Samsung ARTIK Overview
Easy, interoperable, secure IoT

Wei Xiao

May 2, 2018

SAMSUNG ARTIK™

Agenda

- ARTIK Overview
- ARTIK End to End Solution
- ARTIK 05x Module
- ARTIK Security
- Demo, Hands-On
- Q & A

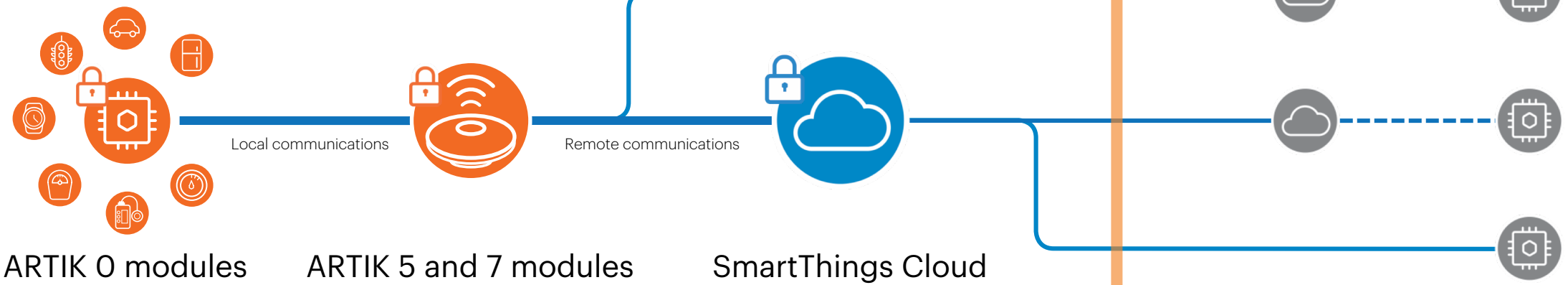
SAMSUNG ARTIK™

Samsung ARTIK™ IoT Platform

End-to-end integration...

...Open and interoperable

ARTIK Security
Secure hardware modules, cloud infrastructure,
local and remote communications



ARTIK 0 modules
Edge nodes,
low-power devices
smart appliances

ARTIK 5 and 7 modules
Gateways, hubs,
high-value devices

SmartThings Cloud
ARTIK cloud services include:
Interoperability, Orchestration,
Over-the-air updates,
Analytics and insights,
Monetization

ARTIK Ecosystem
Consulting services, products, technologies
and specialized assistance

Integrate with existing IoT infrastructure,
third-party devices and clouds including
AWS, Azure, etc.

SAMSUNG ARTIK™

ARTIK End to End Solution

SAMSUNG
ARTIK™

ARTIK Module Family

Samsung ARTIK module product family

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

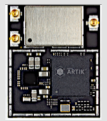
15 x 26 x 3.9
3.3 VDC

- Single, dual Cortex-M, Cortex-R CPUs
- RTOS based OS

ARTIK 5, and 7 Modules

Hubs and gateways

520 | 530 | 530s | 530s_1G | 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-A CPUs
- Linux based platforms

SAMSUNG ARTIK™

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 Security: ARM Cortex M0
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™

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	**DRAM:** 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™ 710/710s high-end gateway

