Zign 100

Zign enables easy, collision-free identification of billions of devices from different vendors

The number of connected devices, machines, sensors, or simply things 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 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, secure device identity is an essential requirement for clone-resistant operational security.

The Intrinsic ID Zign® 100 API enables IoT developers to generate unique device identities, secure cryptographic keys, and random values. It enables easy and collision-free identification of billions of devices from different vendors. Zign 100 can also be integrated as a hardware-based trust anchor for Mbed TLS, OpenSSL, wolfSSL, and other libraries, extending the chain of trust beyond just a single device. Because it is a software-based solution, Zign is the only hardware entropy source currently available that doesn't have to be loaded at silicon fabrication.

Features

- Uses standard SRAM as a physical unclonable function (PUF) to create a device-unique identity and cryptographic keys
- Keys are never stored, but re-created from the PUF each time they are needed
- Keys are bound to the device and can only be recreated and accessed on the device on which they have been created
- NIST SP 800-90A/B compliant random number generator

Benefits

- Easy and collision-free identification of billions of devices from various vendors
- A trust anchor can be installed later in the supply chain, or even remotely retrofitted on deployed devices
- Offers stronger protection than traditional key storage in NVM
- Seamlessly integrates with other crypto such as Mbed TLS, wolfSSL, and OpenSSL
- Proven technology with 500M+ devices in the field
- Zign 100 is post-quantum secure

Markets

- Automotive
- Chiplets
- Financial services
- Internet of things
- Manufacturing
- Medical
- Memory
- Sensors
- Wearables
- Microcontrollers

Applications

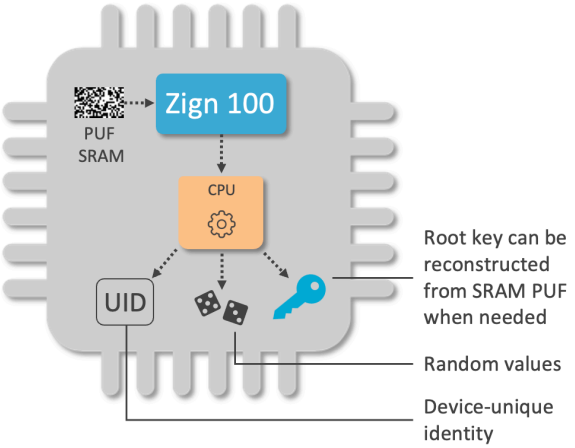
- Device identification
- Secure key storage
- Flexible key provisioning
- Anti-counterfeiting
- Supply chain protection

Certifications

- NIST CAVP
- NIST SP 800-90A
- ISO/IEC 20897-compliant PUF
- Supports NIST SP 800-90B
- Supports FIPS 140-3

Security Based on SRAM PUF

Zign 100 uses the inherently random start-up values of SRAM as a PUF from which a device-unique identity and root key is generated. The root key is never stored and is only available (in volatile memory) when needed. This means the key is never present in persistent memory – even when the chip is powered down – which raises the security significantly and eliminates the need for OTP or other secure memory.



Specifications	Zign 100
Security strength (bits)	128 / 256
SRAM PUF (kB)	0.7 / 1.0
Code size (kB)	6.3 - 7.6
SRAM anti-aging	✓
Device-unique identifier (UID)	✓
Generate device-unique keys	✓
Generate random values	✓
NIST CAVP certifiable (DRBG, KDF, HMAC, SHA-2)	✓
NIST SP 800-90A compliant DRBG	✓
NIST SP 800-90B compliant entropy source for RNG (adds ~3 kB SRAM)	(✓)
FIPS 140-3 ready	(✓)

A potentially unlimited number of keys can be derived from the root key by using the NIST-compliant key-derivation function. Zign 100 also offers random values, generated by a NIST 800-90A/B-compliant random number generator and a unique device identity for each device. All Zign features are accessed by the host software via the API.

Zign 100 Configurations

Zign 100 is available in off-the-shelf configurations with size ranging between 6.3 kB and 7.6 kB. Configurations differ according to functionality, performance and compliance.

Operating Ranges

SRAM PUF responses have been qualified for use with the Zign X00 series 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 [-67°F to 300°F]
- Voltage supply variation +/- 20%
- Lifetime > 25 years

Deliverables

- Target-specific library (C-code)
- Datasheet
- API reference manual
- Code examples (e.g. of integration with Mbed TLS, OpenSSL, wolfSSL)
- NIST documentation
- Application notes