INTRINSIC ID®

Product Brief: Zign X00 Software

Zign X00 Series of Software Products

Zign is the only hardware-based trust anchor currently available that doesn't have to be loaded at silicon fabrication

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.

Root-of-trust (RoT) technology is becoming a requirement for securing connected devices, their data, and, by extension, the entire infrastructure with which they communicate. But, RoT technology shouldn't be limited to hardware design, confining IoT developers to functions programmed at manufacture. The Intrinsic ID Zign® X00 embedded software solutions democratize RoT technology by uncoupling it from silicon fabrication, ensuring it can be accessed, understood, and implemented by IoT application developers at scale.

Features

- Uses standard SRAM as a physical unclonable function (PUF) to create a hardware-based trust anchor and unclonable identities
- Easy and collision-free identification of billions of devices (from various vendors)
- Offers key provisioning, secure key storage, symmetric and asymmetric key cryptography
- 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
- Allows for data encryption on the fly (streaming AES, hash, MAC)
- NIST SP 800-90A/B compliant random number generator

Benefits

- No need for an additional security chip into the device – no SE/TPM needed
- A trust anchor can be installed later in the supply chain, or even remotely retrofitted on deployed devices
- Works on all MCUs, CPUs
- Offers stronger protection than traditional key storage in NVM
- Seamlessly integrates with other crypto such as Mbed TLS, wolfSSL, and OpenSSL
- Intrinsic ID PUFs are post-quantum secure and genuine, no sensitive key material stored
- Proven PUF technology with 650M+ devices in the field
- Higher performance

Proven PUF technology with 500M+ devices in the field

Security Based on SRAM PUF

The Zign X00 series of products use 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.

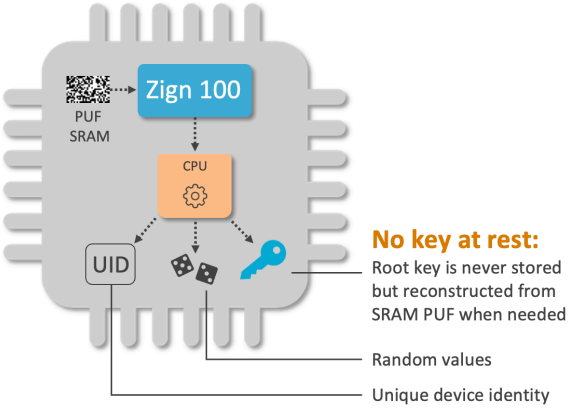
A potentially unlimited number of keys can be derived from the root key by using the NIST-compliant key-derivation function. Zign also offers random values, generated by a NIST 800-90A/B-compliant random number generator. All Zign features are accessed by the host software via the API.

Easy to integrate on any chip, anytime, anywhere

Zign 100

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 various 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.

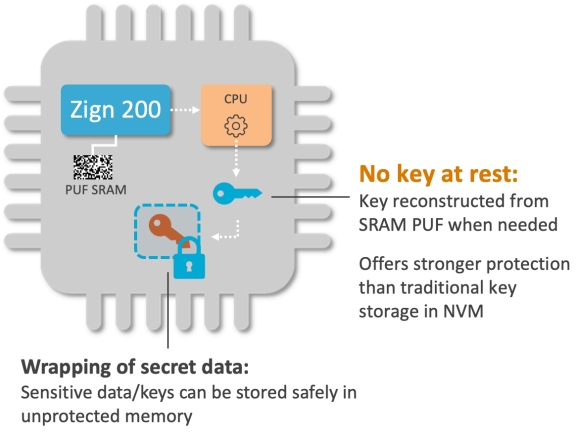
Improve security without the need for additional HW



Zign 200

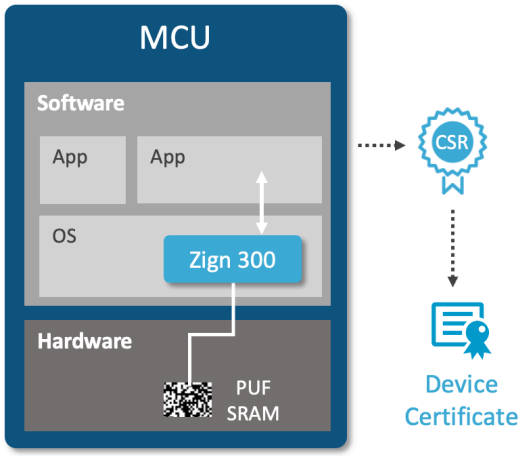
Zign 200 is a secure key generation, management, and storage solution for any IoT device. Zign 200 offers functions to wrap and manage secret keys and encrypt data which then can be stored in unprotected memory or can be securely transmitted over the network.

Zign 200 also offers random values, generated by a NIST 800-90A/B-compliant random number generator and a collision-free unique device identity.



Zign 300

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.



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

Standards & Certifications

- Follows ASPICE Level 1
- MISRA C compliant
- NIST CAVP
- NIST SP 800-90A
- ISO/IEC 20897-compliant PUF
- Supports NIST SP 800-90B
- Supports FIPS 140-3

The biggest challenge is to get these credentials into the device and keep the secret key secret. This can be achieved by using Zign 300. Zign 300 offers the strongest protection of the device secret key and the strongest authentication via unclonable identities.

Zign 300 offers all the features of Zign 200. In addition, Zign 300 offers asymmetric cryptography: public key crypto functions such as ECDSA sign and verify, and ECDH shared secret. PKI elements, such as ECIES and certificate signing request (CSR) are optional.

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

Instruction Set Architecture (ISA) Support

arm RISC-V intel ARC™ xtensa

Configurations

The Zign X00 series of products are available in off-the-shelf configurations with size ranging between 6.3 kB and 30 kB. Configurations differ according to functionality, performance and compliance.

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

Specifications	Zign 100		Zign 200		Zign 300	
	Standard	FIPS 140-3 Ready	Standard	FIPS 140-3 Ready	Standard	FIPS 140-3 Ready
Security strength (bits)	128 / 256	128 / 256	128 / 256	128 / 256	128 / 256	128 / 256
Code size (kB)	6	8	10 / 13	11 / 14	16-21 / 19-28	17-23 / 20-30
SRAM for PUF (KiB)	0.7 / 1.0	2.8 / 4.0	0.7 / 1.0	2.8 / 4.0	0.7 / 1.0	2.8 / 4.0
Unique device identifier (UID)	✓	✓	✓	✓	✓	✓
Generate device-unique keys	✓	✓	✓	✓	✓	✓
Generate random values	✓	✓	✓	✓	✓	✓
Wrap and unwrap secrets			✓	✓	✓	✓
Encryption on the fly			✓	✓	✓	✓
Public key crypto functions*					✓	✓
PKI Elements**					(✓)	(✓)

* Includes ECDSA sign and verify, ECDH shared secret, standard elliptic-curve support set: P256, P384, P521
* Elliptic curve integrated encryption scheme (ECIES), certificate signing request (CSR), self-signed certificates (SSC)