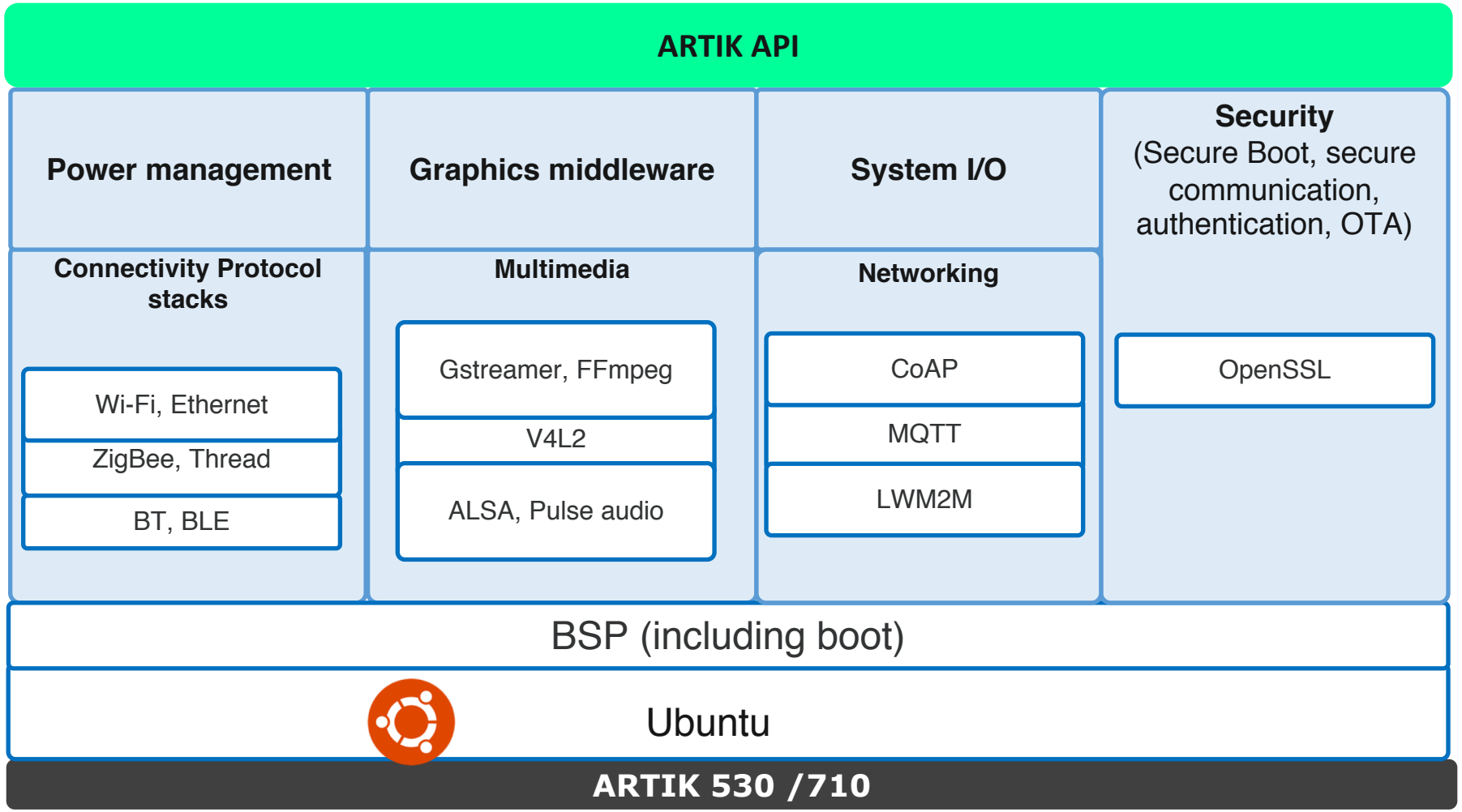
Secure, fully-integrated IoT solution

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

SAMSUNG ARTIK™

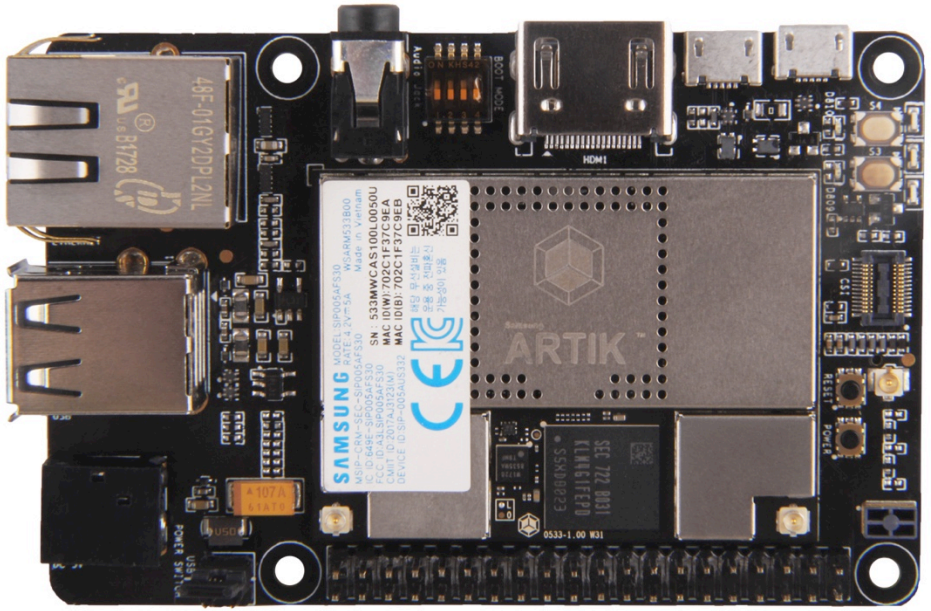
Processor	**CPU:** 8x ARM® Cortex® A53 @ 1.4 GHz **GPU:** 3D graphics accelerator
Memory	**DRAM:** 1 GB DDR3 @ 800 MHz **Flash:** 4 GB eMMC v4.5
Multimedia	**Camera I/F:** 4-lane MIPI CSI **Display:** 4-lane MIPI DSI up to FHD@24 bpp, LVDS, HDMI v1.4 **Audio:** I²S audio interface
Connectivity	**WLAN (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

