Samsung ARTIK Overview
Easy, interoperable, secure IoT

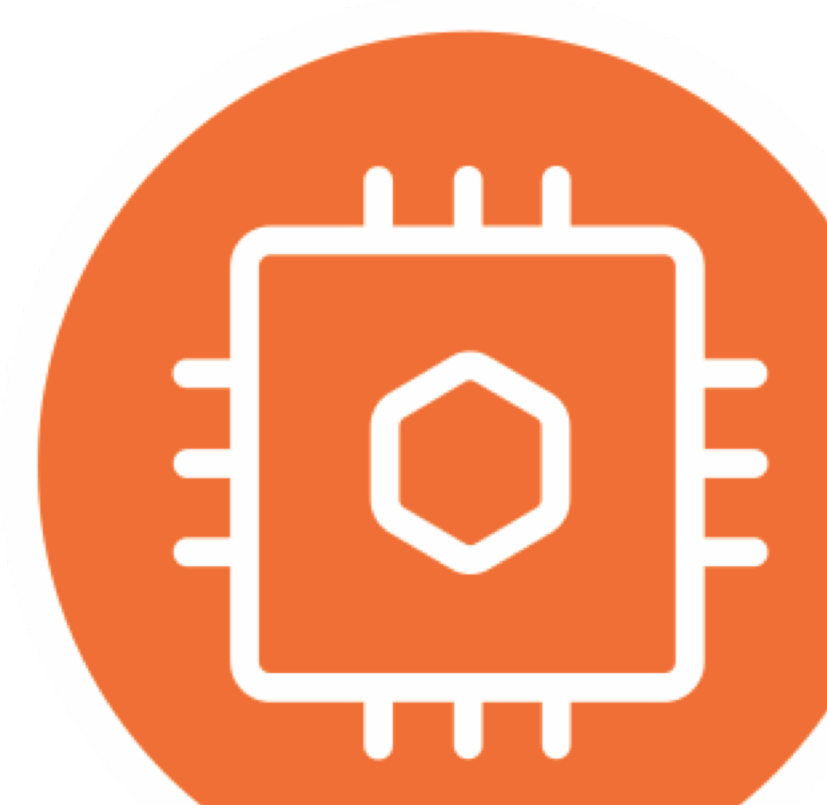
Wei Xiao

Jan 4, 2018

SAMSUNG ARTIK™

Agenda

- ARTIK S-Module Overview
- OS Transition to Ubuntu Linux
- Hands-on / Demos



SAMSUNG ARTIK™

ARTIK S-Module Overview

Module Security

SAMSUNG ARTIK™

Samsung ARTIK™ Modules

ARTIK 0 Modules

Edge nodes, battery-powered devices, intelligent appliances

020	030	053	053s	055s
15 x 12.9 x 2	15 x 12.9 x 2	15 x 40 x 3.9 5-12 VDC		15 x 26 x 3.9 3.3 VDC

- Single, dual Cortex-M, Cortex-R CPUs
- BLE, ZigBee/Thread or WiFi support
- Real-time OS or bare metal
- Hardware Secure Element (05 series; 021)

ARTIK 5, and 7 Modules

Hubs and gateways

520	530	530s	710	710s
30 x 25 x3.4	36 x 49 x 3.4		36 x 49 x 3.4	

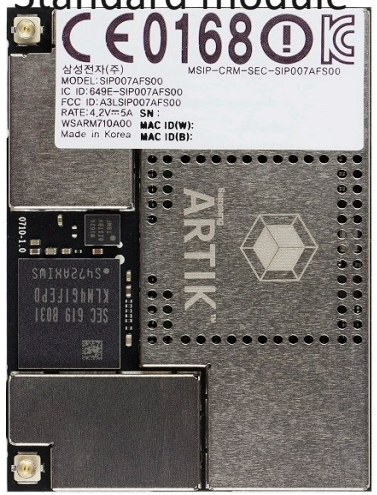
- Dual, quad, up to octa-core Cortex-A53 CPUs
- Linux based Operating System
- Hardware Secure Element

SAMSUNG ARTIK™

Non-S vs. S Modules

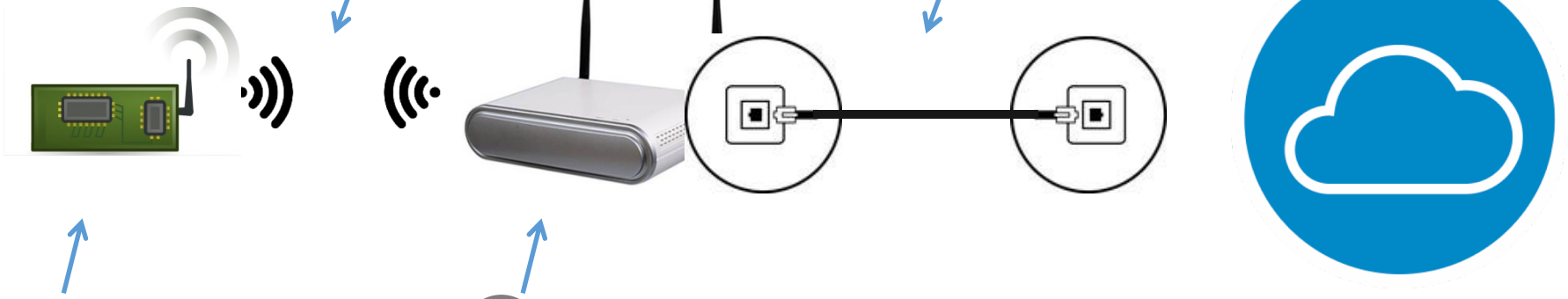
- Same HW specifications other than security features
- "s" type modules can be identified by **blue** labeling

Standard module



"S" module

Why S-Module?



Secure Communication

Device Protection
Secure Code Execution

Data Protection

SAMSUNG ARTIK™

Samsung ARTIK™ S-Module Features

		ARTIK module (05x, 5, 7)	ARTIK S-module	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

SAMSUNG ARTIK™

Samsung ARTIK™ 710/710s high-end gateway

Secure, fully-integrated IoT solution

- High-end gateways
- Cameras
- Human-machine interface
- Machine learning

SAMSUNG ARTIK™

Processor	**CPU:** 8x ARM® Cortex® A53 @ 1.4 GHz **GPU:** 3D graphics accelerator
Memory	**DRAM:** 1 GB DDR3 @ 800 MHz **Flash:** 4 GB eMMC v4.5
Multimedia	**Camera I/F:** 4-lane MIPI CSI **Display:** 4-lane MIPI DSI up to FHD@24 bpp, LVDS, HDMI v1.4 **Audio:** I²S audio interface
Connectivity	**WLAN (Wi-Fi):** IEEE 802.11 b/g/n/ac **Bluetooth:** 4.1+ Smart **802.15.4:** Zigbee, Thread **Ethernet:** 10/100/1000 Base-T MAC (external PHY required)
Security	Secure element, EAL Level 5, unique device certificate and keys, PKI with mutual authentication to cloud, hardware crypto engine; secure boot*, KMS*, TEE*, ***S-modules**
I/O	GPIO, I²C, I²S, SPI, UART, PWM, SDIO, USB 2.0, JTAG, analog input
Temperature range	0° to 70° (°C)
Size	36 mm W x 49 mm H x 3.4 mm D

Samsung ARTIK™ 530/530s (512 MB, 1 GB) mid-range gateway

Secure, fully-integrated IoT solution

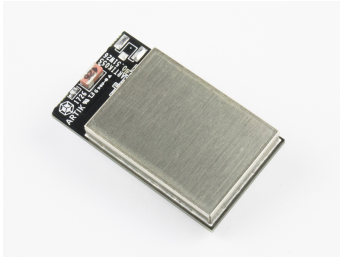
- Industrial and home gateways
- Voice-controlled speakers
- Building zone controllers
- Display-based healthcare monitors

SAMSUNG ARTIK™

Processor	**CPU:** 4x ARM® Cortex® A9 @ 1.2 GHz **GPU:** 3D graphics accelerator
Memory	**DSRAM:** 512 MB/1 GB DDR3 **Flash:** 4 GB eMMC v4.5
Multimedia	**Camera I/F:** 4-lane MIPI CSI up to 5MP **Display:** 4-lane MIPI DSI, HDMI 1.4 a or LVDS (1280 x 720 @ 60 fps) **Audio:** 2x I2S audio input/output
Connectivity	**WLAN (Wi-Fi):** IEEE 802.11 b/g/n single-band SISO **Bluetooth:** 4.2+ Smart **802.15.4:** Zigbee, Thread **Ethernet:** 10/100/1000 Base-T MAC (external PHY required)
Security	Secure element, EAL Level 5, unique device certificate and keys, PKI with mutual authentication to cloud, hardware crypto engine; secure boot*, KMS*, TEE*, ***S-modules**
I/O	GPIO, UART, I2C, SPI, USB Host, USB OTG, HSIC, ADC, PWM, I2S, JTAG
Temperature range	-25° to 85° (°C)
Size	36 mm W x 49 mm H x 3.4 mm D

