INTRINSIC ID®

Product Brief: Zign 300 Software

Zign 300

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 device makers to functions programmed at manufacture. The Intrinsic ID Zign® 300 embedded software solution democratizes RoT technology by uncoupling it from silicon fabrication, ensuring it can be accessed, understood, and implemented by application developers at scale.

Zign is a software security 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. It streamlines OEM and ODM security efforts by creating unique, internally generated device keys and identities derived from the inherent randomness of SRAM physical unclonable functions or PUFs. The Zign 300 API enables developers to generate and store cryptographic keys securely and to perform other symmetric key and elliptic curve cryptographic functions for securing connected devices, their data, and, by extension, the entire infrastructure with which they communicate.

Zign 300 democratizes RoT technology by insuring it can be accessed, understood and implemented by IoT application developers at scale, and is not tied to silicon fabrication

Features

- Secure key generation and management
- Uses standard SRAM as a PUF to create a RoT on any connected device
- Offers key provisioning, secure key storage, symmetric key and elliptic curve 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
- Offers a NIST SP 800-90A/B compliant random number generator

Benefits

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

Markets

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

Applications

- Anti-counterfeiting
- Device-to-host Authentication
- Secure key storage
- Flexible key provisioning
- HW-SW binding
- 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

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 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.

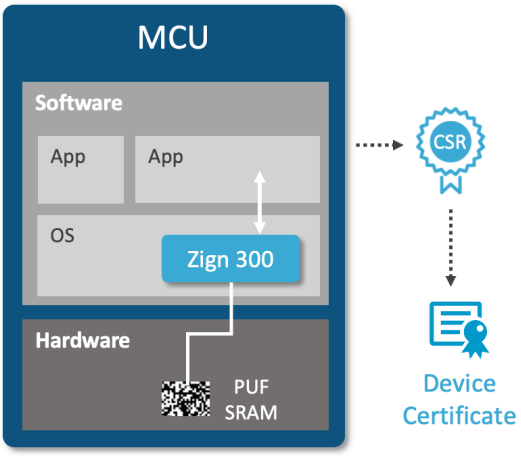
Security Based on SRAM PUF

By using SRAM PUF technology, keys are regenerated when needed, and never present in persistent memory – not even when the chip is powered down – which raises the security significantly and eliminates the need for OTP or secure memory.

Specifications	Zign 300
Security strength (bits)	128 / 256
SRAM PUF (kB)	0.7 / 1.0
Code size (kB)	16-23 / 19-30
SRAM anti-aging	✓
Generate device-unique keys	✓
Generate UID and random values	✓
Wrap and unwrap secrets	✓
Streaming AES, hash, MAC	✓
Public key crypto functions*	✓
PKI elements*	(✓)
NIST CAVP certification (DRBG, AES, KDF, HMAC, SHA-2, ECC)	✓
NIST SP 800-90A compliant DRBG	✓
NIST SP 800-90B compliant entropy source for RNG (adds ~3 kB SRAM)	(✓)
FIPS 140-3 ready	(✓)

* 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)



Zign 300 offers random values, generated by a NIST 800-90A/B-compliant random number generator, and a collision-free unique device identity (UID). It also 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. In addition, Zign 300 offers public key crypto functions such as ECDSA sign and verify, and ECDH shared secret. PKI elements such as certificate signing requests (CSR) are optional. All Zign features are accessed by the host software via the API.

Operating Ranges

SRAM PUF responses have been qualified for use with Zign 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 300 is delivered as a target-specific library (C-code), along with documentation and examples (e.g. of integration with Mbed TLS, wolfSSL, and OpenSSL).