ARTIK 5x/7x Software Stack



SAMSUNG ARTIK™

Reference Design: Seeed Eagleye 530s



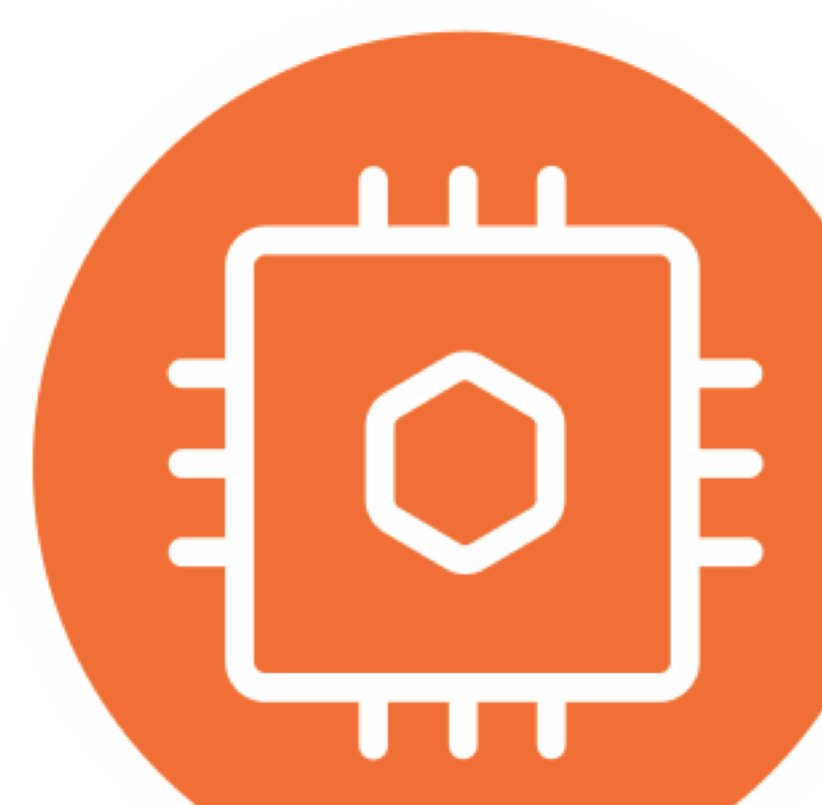
- Powered by the Samsung ARTIK™ 530s module, Raspberry-Pi form factor
- Incorporates ARTIK 530s 1GB SoM, a Quad Core Cortex® A9 running @ 1.2 GHz.
- Includes 40 pin GPIO and accessory interface.
- Support for Micro SD, Ethernet 10/100/1000, Wi-Fi 802.11 a/b/g/n, Bluetooth BLE 4.2 802.15.4, and ZigBee/Thread.
- Supports full HDMI, MIPI camera interface, video, and audio media.

SAMSUNG ARTIK™

Samsung ARTIK™ Modules
Create intelligent, connected devices

Production-ready, secure edge nodes and system-on-modules tightly integrated with ARTIK cloud interoperability and serviceability services

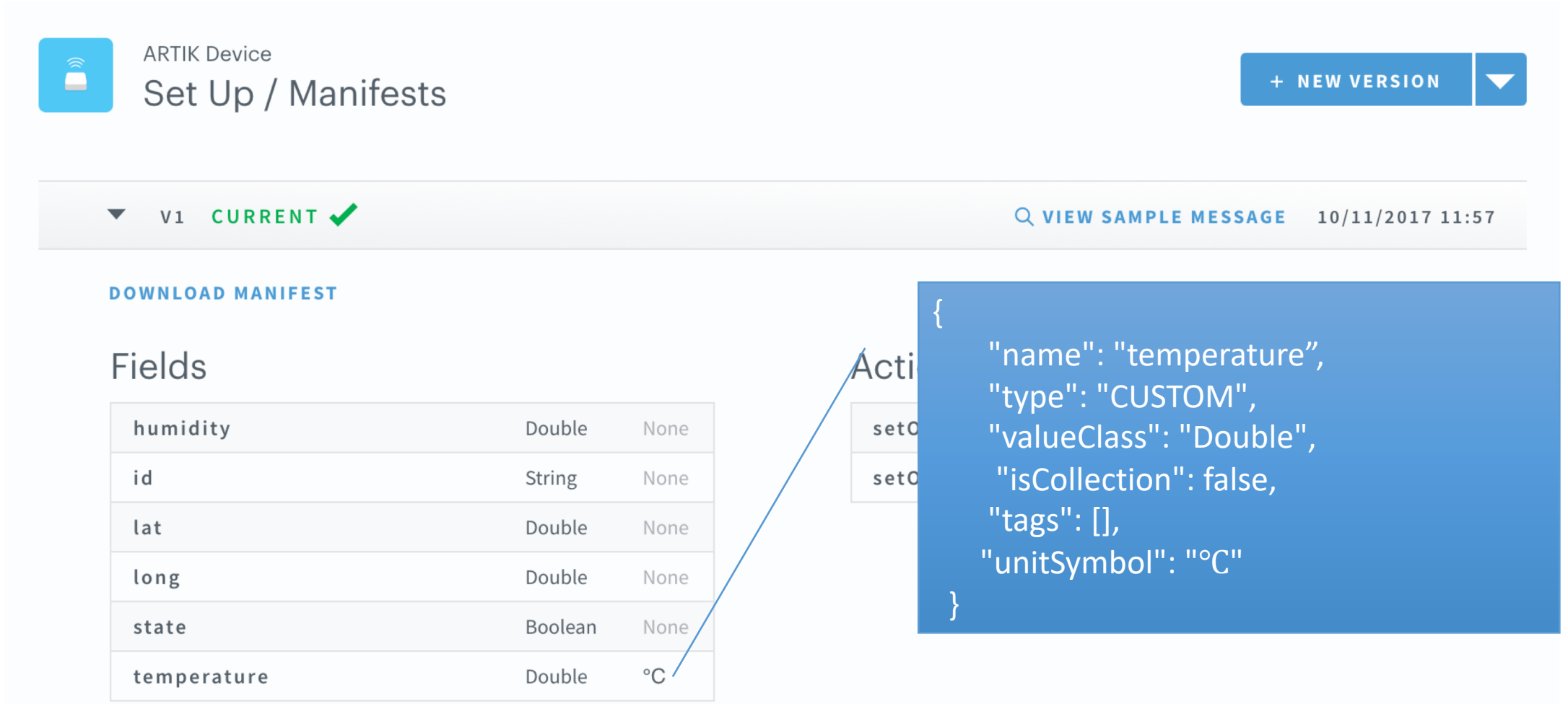
- Production-Ready
- Pre-certified wireless functionality and protocols
- Pre-integrated, fully-tested OS and middleware
- Integrated hardware and software security (s-versions)
- Scalable production volumes