Samsung ARTIK™ 053/053s, 055s Wi-Fi® edge nodes

Create secure, next-gen edge products

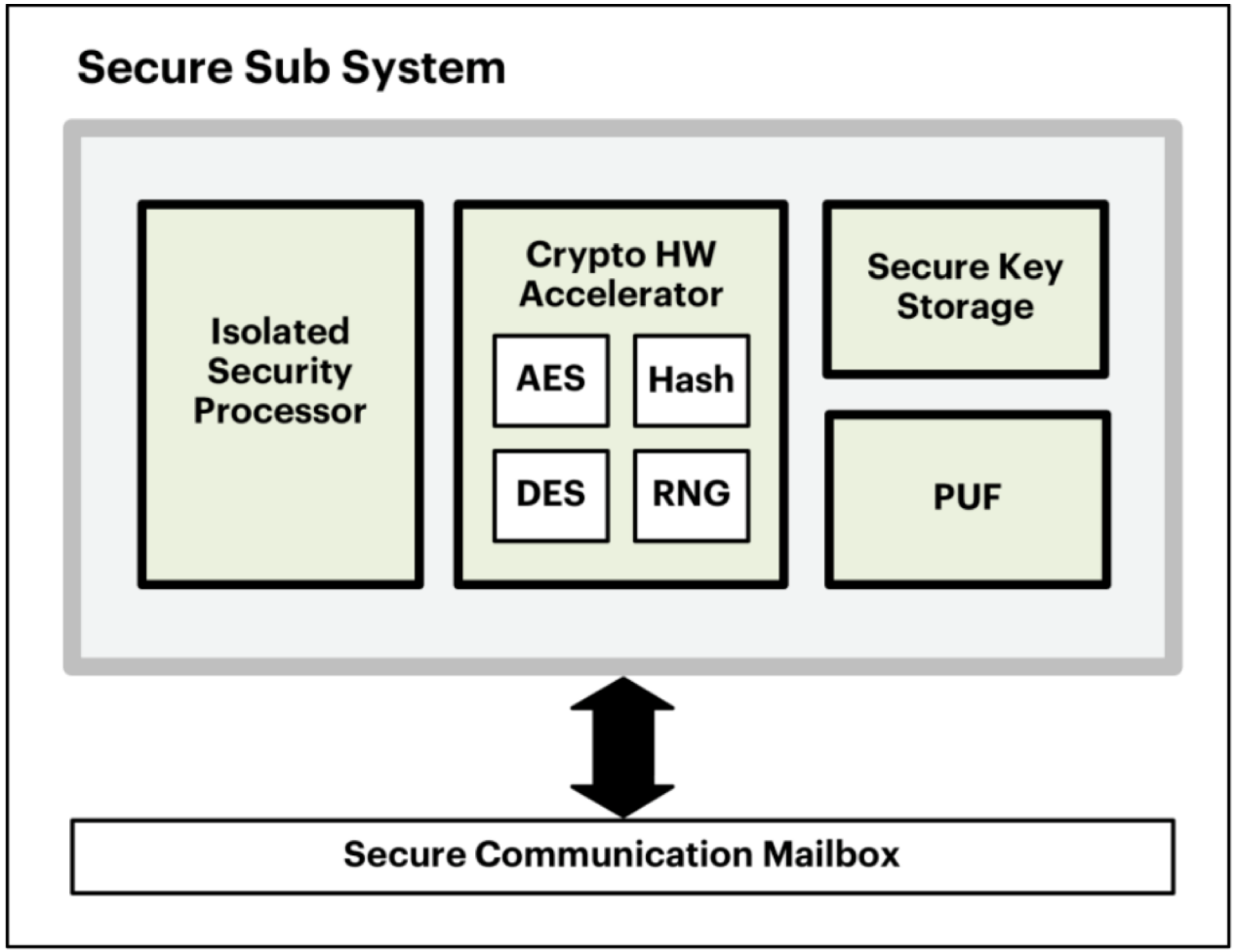


- Home health monitors, AEDs, fitness equipment, CPAP
- Smoke detectors, thermostats, energy monitors, appliances
- Sensors, lighting controllers, motors, valves
- Access control, fire monitors, smart switches

Processor	**Main:** ARM® Cortex® R4 @ 320 MHz **WLAN:** ARM Cortex® R4 @ 480 MHz
Memory	**RAM:** 1.4 MB **Flash:** 8 MB SPI Flash on module
Connectivity	**WLAN (Wi-Fi):** IEEE 802.11 b/g/n
Security	Secure Subsystem, Hardware-protected key storage with secure point-to-point authentication and data transfer, secure boot*, KMS* ***S-versions only**
I/O	2xSPI, 5xUART (2-pin), 4xI2C, 7xPWM, 28xGPIO, 1xJTAG, 4xADC
Operating voltage	**055s:** 3.3 VDC **053, 053s:** 5-12 VDC
Temperature range	-20° to 85° (°C)
Size	**055s:** 15 mm W x 26 mm H x 3.9 mm D **053, 053s:** 15 mm W x 40 mm H x 3.9 mm D

SAMSUNG ARTIK™

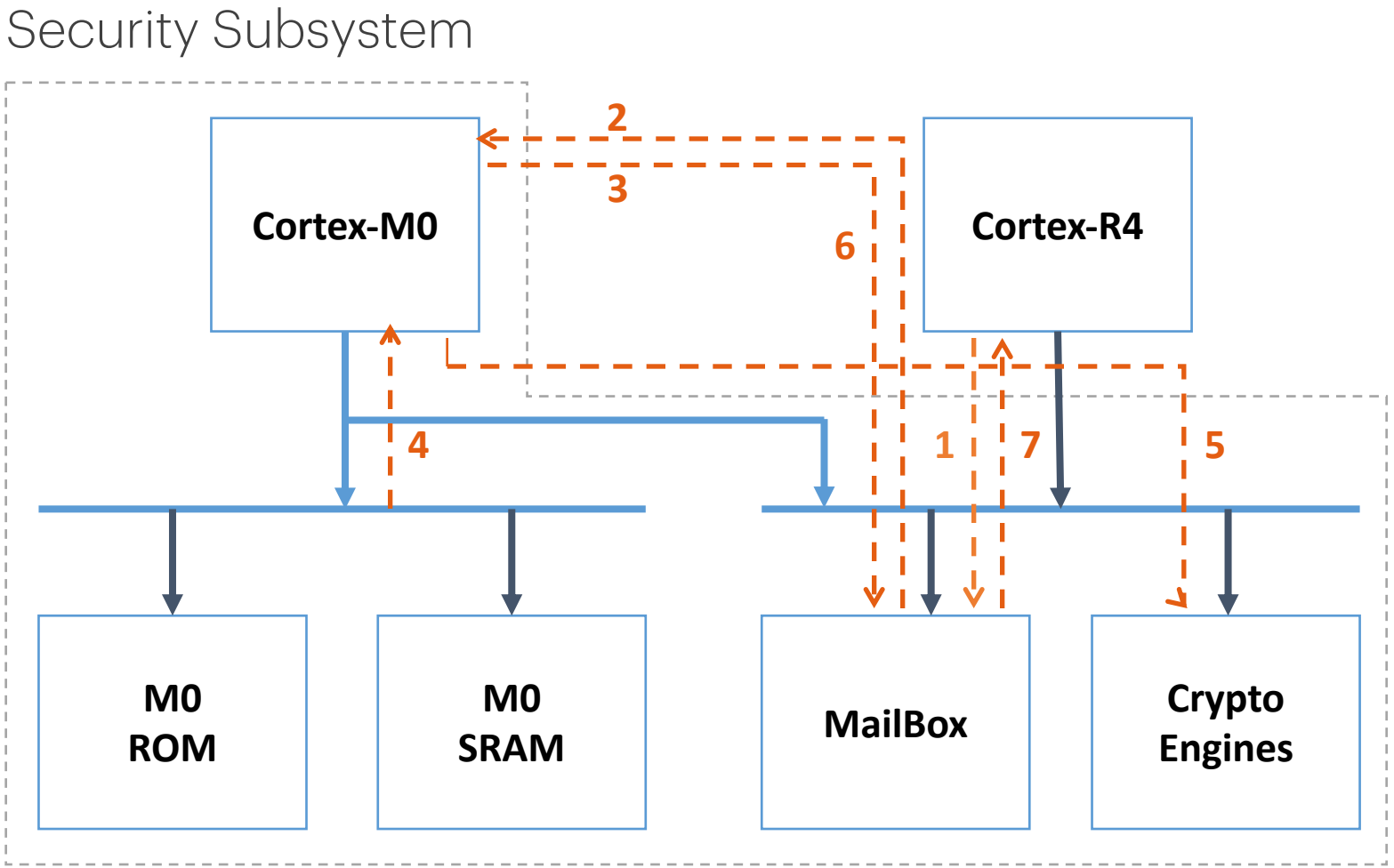
ARTIK 05x Security Subsystem



- Isolated Security Processor
- Cryptographic Hardware Acceleration
- A Physical Uncloneable Function(PUF)
- Secure Key Storage

