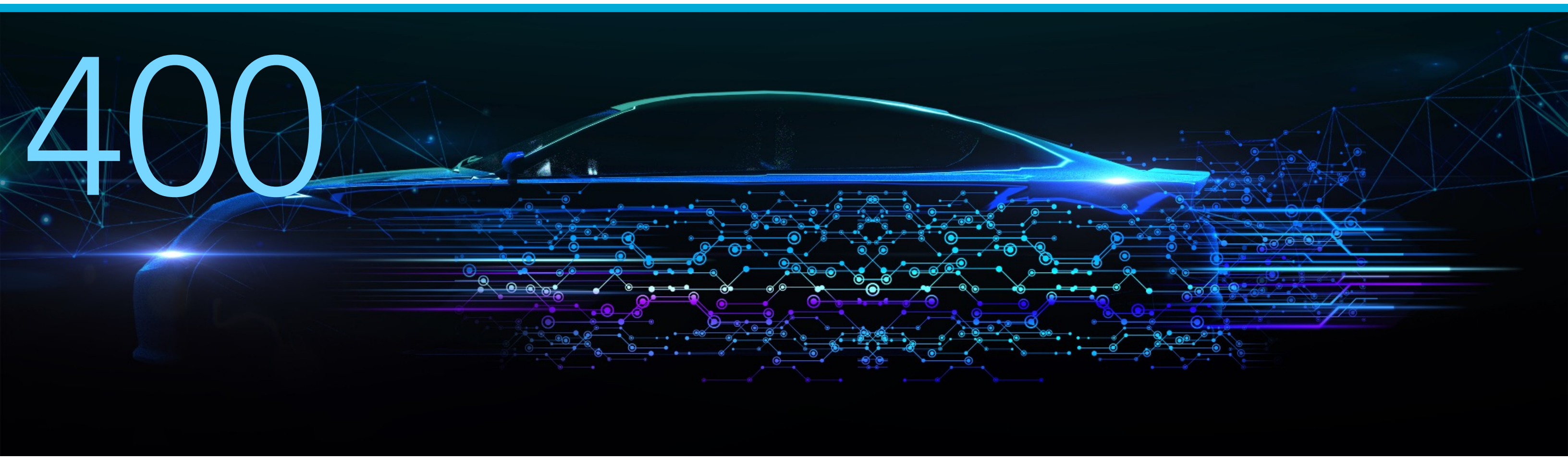
INTRINSIC ID®

Product Brief: QuiddiKey 400



QuiddiKey 400 is agnostic to foundry and process node and has been developed following an ISO 26262 functional-safety-compliant flow to meet the ASIL B fault metric.

QuiddiKey 400 Hardware RoT IP

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. Root-of-trust (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® is a physical unclonable function (PUF)-based RoT solution that can be applied easily to almost any MCU/SoC/ASIC without the need for adding costly, security-dedicated silicon. 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, which was the world's first RoT IP to receive a SESIP and PSA Certified level 3 certification, 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.

Features

- Uses standard SRAM start-up values as a PUF to create a hardware RoT
- Supports fault detection and reporting
- Validates input and output logic, flags observed faults, and offers handholds to check data transfer to and from QuiddiKey
- Offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device
- Binds keys and data to the hardware of the device
- Eases integration with custom driver API

Benefits

- Meets the functional safety ISO 26262 standard ASIL B fault metric
- 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
- Eliminates the need for centralized key management and programming
- Remains secure post quantum computing

Markets

- Automotive
- Aerospace & Defense

Applications

- Authentication
- Secure key storage
- Flexible key provisioning
- Anti-counterfeiting
- Anti-reverse Engineering
- Supply chain protection
- Chiplet security

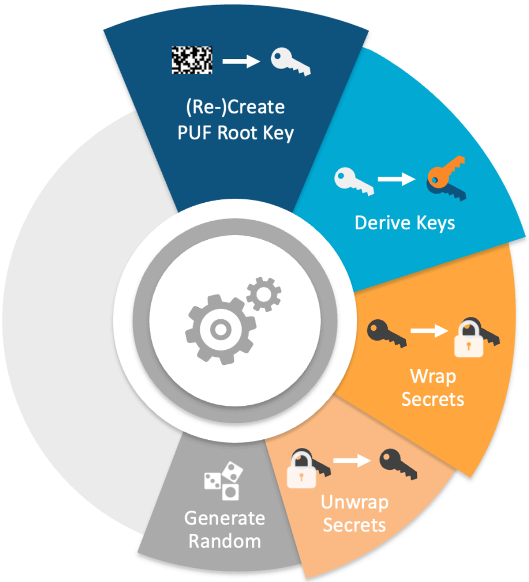
Certifications

- Meets ISO 26262 ASIL B fault metric
- ASIL D for systematic failures
- NIST CAVP
- ISO/IEC 20897-compliant PUF
- FIPS 140-3 support
- SRAM PUF-enabled products have been certified by EMVCo, Visa, CC EAL6+, PSA, and ioXt
- DoD and EU governments qualified

QuiddiKey 400

Intrinsic ID QuiddiKey is the world-leading and certified IP that uses standard SRAM as a PUF to create a strong hardware RoT. The PUF root key is never stored, but re-created from the PUF each time it is needed, offering the highest level of security. A key protected by QuiddiKey is integrity protected and can be decrypted solely on the device on which it was created.

QuiddiKey 400 meets the ISO 26262 Automotive Safety Integrity Level (ASIL) B fault metric. It validates all inputs and critical internal logic through integrity checks and error detection. It continuously asserts that everything runs as intended and flags any observed faults. Additionally, QuiddiKey 400 offers the user hardware and software handholds to check whether all data is correctly transferred to and from QuiddiKey.



QuiddiKey 400	v1.0
Generate device keys and random values	✓
Wrap and unwrap secrets	(✓)
Size (k gates)	115-165
AC size (bytes)	788
Security strength (bits)	256
Maximum key length (bits)	4096
Time to root key (k cycles)	77-95
SRAM required for PUF (kB)	16
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

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

INTRINSIC ID®

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