BroadKey™

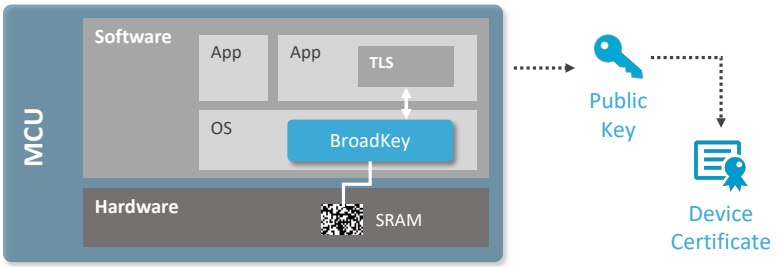
BroadKey software enables a never-before-possible remote "brownfield" installment of a hardware root of trust.

The accelerating expansion of the Internet of Things brings with it a comparably expanding threat model. The growing number of endpoints require strong identities as the foundation of trust to establish and scale robust security. BroadKey is a secure root key generation and management software solution for IoT security that allows device manufacturers to secure their products with an internally generated, unique identity without the need for adding a costly, security-dedicated silicon. Since BroadKey is a software implementation of SRAM PUF, it is the only hardware entropy source option for securing IoT products that does not need to be loaded at silicon fabrication. It can be installed later in the supply chain, and even remotely retrofitted on deployed devices. This enables a never-before-possible remote "brownfield" installment of a hardware root of trust and paves the way for scaling the IoT to billions of devices.

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. The figure below illustrates how this can be achieved by using BroadKey. BroadKey creates the secret key of the unclonable identity from within, derived using the intrinsic randomness in uninitialized SRAM. This secret key is not stored but is dynamically regenerated from the SRAM PUF.

Completing the unclonable identity requires that a public key be generated from the secret key. And this public key can be turned into a certificate by signing it at a certificate authority. At that point the device is ready to prove its identity and set up a secure channel with another device, a server or a cloud.



Applications

- Secure Key Storage
- Authentication
- Flexible Key Provisioning
- Anti-Counterfeiting
- HW-SW Binding
- Supply Chain Protection

Certifications

- EMVCo, Visa, CC EAL6+
- U.S. and EU Governments
- Automotive SPICE Level 1
- BroadKey-Safe compatible w/ China's OSCCA standard

Security Based on SRAM PUF

At power-up, SRAM bits settle in the one or zero state in a non-deterministic way that not even the manufacturer can predict or duplicate. That's what makes it 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 BroadKey software IP. BroadKey reliably reconstructs the same cryptographic key under all environmental circumstances. Upon first use, called the enrollment, it generates an activation code (AC) which, in combination with the SRAM startup behavior, is used to reconstruct on demand, in real time, an intrinsic PUF key. This PUF key is never stored in flash or OTP. When it is needed later it can be reconstructed.

The intrinsic PUF key can be used as a root key to wrap and manage user keys. Reconstruction can be done very quickly starting at 0.7M cycles for 128 bits keys. All of BroadKey's features are accessed by the host software via the

BroadKey API. BroadKey is available in three configurations:

BroadKey-Pro: Device-unique key derivation, random number generation, wrapping and management, including elliptic curve private key generation and storage, importing and exporting of public keys, signature generation and verification, key agreement functionality and public key encryption and decryption.

BroadKey-Plus: Device-unique key derivation, random number generation, application key wrapping and management.

BroadKey-Safe: Low footprint, device-unique key derivation and random number generation.

Low Cost, Flexible & Scalable

Keys are extracted from the chip, on demand and do not need to be programmed in NVM or OTP. Furthermore, keys can be provisioned at any suitable stage in the production process. The low footprint and flexible design make BroadKey suitable for most semiconductor platforms, and scalable to billions of devices.

Operating Ranges

SRAM PUF responses have been qualified for use with BroadKey over a wide operating range:

- Qualified top semiconductor fabs and technology nodes, 350nm → 7nm
- Semiconductor processes include low power, high speed and high density
- Temperature range from -55°C to 150°C [-67°F to 300°F]
- Voltage supply variation +/- 20%
- Accelerated lifetime > 25 years

BroadKey Software IP is delivered as a library compiled for a specific target chip, along with API specifications and user manual.

BroadKey Configurations	Safe	Plus	Pro
Security Strength (bits)	128/256	128/256	128/256
SRAM PUF (KB)	0.7/1	0.7/1	0.7/1
Code Size (KB)	8	10	21
Generate Device Keys and Random Values	Y	Y	Y
Wrap and Unwrap Application Keys		Y	Y
Public Key Management and Crypto Operations			Y