SAMSUNG ARTIK™

Isolated Security Processor



SAMSUNG ARTIK™

Cryptographic Hardware Acceleration

Support for high performance cryptographic acceleration

- Random Number Generation: DTRNG, PRNG
- Block Cipher: Secure AES, DES
- Hash Function: SHA1/SHA2/SHA3 with HMAC
- Public Key Cryptosystem: RSA, ECDSA, DH, ECDH
- FIPS Compliant: CAVP, CMVP, MDFPP

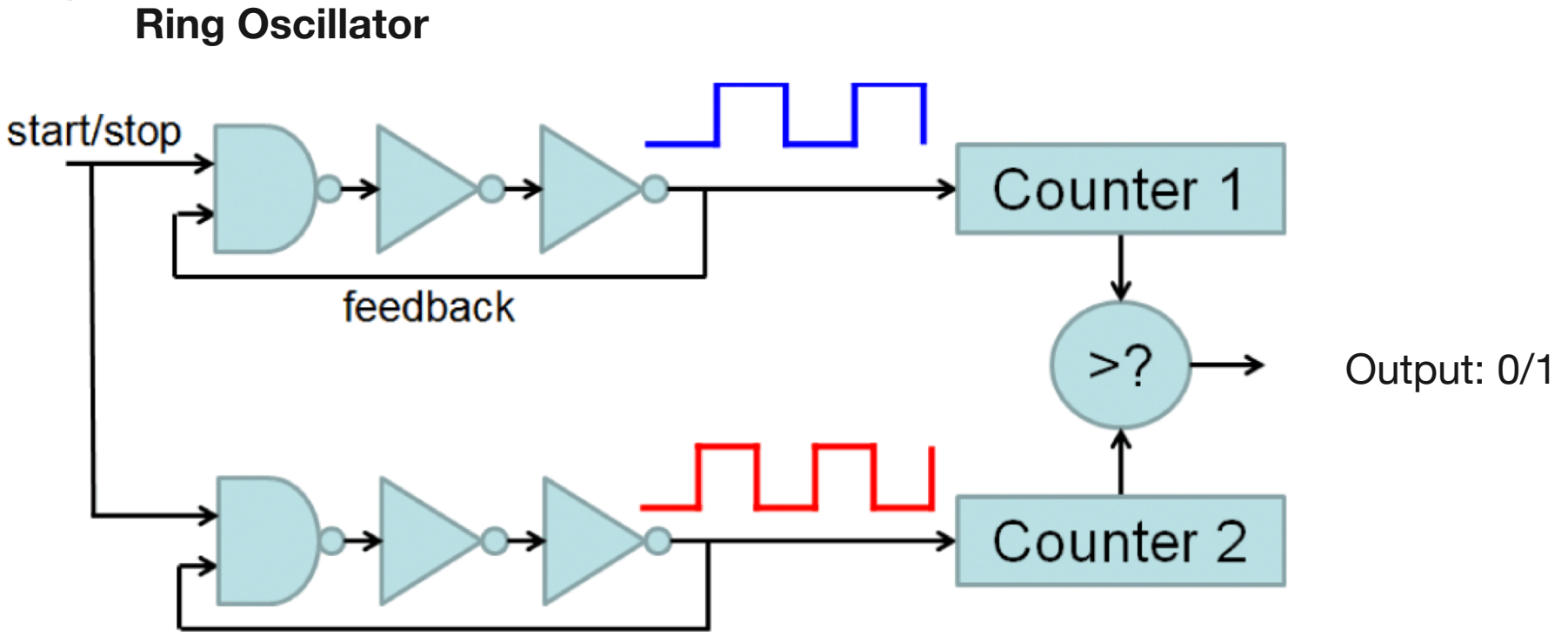
PUF (Physically Unclonable Function)

- Create a cryptographic key(PUF KEY) that can not be cloned by anybody else
  - PUF Key is auto generated using process variation during Manufacturing
  - Unchanging value over product lifetime
  - Unclonable
- Applications of PUF:
  - Device identification
  - Key generation and storage (seed key that never generates the same key)
  - Etc.

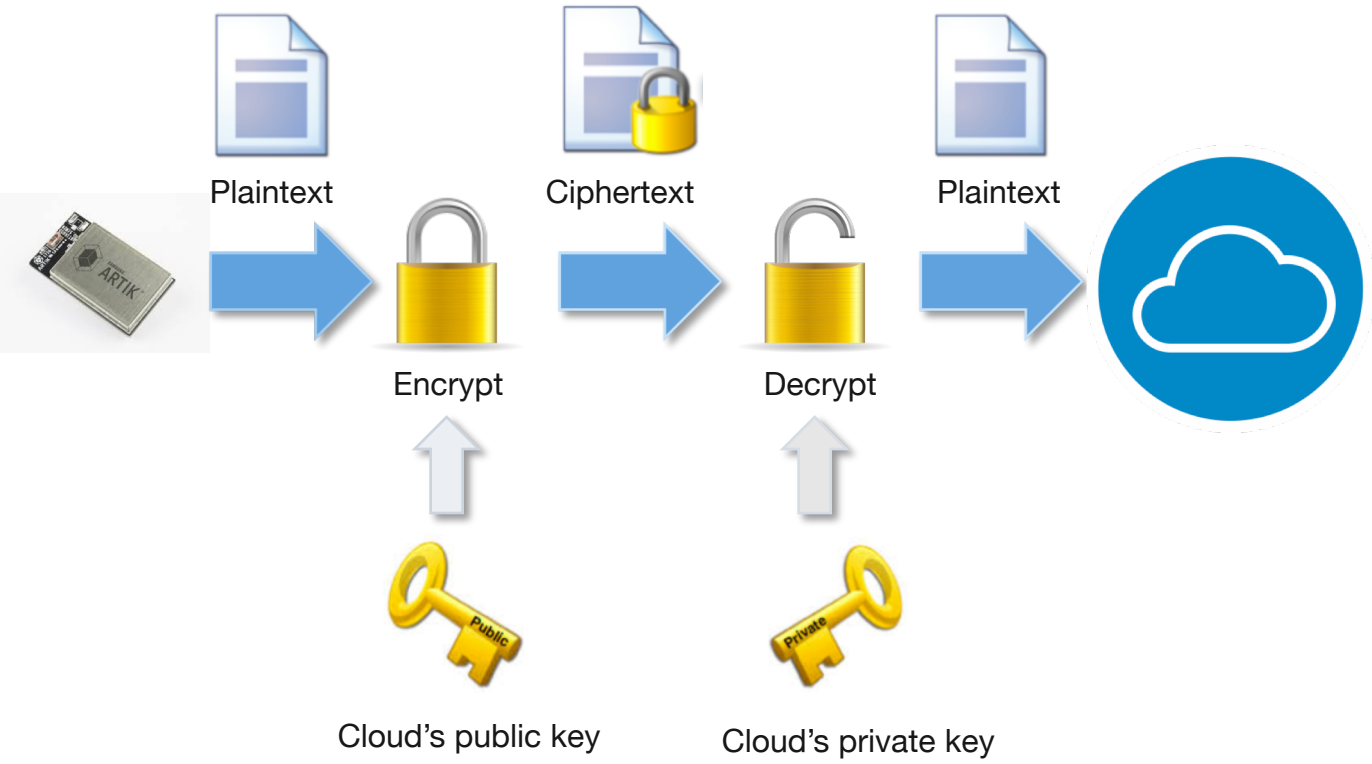
SAMSUNG ARTIK™

RO Frequency PUF

- RO (Ring-Oscillator) frequency is used as the PUF input to generate a unique key for each chip



Public Key Infrastructure (PKI)

