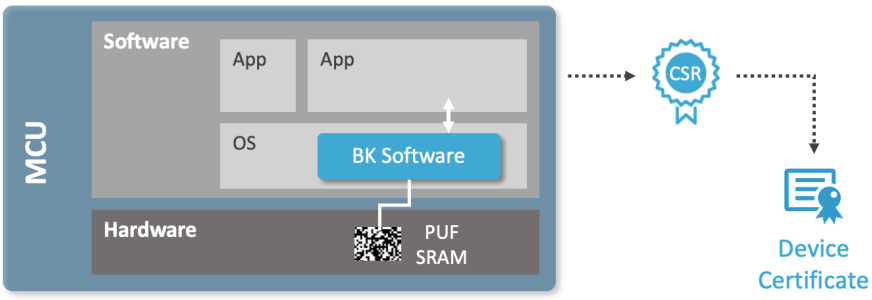
BK Software

BK 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. BK 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 BK 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 BK. BK software 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



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
- BK-Safe compatible w/ China's OSCCA standard

identity and establish a secure channel with another device, a server or a cloud.

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 is what makes the SRAM response a PUF, which can be used as a unique "silicon fingerprint." By nature some of the SRAM bits are unstable, making the fingerprint unstable. Turning a noisy fingerprint into a high-quality, secure key vault requires further processing. BK software IP provides this processing, which enables BK to reliably reconstruct the same cryptographic key under all environmental circumstances.

Upon first use, called the enrollment, the BK software generates an activation code (AC) which, in combination with the SRAM startup behavior, is used to reconstruct the intrinsic PUF key on demand, in real time. This PUF key is never stored but reconstructed when needed. Reconstruction is fast, starting at 0.5M cycles for 128-bit keys. BK software offers functions to wrap and manage secret keys and data which then can be stored in unprotected memory. All of the BK features are accessed by the host software via the API.

BK software is available in different configurations and sizes as indicted in the table below.

Low Cost, Flexible & Secure

This software-only product is easy to integrate and improves time to market. No need for additional or modified silicon. Wrapped keys can be stored securely in unprotected memory. BK software works on all MCUs, CPUs and allows for brownfield deployments of hardware-based security.

Operating Ranges

SRAM PUF responses have been qualified for use with BK 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

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

BK 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)	7	8	14-26
Generate device keys and random values	✓	✓	✓
Wrap and unwrap application keys		✓	✓
Public key crypto functions (ECDSA and ECDH)*			✓
PKI elements: cryptogram, certificate signing request (CSR), self-signed certificates (SSC)			(✓)

* Includes ECDSA sign and verify, ECDH shared secret, elliptic-curve support set: P192, P224, P256, P384, P521