SAMSUNG ARTIK™

End-to-end security

Product Brief

Samsung ARTIK™ Smart IoT Platform: Comprehensive, integrated, end-to-end IoT security

The fastest path to IoT security best practices

Do you know what it takes to secure your IoT hardware, software, and communications against malicious attacks? Do you know how to implement the necessary technology? Do you know how much that will cost?

Edge-to-cloud IoT security with the Samsung ARTIK

The ARTIK™ IoT platform is a scalable, open solution from Samsung, the global leader in connected devices and embedded components. Tight integration between ARTIK hardware, software, connectivity, and cloud services allows for integrated, edge-to-cloud security. This is achieved with device protection and trusted code execution, secure communications, and secure storage.

Device protection and trusted code execution

The ARTIK IoT platform includes several families of systems-on-modules (SoMs) ranging in computing power and connectivity options. Device protection and trusted code execution is built into every ARTIK SoM. Each SoM is injected with a unique, tamper-resistant ID during the manufacturing process.

ARTIK key management service (KMS), code signing, and secure over-the-air (OTA) updates ensure that only signed, authentic code runs on ARTIK SoM-powered devices.

Secure communications with ARTIK devices and SmartThings Cloud

The ARTIK IoT platform encrypts communications between different ARTIK-based devices and between those devices and the SmartThings cloud using TLS 1.2, industry-standard cryptographic algorithms, and mutual authentication using a shared root of trust.

Secure storage, secure file system, and secure element

A specific partition is managed by the Samsung Secure OS which is based in an ARM® TrustZone. All data in this partition is encrypted using a unique key generated in runtime and stored as a file unit.

Inside the ARTIK SoM secure storage is a tamper-resistant Common Criteria EAL5 secure element provisioned with X.509 certificates and corresponding keys and identities.

Top 10 security components of Samsung™ ARTIK

1. **Device integrity protection and detection**
   Each device includes secure boot to validate the integrity of the critical code and can stop the boot process if it's compromised.
2. **Hardware root-of-trust**
   The first code executed by an ARTIK SoM when powered-on is stored in ROM. This assures device integrity and prevents hackers from injecting malware.
3. **Trust chain**
   To ensure attackers cannot replace or modify software, each ARTIK-based device can be equipped with a security certificate issued by Samsung or a third-party certificate issuing agency.
4. **Secure updates**
   ARTIK provides secure over-the-air (OTA) updates. Combined with code signing, this ensures that only authentic code runs on ARTIK devices.
5. **Protected communication**
   Communications between different ARTIK-based devices and between those devices and ARTIK cloud services are encrypted. Mutual authentication is provided by a shared root of trust.
6. **Secure storage**
   ARTIK IoT devices provide secure storage to guarantee confidentiality and data integrity, and all storage security features are hardware-backed.
7. **Hardware protection**
   Most ARTIK systems-on-modules (SoMs) include a Common Criteria EAL5 hardware secure element which is optimized for IoT and provisioned with X.509 certificates and corresponding keys.
8. **Device identity**
   All ARTIK SoMs have a unique certificate, injected during manufacture, which the device uses to establish its identity with ARTIK cloud services on SmartThings Cloud.
9. **Mutual authentication**
   The ARTIK platform uses strong, certificate-based, mutual authentication between gateway devices and ARTIK cloud services on SmartThings Cloud.
10. **Disable hardware debug ports**
    Samsung ARTIK SoMs support Secure JTAG, which requires the use of a password unique to each SoM.

Samsung ARTIK end-to-end security

Feature Summary

Device protection and trusted code execution

- Unique, tamper-resistant ID injected during the manufacturing process.
- ARTIK key management service (KMS) and code signing service
- Secure over-the-air (OTA) updates

Secure communications with other devices and the cloud

- TLS 1.2 industry-standard cryptographic algorithms
- Mutual authentication and root of trust
- Secure device registration (SDR)
- Secure JTAG

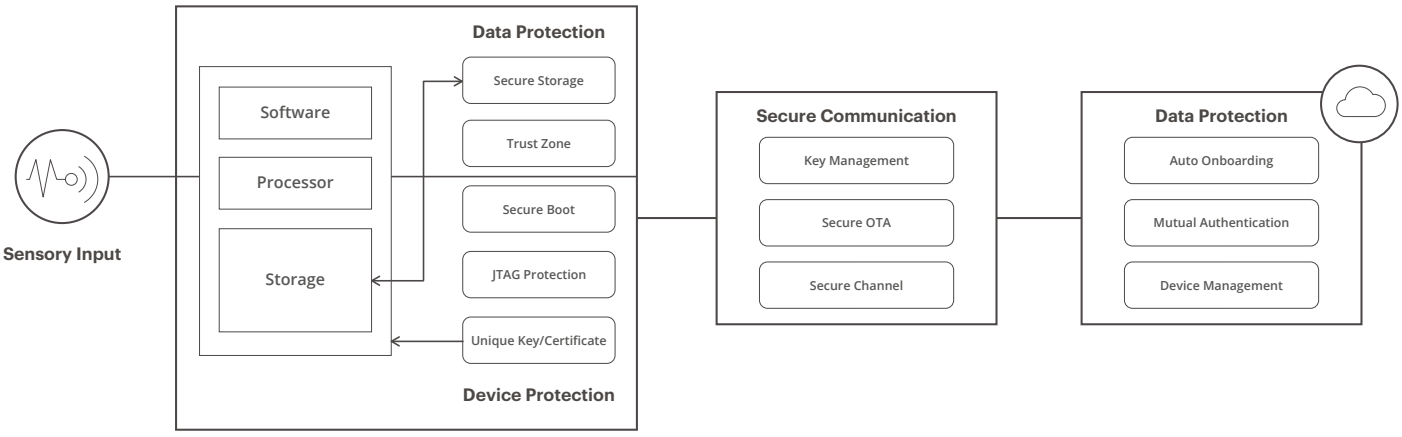
Secure storage, secure file system, and secure element

- The Samsung eMMC secure file system
- ARM® TrustZone
- Data encrypted with runtime-generated key
- Tamper-resistant Common Criteria EAL5 secure element
- Physically unclonable function (PUF) (ARTIK 053)

		ARTIK module	ARTIK S-module	Comments
Device protection and trusted execution	KMS infrastructure for code signing		✓	Key management service
	Code verification key in HW		✓	Secure key storage
	Secure boot (checks for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Secure communications	Per-device unique key and certificate	✓*	✓	Uniquely identifies device
	Key stored in HW secure element	✓*	✓	Secure key storage
	PKI infrastructure: mutual authenticaion of device and cloud	✓*	✓	Device talks to authorized cloud and vice versa
Secure storage, secure file system, and secure element	Secure OS (separates normal and secure operations)		✓	Hardware enforced secure applications via TEE
	Limited security lib API (3 API calls)	✓*	✓	Random number generator, get certificate and signature
	Full security lib API (27 API calls)		✓	Key manager, authentication, secure storage, encrypt/de-crypt
	Credential provisioning		✓	Add and manage certificates and keys on device (and in secure element)
	Secure storage		✓	Encrypt data stored on Flash

* Not including 020 and 030

Security architecture



Version - 11/29/17

SAMSUNG ARTIK™