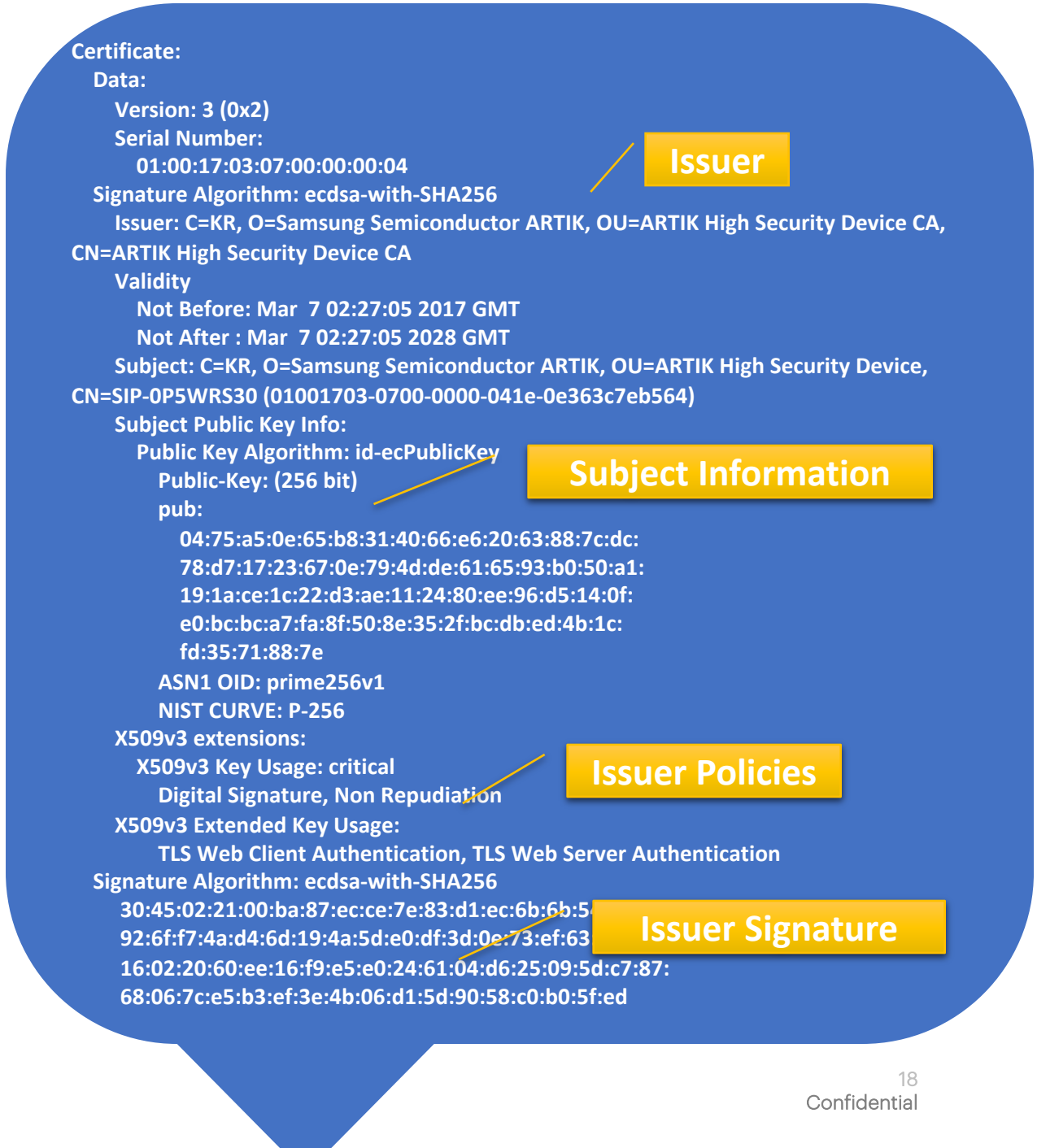


- A Public Key Infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users to securely exchange data over networks
- ARTIK provides PKI, an ARTIK Root CA, which is used to generate and apply unique certificates and key pairs for module/Cloud mutual authentication.

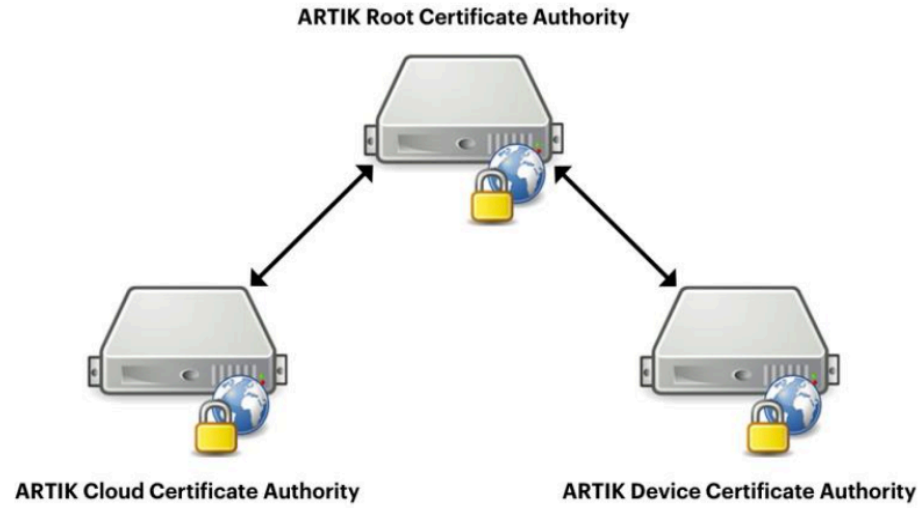
SAMSUNG ARTIK™

Digital Certificate

- PKI's core concept is Digital Certificate
- Issued by a **Certificate Authority,** e.g, GlobalSign, Symantec
- A Digital Certificate contains a public key and an identity (a hostname, or an organization, or an individual)
- X.509 is a standard that defines the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS



Mutual Authentication



- Each ARTIK module is provisioned with:
  - An unique private key
  - Its associated X.509 certificate with a public key. The X.509 certificate is issued as part of the PKI trust hierarchy that roots back to an ARITK Root CA
  - An ARTIK Root CA certificate
- Provision X.509 certificates in the cloud services interacting with ARTIK devices. Server certificates are also issued through a chain rooting back to the same ARTIK Root CA
- At connect time, server and client exchange certificates for mutual authentication

SAMSUNG ARTIK™

Post Provisioning

- To set up a secure connection with a 3rd party Cloud service or implement a secure link between two ARTIK modules, you need to retrieve/generate your own certificate/key-pair.
- We can use ARTIK Security APIs to post provision customer credentials(key, certificate) to Secure Element

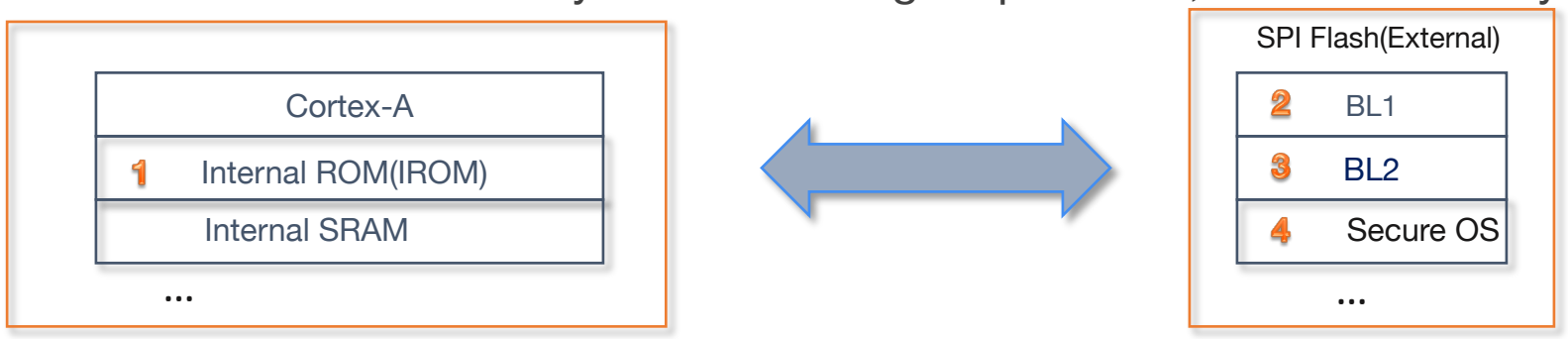
Secure Communication

		ARTIK module (05x, 5, 7)	ARTIK S-module	Comments
Secure communication	**Per device unique key & certificate**	✓	✓	**Uniquely identifies device**
	Key stored in HW secure element	✓	✓	**Secure key storage**
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	**Device talks to authorized cloud and vice versa**
	Post Provisioning		✓	**Provision with your own keys and certificates**
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