SAMSUNG ARTIK™

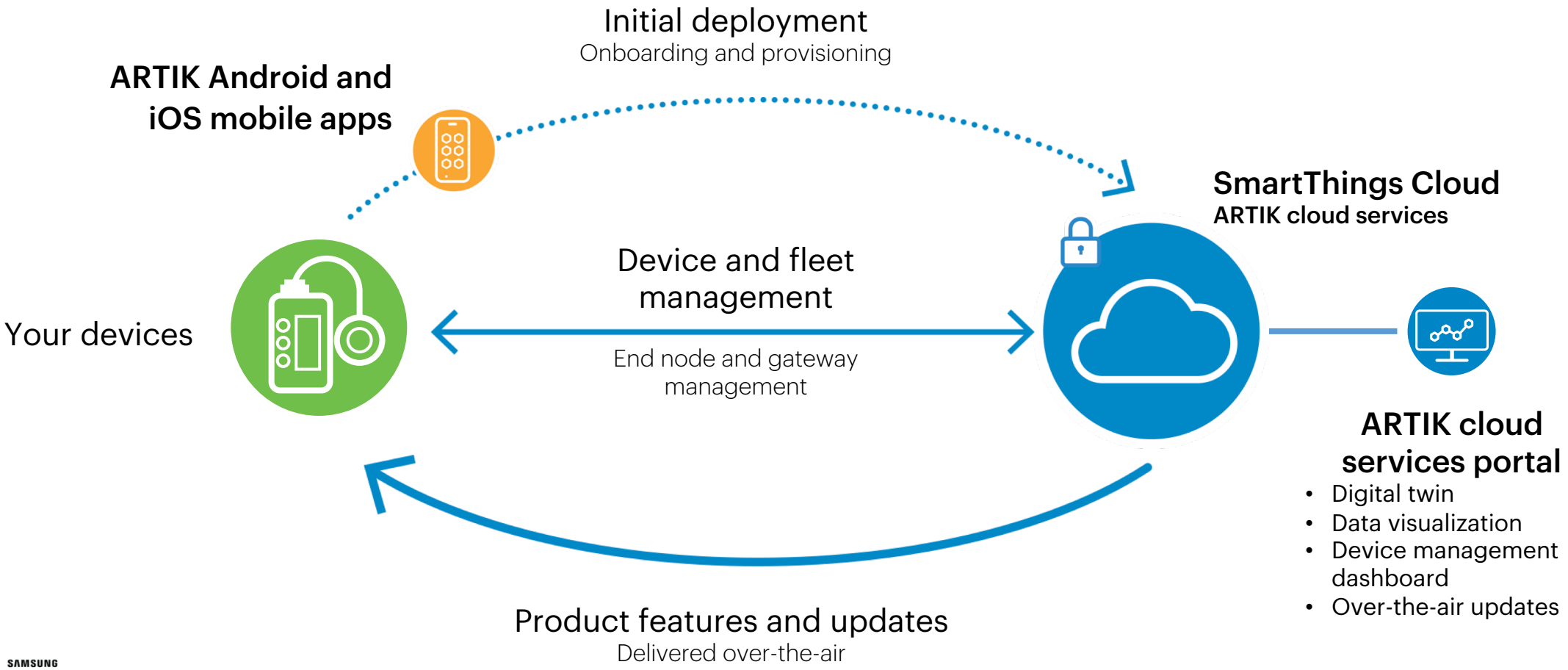
ARTIK Cloud service

Device Type, Manifest



Samsung ARTIK™ Device management and OTA

Onboard, manage, and service devices in the field

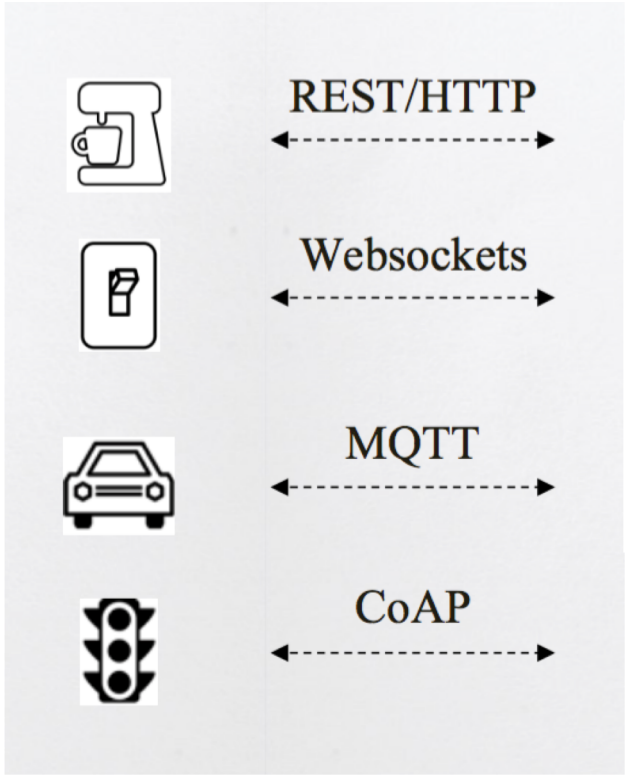


SAMSUNG ARTIK™

Platform / Cloud Software Development

Platform Development:

- 02x/03x: Simplicity Studio
- 05x/5/7: ARTIK SDK / IDE
- Other Options for 5/7 series



Cloud Development:

Easy to use open APIs

10 Mobile & platform SDKs

Developer Portal

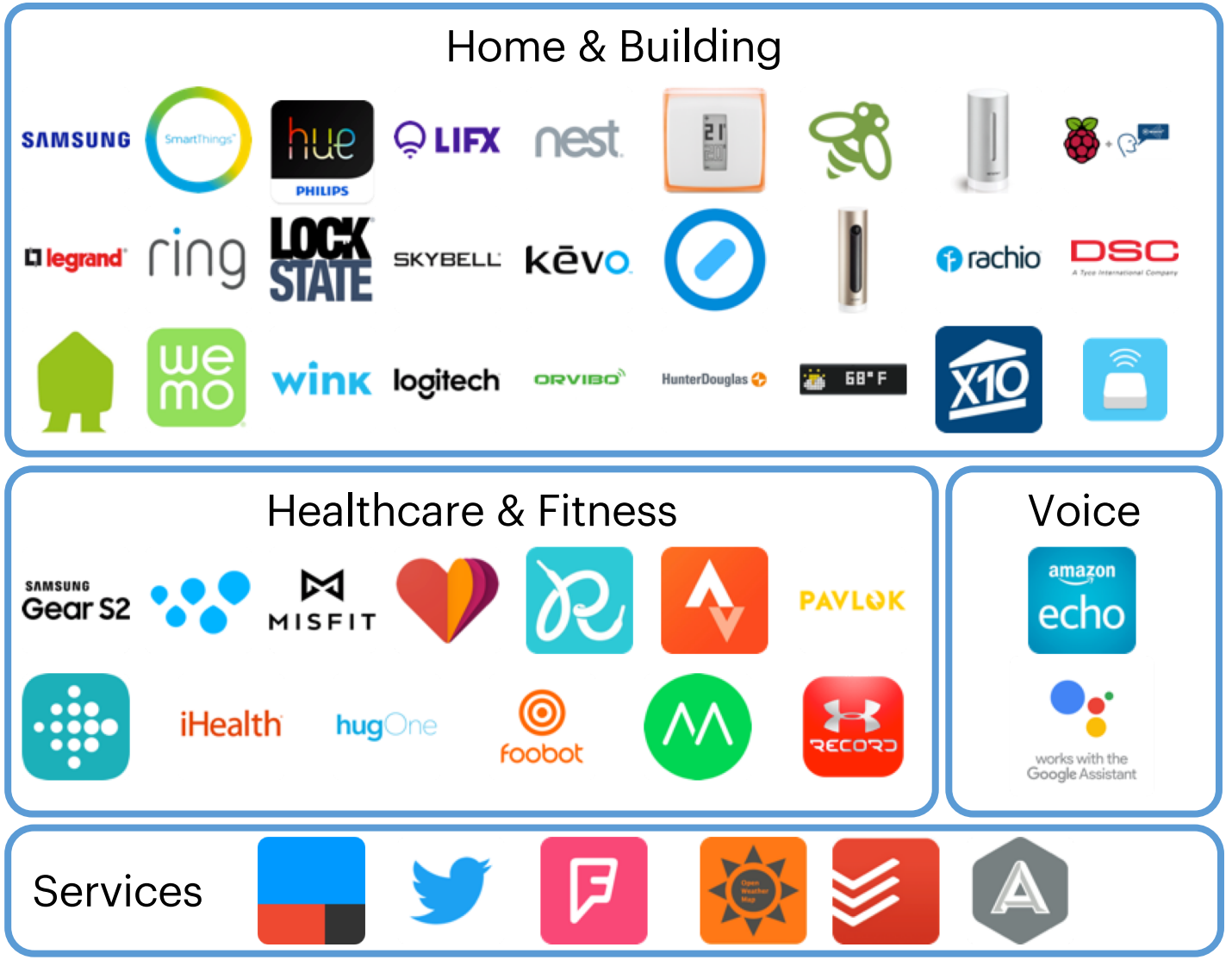
API Console

Device Simulator

Samsung ARTIK™ cloud connectors

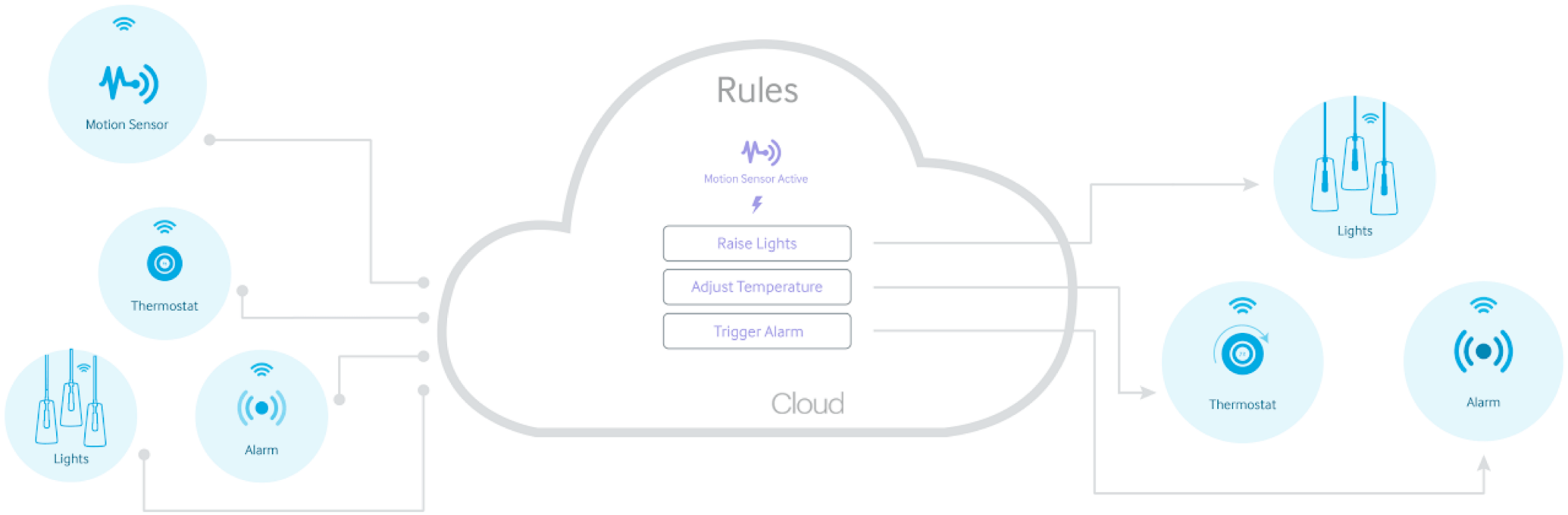
Expanded IoT solutions

- Connect to Samsung and third-party devices, clouds, and apps
- 50+ built-in and verified by Samsung
- Open technology: 100's available from ARTIK community

