INTRINSIC ID

Product Brief: Zign 200 Software

Zign 200

Zign 200 is a secure key generation, management, and storage solution for any device and doesn't need to be loaded at silicon fabrication

The number of devices, machines, or sensors linked over open communication networks on the internet of things (IoT) has exploded. Every device represents a potential entry point for malicious intrusion – into the device itself, or its network.

Cryptographic keys are needed to verify a device's identity, secure communication between devices, and encrypt sensitive data at rest as well as in transit. Zign® 200 is a secure key generation, management, and storage solution for any IoT device. Zign is a software solution that has been developed according to ASPICE and is the only hardware entropy source currently available that doesn't have to be loaded at silicon fabrication.

The Zign 200 API enables IoT developers to generate cryptographic keys securely and to perform other symmetric key functions. It can also be integrated as a trust anchor for Mbed TLS, OpenSSL, wolfSSL, and other libraries, extending the chain of trust beyond just a single device .

Features

- Uses standard SRAM as a physical unclonable function (PUF) to create a secure key generation and management solution
- Offers key provisioning, secure key storage, and symmetric key cryptography
- Root 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 that 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
- Proven technology with 650M+ devices in the field
- Intrinsic ID PUFs are post-quantum secure and genuine, no sensitive key material stored

Markets

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

Applications

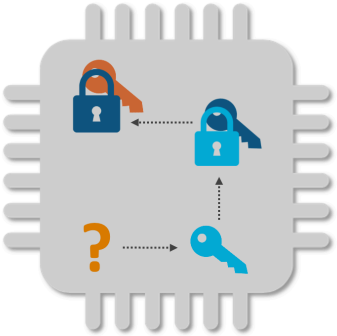
- Secure vault
- Data protection, at rest and in transit
- Flexible key provisioning
- HW-SW binding
- Supply chain

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

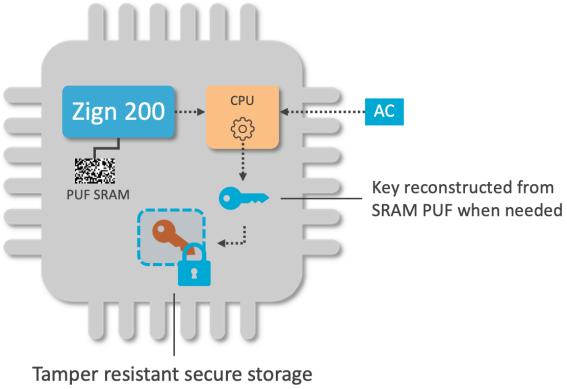
Secure Vault with SRAM PUF

Device makers need a way to protect keys and other secret material. This is typically done by encrypting or wrapping them with other keys. But how do you protect the encryption root key? How to keep secrets secret?



Zign 200 uses inherently random SRAM start-up values as a PUF from which the 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

Specifications	Zign 200
Security strength (bits)	128 / 256
SRAM PUF (kB)	0.7 / 1.0
Code size (kB)	10-14
SRAM anti-aging	✓
Device-unique identifier (UID)	✓
Generate device-unique keys	✓
Generate random values	✓
Wrap and unwrap secrets	✓
Streaming AES, hash, MAC	✓
NIST CAVP certification (DRBG, AES, 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	(✓)



persistent memory – not even when the chip is powered down – which raises the security significantly and eliminates the need for OTP or other secure memory.

Zign 200 offers functions to wrap and manage secret keys and data which then can be stored in unprotected memory or can be securely transmitted over the network. A potentially unlimited number of keys can be derived from the root key by using the NIST-compliant key-derivation function. Zign 200 also offers random values, generated by a NIST 800-90A/B-compliant random number generator and a collision-free unique device identity (UID). All Zign features are accessed by the host software via the API.

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

Zign 200 is delivered as a target-specific library (C-code), along with documentation and examples (e.g. of integration with Mbed TLS, wolfSSL, and OpenSSL). The solution is available in off-the-shelf configurations with size ranging between 10 kB and 14 kB.