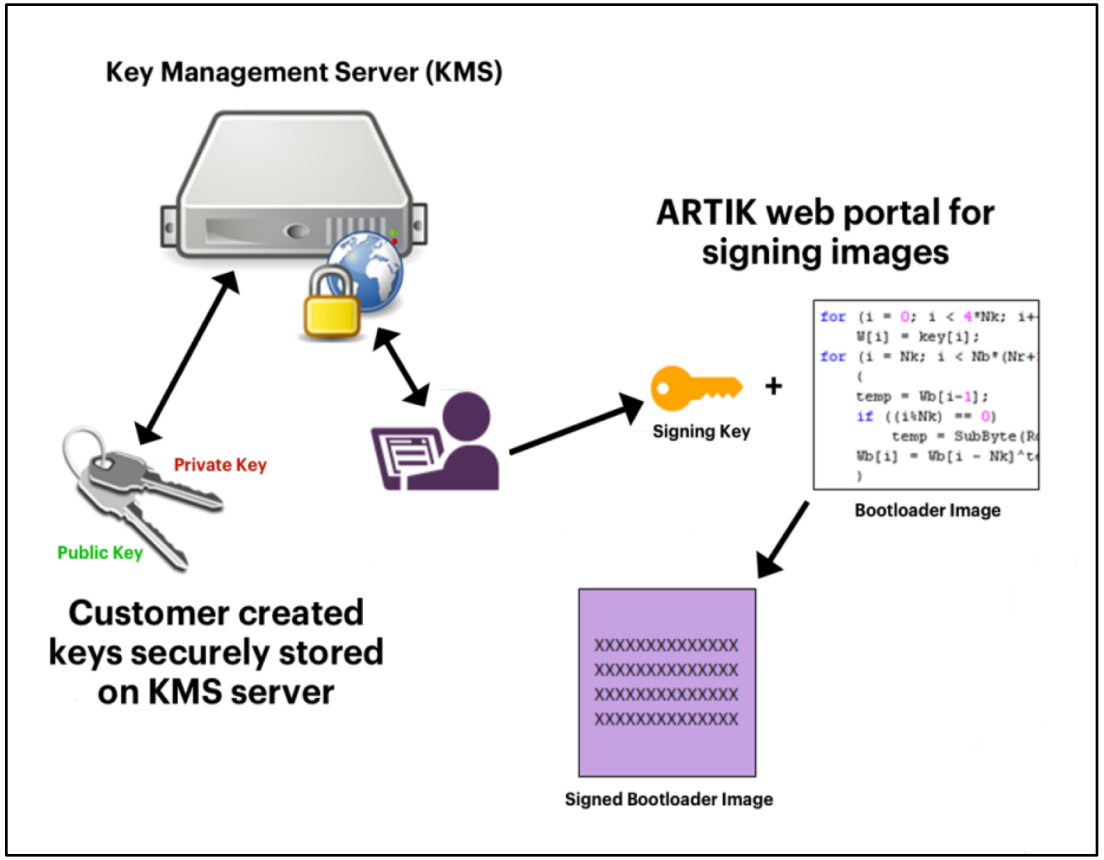
SAMSUNG ARTIK™

Secure Boot

- Secure Boot adds crytographic checks to each stage of the boot process.
- Boot Sequence: (ARTIK 5/7 as an example)
  1. Start to execute BL0 code at 0x0000.0000, where the internal ROM (IROM) is mapped to.
  2. IROM loads the first stage bootloader, BL1, verifies its integrity and signing hash of BL1 binary. BL1 turns Secure System core on and loads the Secure System F/W binary to it.
  3. Then, BL1 verifies the second stage bootloader BL2 binary and jumps to BL2 to boot.
  4. BL2 verifies secure OS binary before booting it up. In turn, OS can securely boot an application.



Key Management System(KMS)

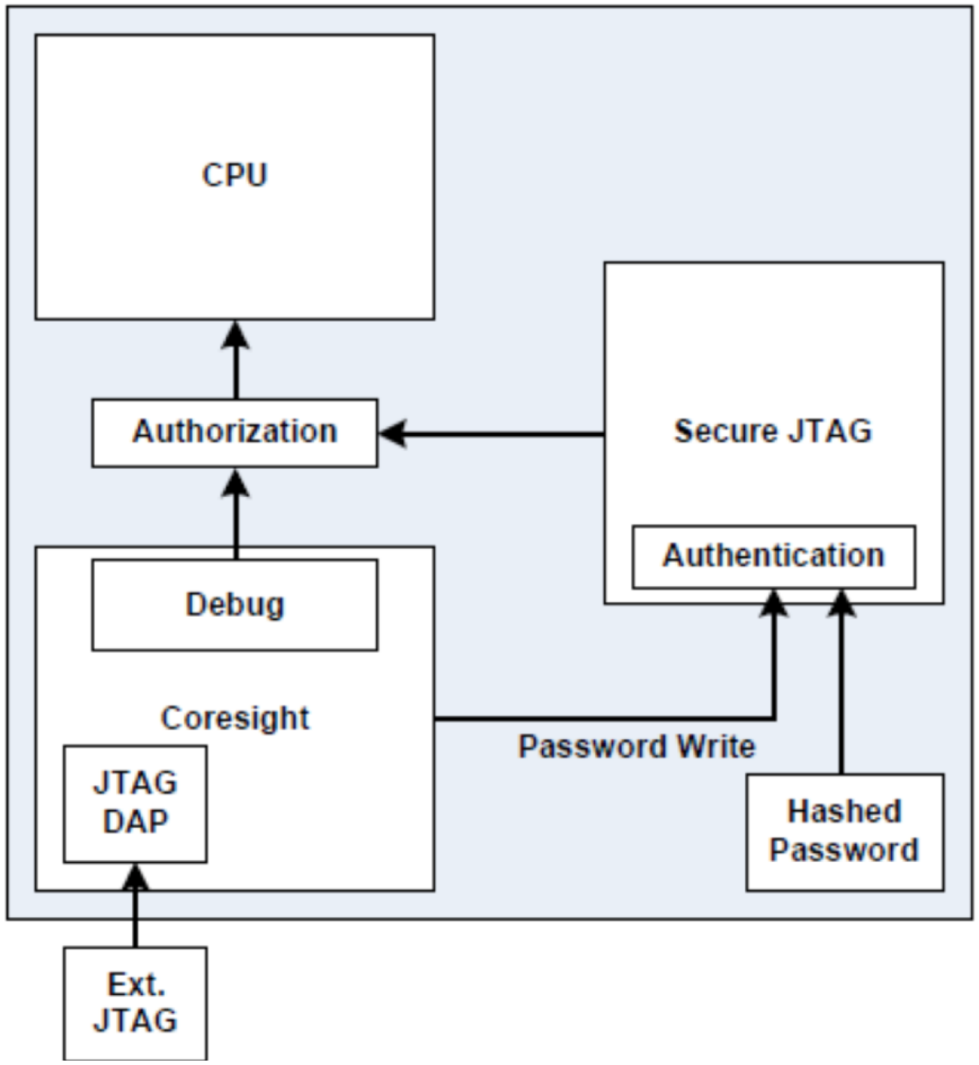


- Images are signed through a highly secure cryptography standard (SHA256wRSA2048)
- Signing keys are stored and operated within FIPS 140-2 certified Hardware security modules (HSM)
- Strict access control policies.
- Accessed through a web portal from only whitelisted IP only

SAMSUNG ARTIK™

Secure JTAG

- Secure JTAG authenticates and authorizes JTAG access
- It requires a password to gain access to the JTAG chain. The password is based on the serial number of module
- The information is only made available through an authorized request to Samsung.

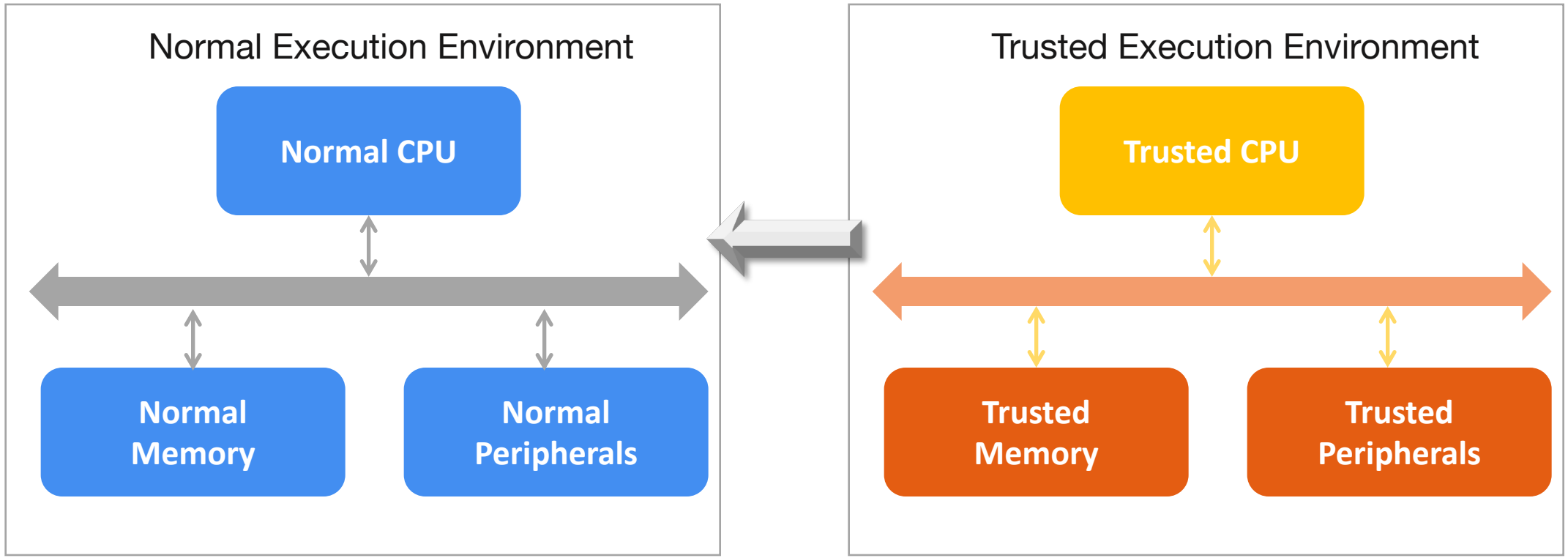


Device Protection

		ARTIK module (05x, 5, 7)	ARTIK S-module	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	**KMS infrastructure for code signing**		✓	**Key Management Service**
	Code verification key in HW		✓	**Secure key storage**
	Secure boot (check for authorized code)		✓	**Boot image verification**
	JTAG access locked		✓	**Lock out debug access**
Data protection/ Secure storage	Secure OS (separate normal & secure operations)		✓	Hardware enforced secure applications via TEE
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt
	Secure storage		✓	Encrypt data stored on Flash