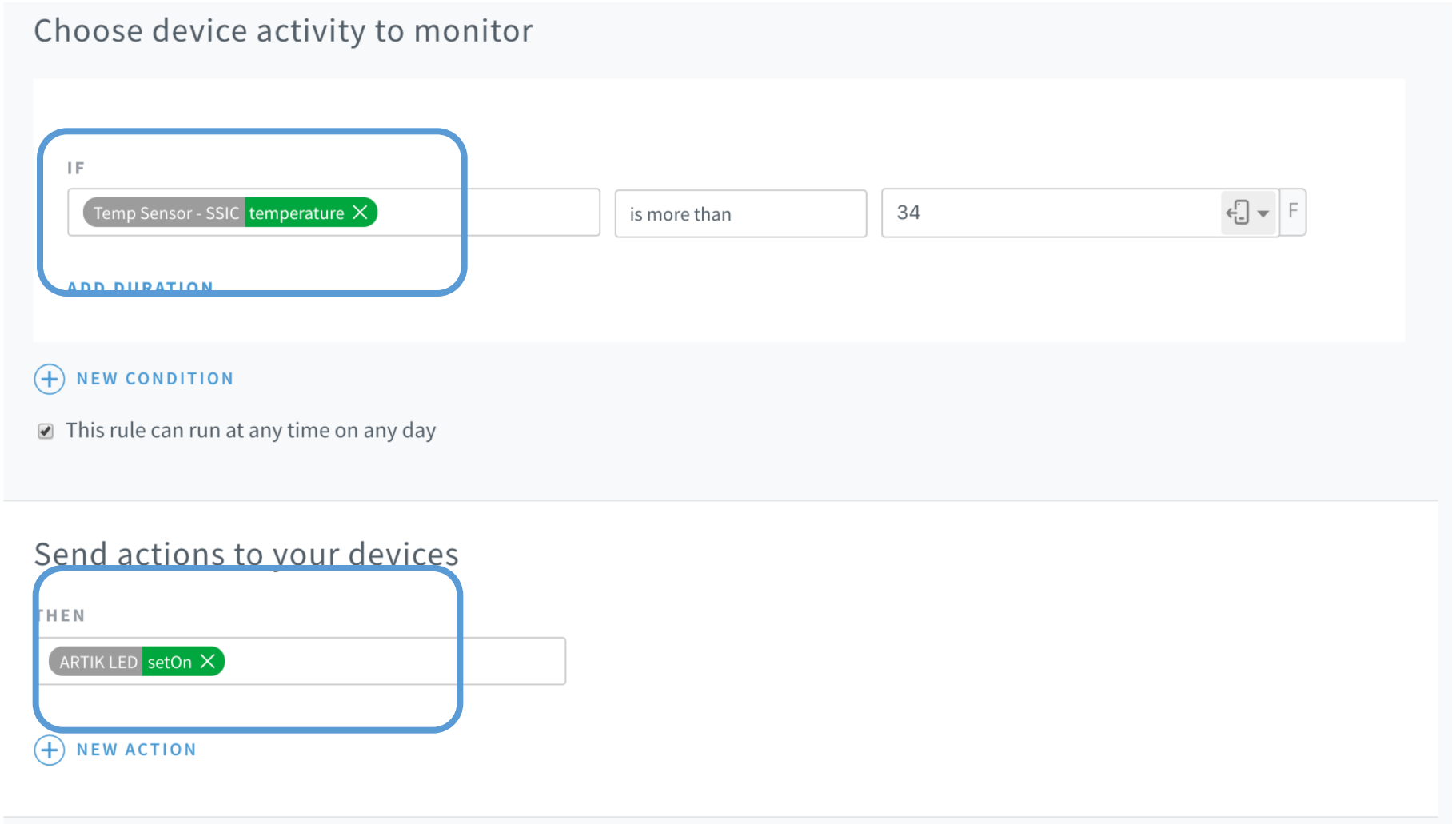


SAMSUNG ARTIK™

Orchestration Engine

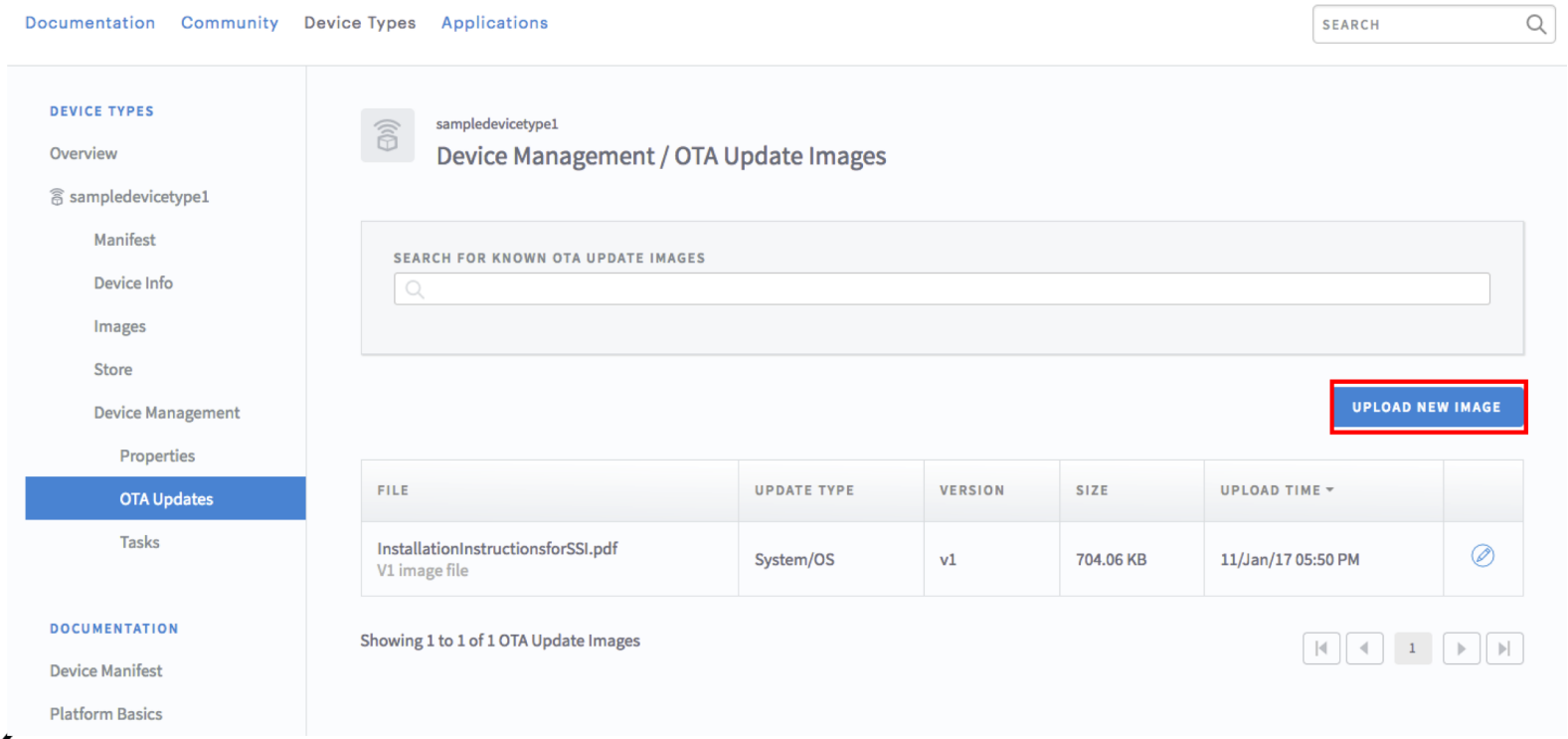


Rules


Choose device activity to monitor
IF
Temp Sensor - SSIC
temperature
is more than
34
F
ADD DURATION
NEW CONDITION
This rule can run at any time on any day
Send actions to your devices
THEN
ARTIK LED
setOn
NEW ACTION

