INTRINSIC ID

Citadel Infrastructure Tools

for SRAM PUF Deployment

Tool Benefits

- Easy deployment of SRAM PUF
- Flexible provisioning in supply chain
- Trusted supply chain
- Reduced liability
- No stock of provisioned devices
- Suitable for low, mid, and high volumes
- No specialized equipment needed for secret programming

Use Cases

- Device authentication
- Flexible key provisioning
- Device credential provisioning
- Integrity of the supply chain
- Anti counterfeiting
- Anti-cloning
- Protection against reverse-engineering

IoT Markets

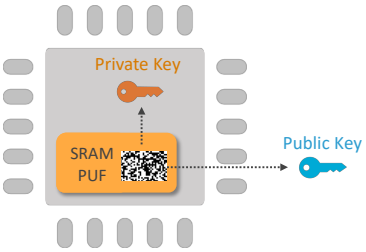
- Critical infrastructure
- Automotive
- Medical
- Smart city
- Industrial IoT
- Smart buildings

Overview

Citadel™ Infrastructure Tools is a suite of software products which accelerate SRAM PUF deployment of unclonable device identities for securing IoT applications, particularly those targeting wide-scale deployment. They can be used by semiconductor vendors and OEMs to provision their devices and by OEMs and application developers to create applications that are using SRAM PUF-based security. Available are tools for provisioning and for crypto applications which, along with BroadKey™ and QuiddiKey® key-management products, form the basis of secure device lifecycle management. Citadel infrastructure tools enable easy setup, management and use of SRAM PUF-based root of trust (RoT) in IoT devices. Through a tight integration with the IoT ecosystem, semiconductor manufacturers and OEMs will benefit from all the advantages of SRAM PUF-rooted security while experiencing full application flexibility and ease of design.

Unclonable Identity

Due to the deep sub-micron process variations, every semiconductor device is different at the atomic level. These differences are expressed in the power-up state of uninitialized SRAM. This state forms a unique pattern for every device and acts like a “silicon fingerprint”. Secret keys created from these device characteristics act as aa physical unclonable function (PUF). When the SRAM is not powered there is no key present on the chip, making the solution very secure from reverse-engineering and key extraction.



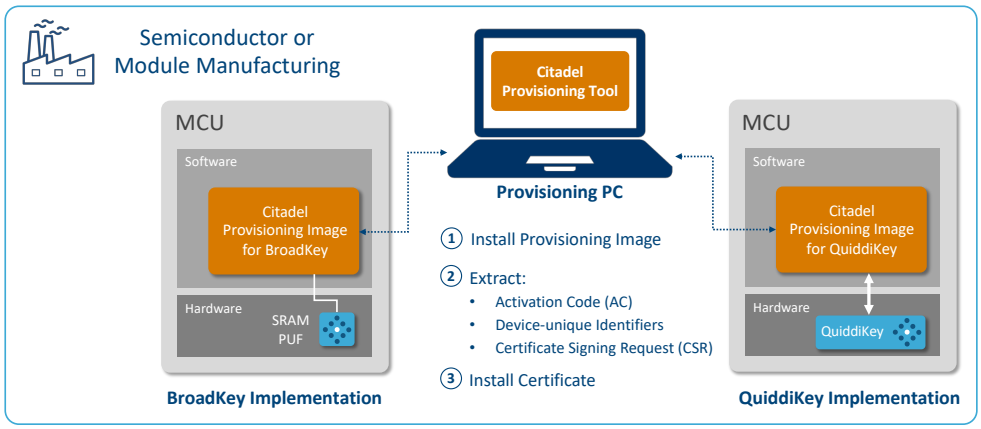
In order to solve several security problems in IoT systems, such as authentication, product life-cycle management, reverse engineering and cloning, every device needs an Unclonable Identity. This consists of a secret key, a public key and a certificate. The secret and public key components of the unclonable identity are created by QuiddiKey or BroadKey.

Citadel Provisioning Tool

The provisioning capability initializes an IoT device’s SRAM PUF-based root of trust, to generate its unclonable identity. The tool requests the device to output a certificate signing request (CSR) and send that to a certificate authority (CA) for the creation of a certificate. Once the certificate is generated, the tool provisions the certificate into the device. The software combines a PC-based application with a provisioning image that runs on the IoT device. It let’s the user:

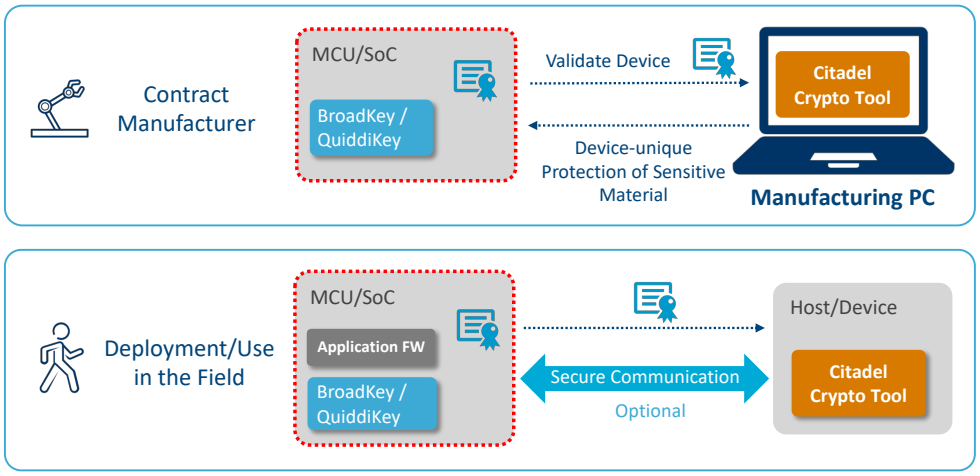
- Enroll the device to activate a fresh cryptographic context based on the SRAM PUF RoT and extract the corresponding activation code (AC)

- Generate and install device-unique identifiers
- Generate device-unique key pairs and extract public keys based on elliptic-curve cryptography
- Generate and extract device CSRs
- Create and sign device certificates with a local, cloud or global CA
- Install device certificates on the device, and/or automatically attach them to an IoT cloud service for just-in-time registration



Citadel Crypto Tool

The crypto tool consists of PC-host software that enables full use of unclonable device identities to secure operations in the field. It is compatible with and communicates with BroadKey-Pro and QuiddiKey-Pro on the IoT device. The fact that these cryptogram functions constitute a one-pass secure protocol with these security properties makes them well suited for import/export functions of external secrets in key provisioning or as a payload protection mechanism, such as a secure update flow.



Features include the generation and processing of a cryptogram, for secure messaging based on public key cryptography, to and from a SRAM PUF-backed application. The cryptogram functions enable a secure one-pass messaging protocol based on elliptic curve cryptography. A sending system can transform a plaintext message into a secure cryptogram using its own elliptic curve private key and a receiver's elliptic curve public key. The corresponding receiving system can unpack the message from the cryptogram using its own elliptic curve private key and the sender's public key. The basic properties achieved by this one-pass protocol are:

- The message contained in a cryptogram is confidential
- The cryptogram is integrity-protected
- The receiver can authenticate the sender of the message in the cryptogram
- Cryptograms are non-replayable

Easy Integration and Operation

The infrastructure tools have a straightforward human-operator interface which can also be easily automated and fully integrated in a semiconductor manufacturer's or OEM's provisioning flow, application tools, and back-end services. The software of the infrastructure tools is written in portable code and the tools are available for Windows, Linux and Mac.

info@intrinsic-id.com
www.intrinsic-id.com
INTRINSIC ID