SAMSUNG ARTIK™

Trusted Execution Environment(TEE)

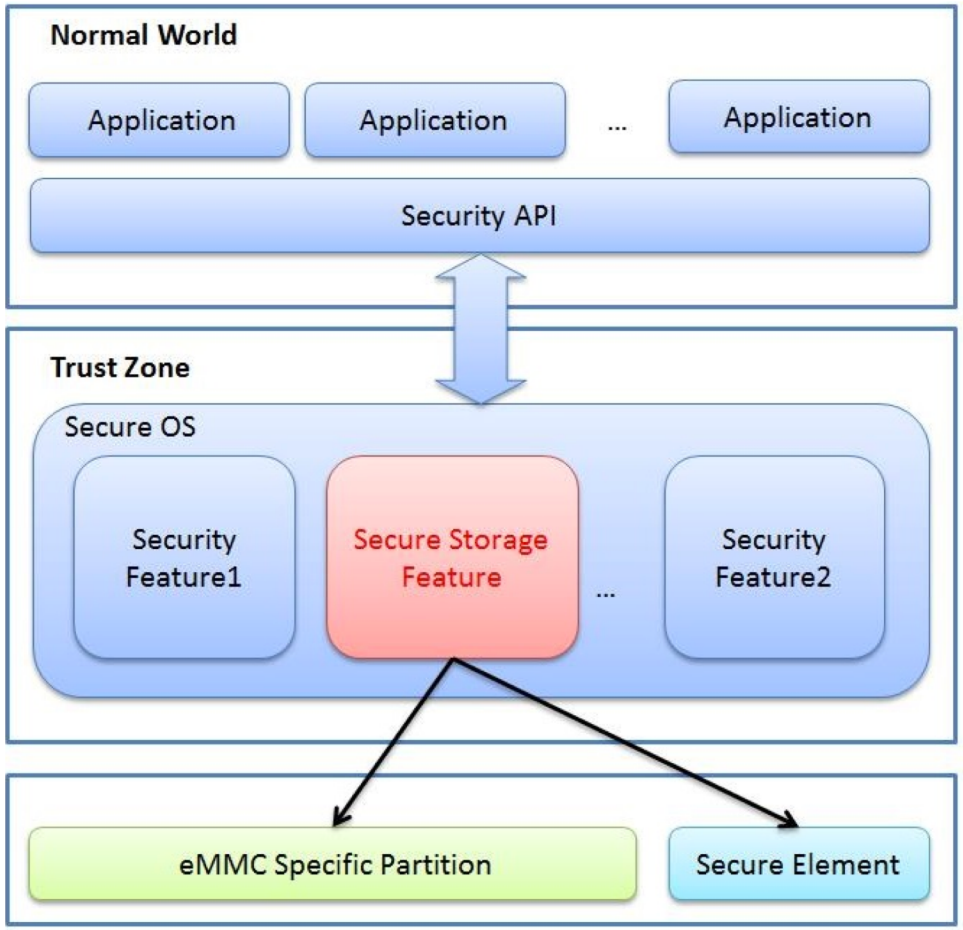


- ARTIK 5 and 7 module families support Trusted Execution Environment(TEE)
- Samsung TEE implementation is based on ARM TrustZone hardware architecture
- TEE provides a fully-isolated and secured operation environment

SAMSUNG ARTIK™

Secure Storage

- eMMC file system (Flash-based)
  - Uses the same storage as the normal operating system. However, a specific partition is managed by the TrustZone-based Secure OS.
  - All data in this partition is encrypted with a unique key generated at run time, and is stored as a file unit of 32KB with a maximum of 1024 files that may be stored.
- Secure Element – an isolated storage device that supports the storage of up to 16 AES 128-bit keys.
  - The Secure Element provides high levels of security as hardware with anti-tamper measures.
  - All communication from the Secure Element to the processor is secured and encrypted.



SAMSUNG ARTIK™

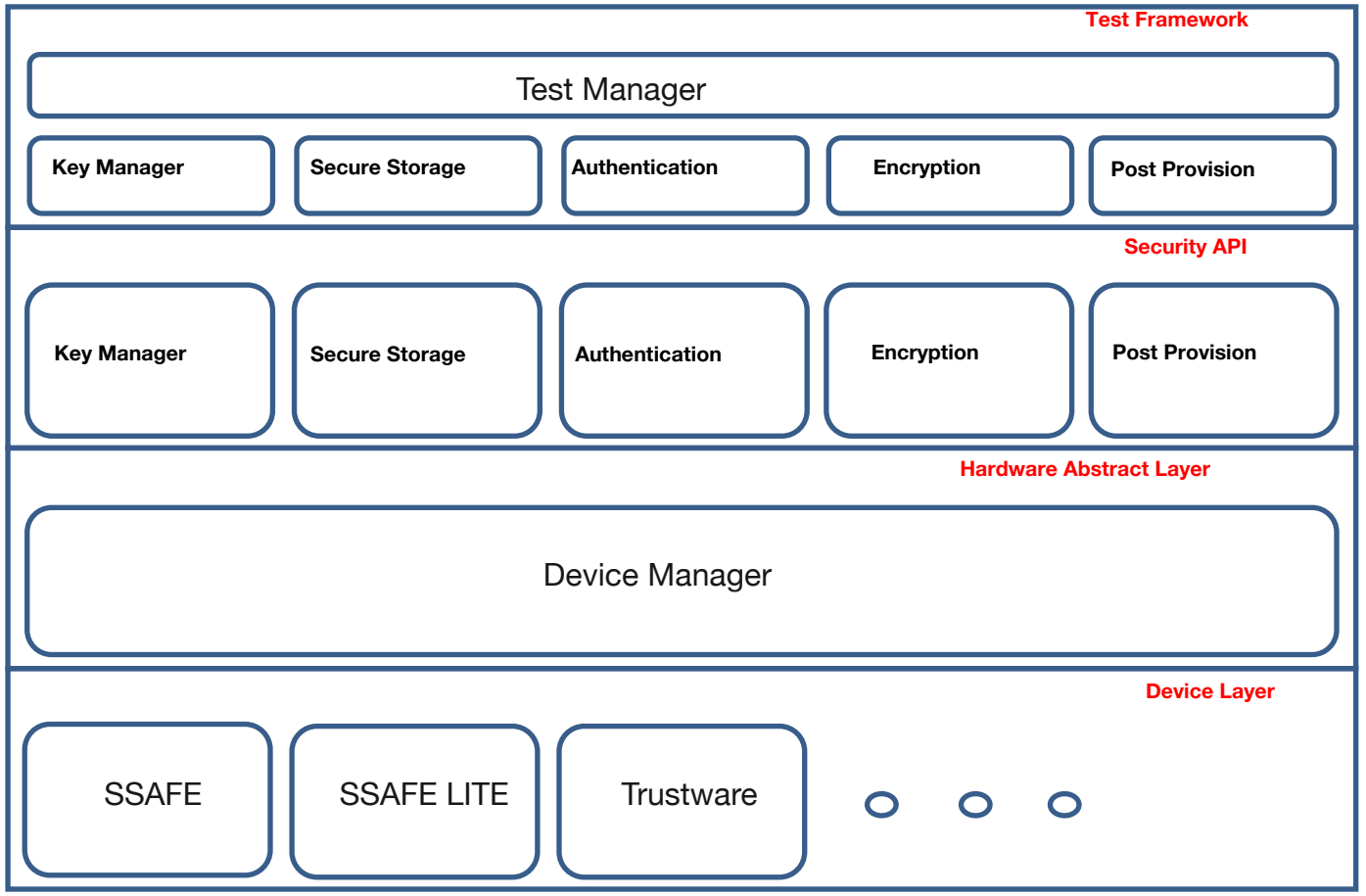
Secure Element

- The Secure Element provides services for the secure storage of cryptographic material and other protected content.
- It includes cryptographic services such as random-number generation, key/data secure storage, and certificates handling and processing.
- Secure Element uses Smart Shield, Smart Sensor, Smart Core technologies to achieve the highest level of security and protection.
- The Secure Element meets the Common Criteria (CC) certification for security and for Evaluation Assurance Level (EAL) 5.

