Overview

IoT device manufacturers are under immense pressure to provide device personalization, strong protection of sensitive assets, and in-field application services in order to help their products stand out from the crowd. All of these features come at the high cost of key delivery methods that don’t allow for the scalability of device appropriate security.

CITADEL is the world’s first SRAM PUF-based key provisioning system designed to keep pace with the growing demand for the generation, distribution, and protection of cryptographic keys for IoT applications.

SRAM PUF Benefits
- Uses standard SRAM
- Device-unique keys
- No secrets reside on the chip

Key Provisioning Benefits
- On-chip key generation
- Reduced risks and liabilities
- Lower total cost of ownership

Ideal for the IoT Market
- Industrial
- Automotive
- Health
- Wearables
- Smart grid
- Home

STRENGTH
Using SRAM PUF for cryptographic functions introduces a new method of protecting valuable assets. The root keys are created from the silicon characteristics unique to each chip and never leave the chip boundary. This creates a tighter security perimeter that is managed by the System OEM, reducing the risks and liabilities in the supply chain.

FLEXIBILITY
Since CITADEL is not dependent on the alteration of silicon at the chip manufacturing stage, the provisioning of keys can take place anywhere in the supply chain, creating the concept of just-in-time key generation. SRAM PUF root keys for anti-cloning, certificates for device personalization, and application keys for in-field services can all be created at the point of use instead of being passed through the logistics network.

AFFORDABILITY
Scalability of security in the IoT market is tightly connected to the high cost of creating and protecting keys on chips that have been stripped down to their essential compute functions. This leads system OEMs to ask the question “How important is security on this device?” The CITADEL key provisioning system makes the answer easy by cutting key costs down to device-appropriate levels instead of the one-size fits all model.
The CITADEL key provisioning system is built around a full-featured set of manufacturing and OEM managed tools. The software libraries that run on manufacturing equipment have been designed for full-speed production. The OEM management modules are ready for integration into enterprise class infrastructures.

**Use Cases**
- Advanced DRM and content locking with flexible certificate modes and revocation of keys
- OEM management for cloud-based inventory tracking, monitoring and secure usage metering
- Trusted applications for payments, authenticated health, automotive, and building access control
- In-field device upgrades, updates, and deactivation including remote service diagnostics and service
- Supply-chain management with zero-knowledge transfer, anti-cloning and reverse engineering protection