INTRINSIC ID®

Fact Sheet

At a Glance

- Provider of security IP based on PUF technology
- Spun out of Royal Philips Electronics in 2008
- Investors include Prime Ventures and Robert Bosch Venture Capital
- Headquarters: Sunnyvale, Calif. U.S.
- R&D: Eindhoven, The Netherlands

Founders

- Dr. Pim Tuyls, CEO
- Geert-Jan Schrijen, CTO

Intrinsic ID

Intrinsic ID is the world's leading provider of security IP for embedded systems based on physical unclonable function or PUF technology. The technology provides an additional level of hardware security utilizing the inherent uniqueness in each and every silicon chip. The IP can be delivered in hardware or software and can be applied easily to almost any chip – from tiny microcontrollers to high-performance FPGAs – and at any stage of a product's lifecycle. It is used as a hardware root of trust to validate payment systems, secure connectivity, authenticate sensors, and protect sensitive government and military data and systems.

Intrinsic ID has become the world's first IP vendor with PSA Certified level 3 and SESIP level 3 certification. Intrinsic ID security IP has been deployed and proven in hundreds of millions of devices certified by EMVCo, Visa, CC EAL6+, PSA, IoXt, and governments across the globe.

Mission

It is our mission to make it easy for semiconductor manufacturers and OEMs to secure their smart devices and create a connected world that can be trusted.

Our PUF IP enables chip designers to build secure key vaults or provision their chips with an unclonable identity in the most secure, seamless, cost-effective manner.

Leader in PUF Technology

- More than 600 million secured ICs
- Most scalable/robust PUF technology
- Largest SRAM PUF patent portfolio
- >15 years proven entropy and reliability
- Enables secure key storage in any memory
- Intrinsic ID PUFs are post-quantum secure and genuine, no sensitive key material stored

Featured Customers

NXP MICROCHIP intel Micron

RENESAS qorvo TDK InvenSense infokeyVault

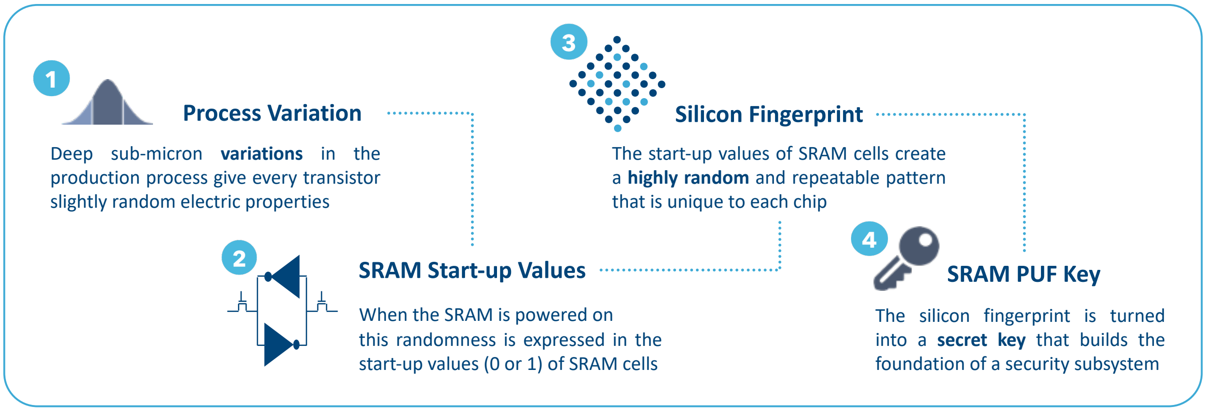
Fact Sheet

Use Cases

- Secure Key Storage
- Authentication
- Flexible Key Provisioning
- Anti-counterfeiting
- IP Binding
- Supply Chain Protection

Operating Specifications

- 256- or 128-bit key entropy
- Highly reliable in a wide range of operational environments and across all foundries and process node
- Lifetime > 25 years



1 **Process Variation**

Deep sub-micron **variations** in the production process give every transistor slightly random electric properties

2 **SRAM Start-up Values**

When the SRAM is powered on this randomness is expressed in the start-up values (0 or 1) of SRAM cells

3 **Silicon Fingerprint**

The start-up values of SRAM cells create a **highly random** and repeatable pattern that is unique to each chip

4 **SRAM PUF Key**

The silicon fingerprint is turned into a **secret key** that builds the foundation of a security subsystem

Core Technology: SRAM PUF

The SRAM PUF is based on the unique characteristics of unitialized static RAM. At power up, SRAM bits settle in the one or zero state in a non-deterministic way that not even the fabricator or designer can predict or duplicate. That is what makes a physical unclonable function, or PUF, which can be used as a unique "silicon fingerprint".

An SRAM PUF response is a noisy fingerprint, and turning it into a high-quality and secure key vault requires further processing. This is done with the Intrinsic ID IP. It reliably reconstructs the same cryptographic key under all environmental circumstances. This (PUF) key is never stored in NVM or OTP. When it is needed, it can be reliably reconstructed.

Other PUFs

Apart from the SRAM PUF, Intrinsic ID has developed other PUF technologies, such as Buskeeper PUF and Butterfly PUF. Butterfly PUFs are being used on Xilinx FPGAs where there is no uninitialized SRAM available.

Featured Products

QuiddiKey® Hardware RoT IP

Hardware root-of-trust IP which allows chip designers to create, wrap and manage keys based on SRAM PUF. This certified IP has earned its stripes from massive volume IoT deployments to high security payment systems and aerospace & defense applications.

Apollo - Trust Anchor on FPGA

Apollo uses circuits present inside Xilinx FPGAs to create a key vault which allows designers to secure data in transit and on chip. Since Apollo is part of the FPGA configuration file it is a "soft PUF" implementation and security functionality can be retrofitted on deployed devices, enabling remote "brownfield" installation of a hardware root of trust.

Zign® Software Solutions

The Intrinsic ID Zign key generation and management software solutions combine the benefits of SRAM PUF technology with the flexibility of software. Zign contains all the crypto functionalities to upgrade the security in any MCU/CPU e.g by building a secure element or provisioning the chip with an unclonable identity.

INTRINSIC ID

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