ARTIK Security APIs

ARTIK SDK provides APIs for accessing the secure resources managed by the Secure OS.

- **Key Manager:** Provides APIs to generate, setup, and remove keys
- **Certificate Manager:** Provides APIs to generate, manage, and verify certificates and signatures
- **Crypto Manager:** Provides APIs for AES and RSA encryption and decryption
- **Secure Storage Manager:** Provides APIs for initializing and managing the secure storage
- **Post Provision:** Provides APIs for injecting and provisioning a certificate and key into Secure Element



SAMSUNG ARTIK™

Security APIs

Category	ARTIK API	Description
Initialize	see_init	
	see_deinit	
Key Management	see_generate_key	generate symmetric and asymmetric keys(AES, ECC Curve, HMAC type)
	see_set_key	set external symmetric and asymmetric key to secure storage
	see_get_pubkey	get public key of asymmetric key from secure storage
	see_remove_key	remove a key from secure storage
Authentication	see_generate_random	Generate a random number
	see_generate_certificate see_set_certificate see_get_certificate	Generate, set and get a certificate
	see_get_rsa_signature see_verify_rsa_signature see_get_ecdsa_signature see_verify_ecdsa_signature	Get , verify signature using RSA, ECDSA algorithm
	see_get_hash,see_get_hmac	Hash Messages
	see_generate_dhparams(ecdhkey)	

Security APIs

Category	ARTIK API	Description
Secure Storage	see_read_secure_storage	Read data from secure storage
	see_write_secure_storage	Write data to secure storage
	see_delete_secure_storage	Remove data from secure storage
	see_get_size_secure_storage	Get data size from secure storage
	see_get_list_secure_storage	List data in secure storage
Post Provision	see_post_provision	Injecting an HMAC key or asymmetic key pair(ECC/RSA) into the secure element
	see_post_provision_lock	
Encryption/Decryption	see_aes_encryption see_aes_decryption	AES Encryption/Decryption
	see_rsa_encryption see_rsa_decryption	RSA Encryption/Decryption

Device Protection

		ARTIK module (05x, 5, 7)	ARTIK S-module	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to authorized cloud and vice versa
	Post Provisioning		✓	Provision with your own keys and certificates
Device protection/ secure code execution	KMS infrastructure for code signing		✓	Key Management Service
	Code verification key in HW		✓	Secure key storage
	Secure boot (check for authorized code)		✓	Boot image verification
	JTAG access locked		✓	Lock out debug access
Data protection/ Secure storage	**Secure OS (separate normal & secure operations)**		✓	**Hardware enforced secure applications via TEE**
	Security Lib API (27 API calls)	Limited(random number generator, get cert and signature)	✓	**Key Manager, Authentication, Secure Storage, Post Provisioning, Encrypt/Decrypt**
	Secure storage		✓	**Encrypt data stored on Flash**

SAMSUNG ARTIK™

Samsung ARTIK™ Security Features by Portfolio

		020	030	053	520	530	710	021s	053s	055s	305s	310s	530s	710s
Secure communication	Per device unique key & certificate			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Secure element key storage			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	PKI			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Protection/ secure code execution	KMS								✓	✓	✓	✓	✓	✓
	Code verification key in HW							✓	✓	✓	✓	✓	✓	✓
	Secure boot							✓	✓	✓	✓	✓	✓	✓
	JTAG access locked								✓	✓	✓	✓	✓	✓
Data protection/ Secure storage	Secure OS (TEE)										✓	✓	✓	✓
	Limited Security Credential Access API			✓	✓	✓	✓							
	Full Security Lib API w/ crypto.								✓	✓	✓	✓	✓	✓
	Secure storage								✓	✓	✓	✓	✓	✓

SAMSUNG ARTIK™

Platform Security

SAMSUNG ARTIK™

End-to-End Security

- Secure Device Registration: ARTIK Cloud services support secure device registration for communicating securely to devices.
  - The device is genuine
  - Every message exchanged between the device and ARTIK cloud services is verified
  - Use TLS for mutual client/server authentication
- Secure OTA:

Samsung ARTIK™ End-to-end Platform Security*

	Feature	ARTIK
Modules	Secure element key storage, secure boot	Included
	Security infrastructure: PKI and KMS	Included
	Unique device ID and certificate	Included
	Secure data storage with data encryption	Included
Platform software	Secure device registration	Included
	Secure OTA updates	Included
Cloud Infrastructure	Supports HIPAA compliant solutions	Included
	OWASP top 10	Included
	Internal and external security audits	Included
Cloud services	AAA (Authentication, Authorization, Accounting)	Included
	API Security	Included
	3rd party device discovery and mutual authentication	Included
	Data privacy management, identity, permissions,	Included
Communications	TLS, VPN	Included
	DTLS Application level security; BLE session security	Included
Applications	Key and secure app data encryption and storage	Included
	2-factor authentication; OAuth; client side certificates	Included

SAMSUNG ARTIK™

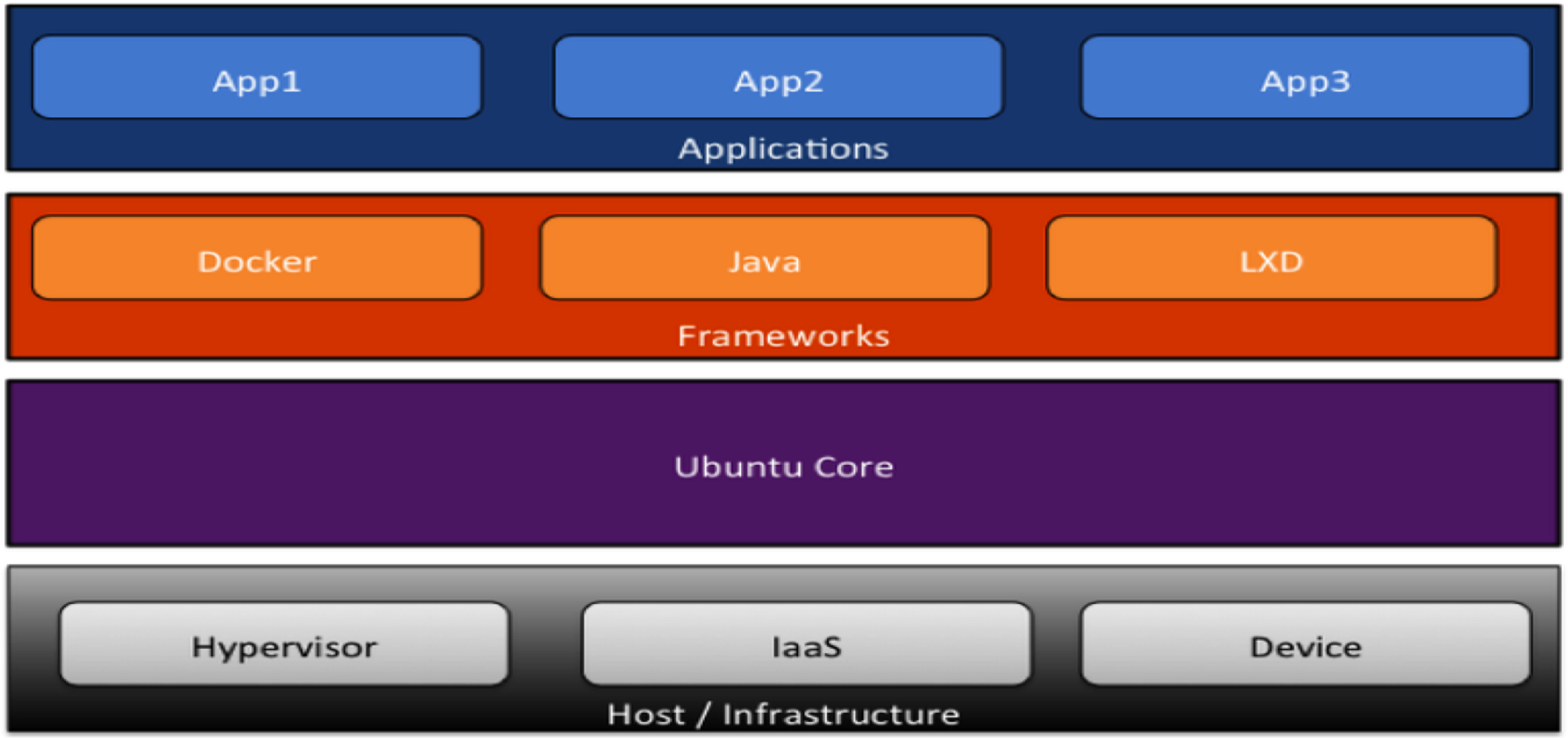
* Feature list is not exhaustive

OS Transition
To Ubuntu

Why Ubuntu OS?

