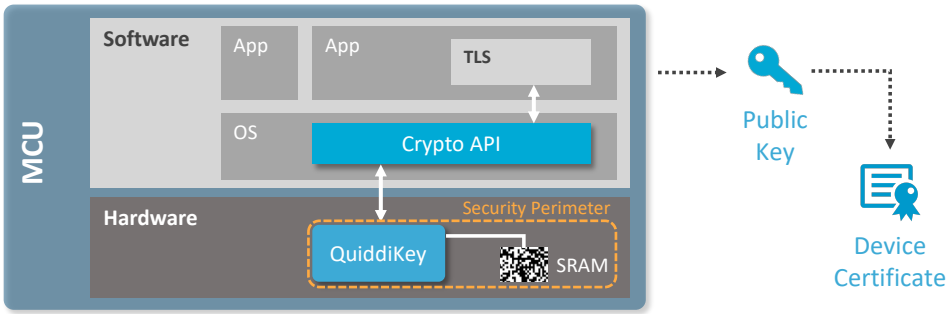
Since QuiddiKey hardware IP is based on SRAM PUF, it not only improves time to market but delivers better security for lower TCO.

The accelerating expansion of the Internet of Things brings with it a comparably expanding threat model. The growing number of endpoints require strong identities as the foundation of trust to establish and scale robust security. QuiddiKey is a secure root key generation and management solution that allows device manufacturers to secure their products with an internally generated, unique identity without the need for adding costly, security-dedicated silicon. The NIST-compliant hardware IP is based on SRAM Physical Unclonable Function (PUF) technology and is the foundation of a device's hardware-based root of trust. The IP is agnostic to fab and technology choice and has been deployed in 150 million+ devices. QuiddiKey not only improves time to market and delivers better security at lower TCO, but paves the way for scaling the IoT to billions of devices.

Unclonable Identities for the IoT

To solve security problems in IoT systems, such as authentication, product lifecycle management, reverse engineering and cloning, every device needs an unclonable identity. This consists of a secret key, a public key and a certificate. The biggest challenge is to get these credentials into the device. QuiddiKey is embedded hardware IP that creates the secret key of the unclonable identity from within, derived using the intrinsic randomness in uninitialized SRAM. This secret key is not stored but is dynamically regenerated from the SRAM PUF inside a secure perimeter.

Completing the unclonable identity requires that a public key be generated from the secret key. And this public key can be turned into a certificate by signing it at a certificate authority. At that point the device is ready to prove its identity and set up a secure channel with another device, a server or a cloud.



QuiddiKey Hardware IP

Applications

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

Certifications

- EMVCo, Visa, CC EAL6+
- U.S. and EU Governments
- Automotive SPICE Level 1
- QuiddiKey compatible w/ China's OSCCA standard

Security Based on SRAM PUF

At power-up, SRAM bits settle in the one or zero state in a non-deterministic way that not even the manufacturer can predict or duplicate. That's what makes it a physical unclonable function, or PUF, which can be used as a unique "silicon fingerprint." An SRAM PUF response is a noisy fingerprint, and turning it into a high-quality and secure key vault requires further processing. This is done with the QuiddiKey hardware IP. QuiddiKey reliably reconstructs the same cryptographic key under all environmental circumstances. Upon first use, called the enrollment, it generates an activation code (AC) which, in combination with the SRAM startup behavior, is used to reconstruct on demand, in real time, an intrinsic PUF key. This PUF key is never stored in flash or OTP. When it is needed later it can be reconstructed.

The intrinsic PUF key can be used as a root key for key derivation and key wrapping. A key protected by QuiddiKey is integrity protected and can be retrieved only on the same device, while it will be meaningless on other devices.

QuiddiKey is available in two configurations:

QuiddiKey-Plus: Device-unique key creation, derivation, wrapping and management

QuiddiKey-Safe: Device-unique key creation and derivation

Low Cost, Flexible & Scalable

Keys are extracted from the chip, on demand, and do not need to be programmed in NVM or OTP. Furthermore, keys can be provisioned at any suitable stage in the production process. The low footprint and flexible design make QuiddiKey suitable for most semiconductor platforms, and scalable to billions of devices.

Operating Ranges

SRAM PUF responses have been qualified for use with QuiddiKey over a wide operating range:

- Qualified top semiconductor fabs and technology nodes, 350nm → 7nm, low power → high speed
- Temperature range from -55°C to 150°C [-67°F to 300°F]
- Voltage supply variation +/- 20%
- Lifetime > 25 years

Deliverables

QuiddiKey hardware IP is easily integrated in any semiconductor design or firmware. Standard deliverables include:

- Synthesizable RTL netlist (VHDL and Verilog)
- APB interface, driver
- Test bench, synthesis constraints
- Datasheet and integration manual

QuiddiKey 3.6	Safe	Plus
Security Strength (bits)	256	256
Maximum Key Length (bits)	4096	4096
SRAM PUF (KB)	2	2
Size (K gates)*	24	42
Generate Device Keys and Random Values	Y	Y
Wrap and Unwrap Keys		Y
RNG according to NIST SP 800-90**		Y

*APB interface and BIST logic are optional and will add 1 K or 5 K gates respectively
**NIST-compliant RNG will add 7 K gates and 2 KB PUF SRAM