- Security
- Product Life Cycle Management

Ubuntu OS

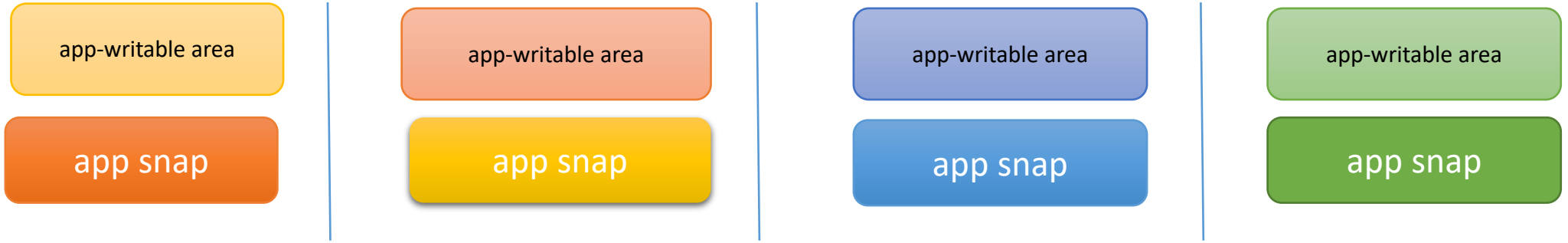


- Ubuntu Core is a tiny, transactional version of Ubuntu for IoT devices
- It is faster, more reliable, and offers stronger security guarantees
- Transactionally updated Ubuntu for devices and Cloud
- A new, simpler application packaging system, called **SNAP**.

SAMSUNG ARTIK™

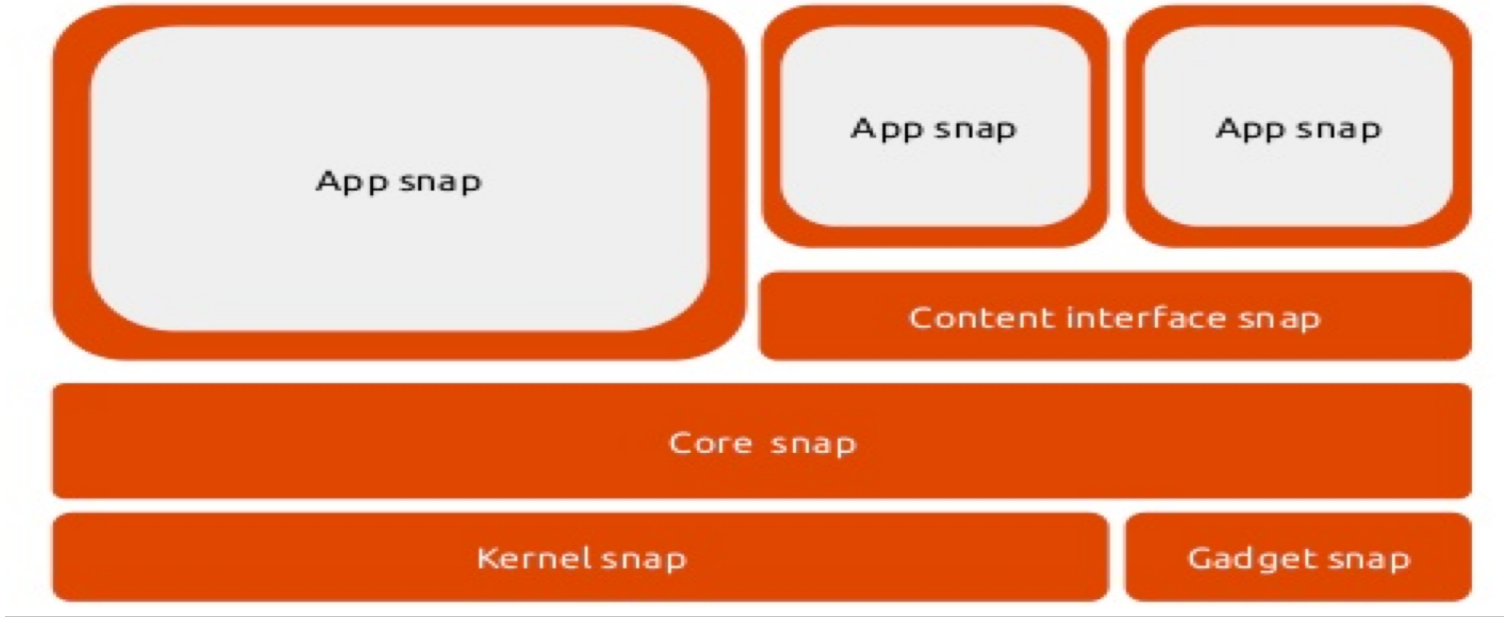
Ubuntu OS

- Apps are contained and isolated
  - System is read-only(even app code)
  - App can’t even read other’s app’s files
  - Fine grained control
  - No script running as root when installed or removed.



SAMSUNG ARTIK™

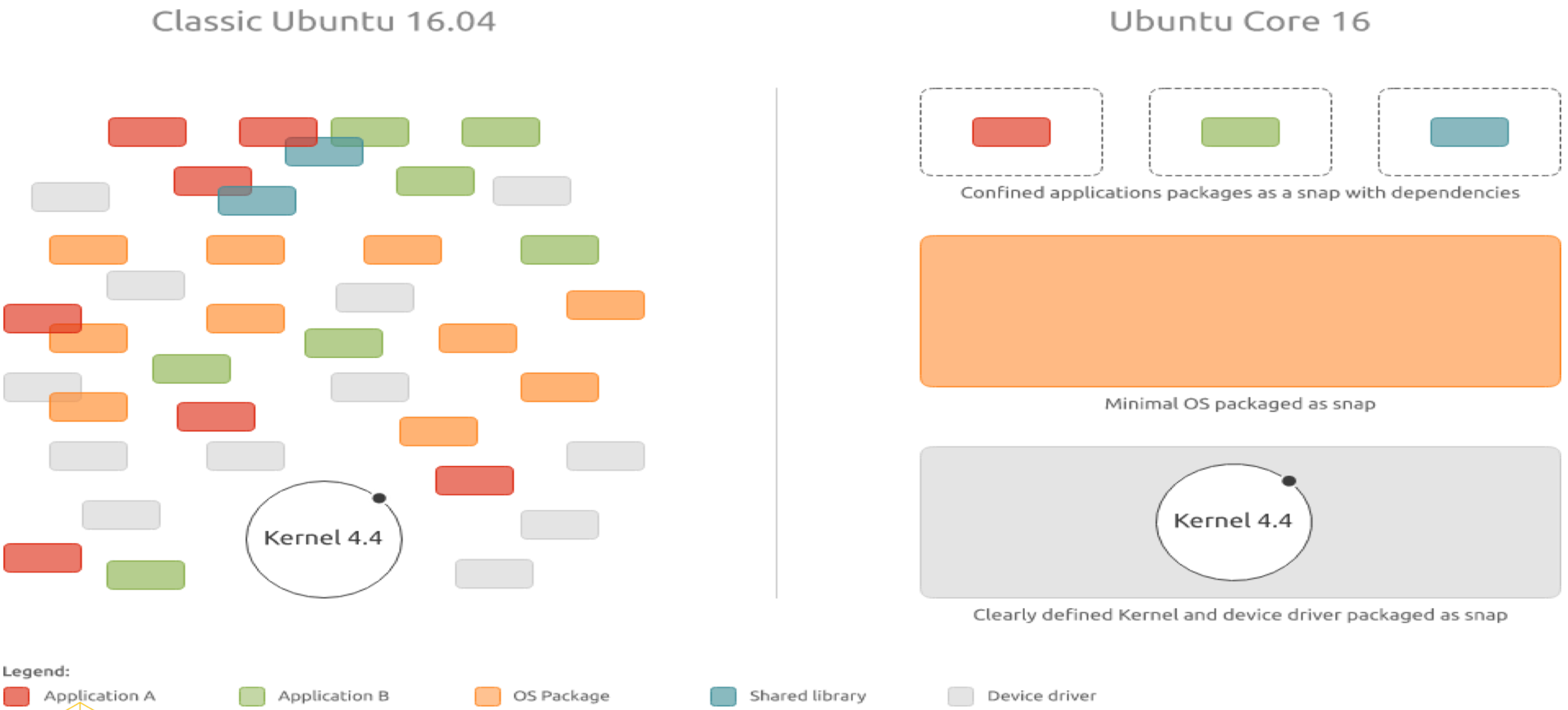
Ubuntu OS



Ubuntu Core has an all-snaps architecture, where all tiers are provided as snaps, including the OS and kernel.

- Any snap can be upgraded and rolled back independently and automatically
- App snap ships all their dependencies.

Ubuntu OS



Source: www.ubuntu.com

Ubuntu OS on ARTIKs

- Ubuntu 16.04 LTS is supported on ARTIK 5/7 families of modules
- Developer support for numerous connectivity options, including WiFi, Zigbee, Bluetooth, audio, video and graphical framework
- Integrated with ARTIK IDE/SDK

APPENDIX