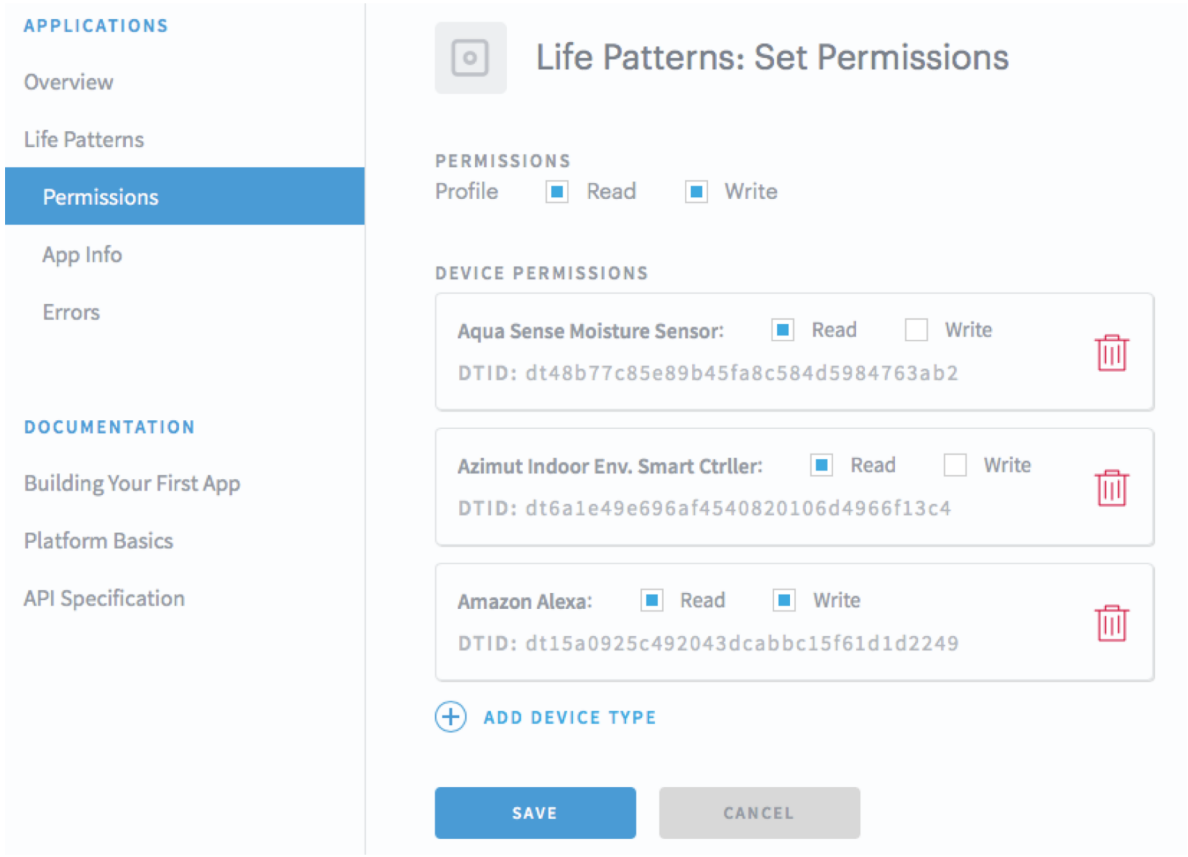
Device Management & Over the Air Update

- Based on Lightweight Machine to Machine(LWM2M)
- Monitors device presence, also properties like firmware version memory usage, battery consumption etc.
- OTA



SAMSUNG ARTIK

Secure Transaction



- Secure Device Registration
- Authentication & Authorization
- Data Encryption
- Privacy Management

SAMSUNG ARTIK™

Samsung ARTIK™ cloud services on SmartThings Cloud

Connect devices, connect clouds, and put them to work

Serviceability features and unparalleled interoperability for ARTIK modules and third-party devices and clouds

- Interoperability: Data Normalization; Cloud Connectors;
- Device Management: Provisioning, and over-the-air updates
- Sophisticated orchestration engine to define one-to-many or many-to-many actions between connected devices and data sources
- Security & Privacy Management

SAMSUNG ARTIK™

Use Cases

Customer Use Cases

Legrand: Global residential and commercial digital building infrastructure

Challenge: Transform product line to meet new connected digital mkt requirements. Fast time to mkt. Interoperability.

Products: ARTIK 0x, ARTIK 5/7 secure system-on-modules, ARTIK cloud services

Why ARTIK? Reduced product development time. Built-in software eliminated internal dev skills roadblock. Security allows them to meet new customer reqs. Interoperabilty expands switch capabilities, helped them get POC with Marriott “Room of the Future”.

NDA Customer: Factory automation provider

Challenge: Retrofit customer OT to meet requirements for Industry 4.0, enable access to data and create digital twins for more efficient operations. Ensure secure operations.

Products: ARTIK 530s secure system-on-module, ARTIK partner PTC

Why ARTIK? Secure gateway solution for their industrial gateway with access to local sensors, ability to do local processing and edge node management, application to view data via integration with PTC Thingworx front end application.

SAMSUNG ARTIK™

ARTIK 05x Modules

SAMSUNG
ARTIK™

ARTIK 05x Module Overview

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

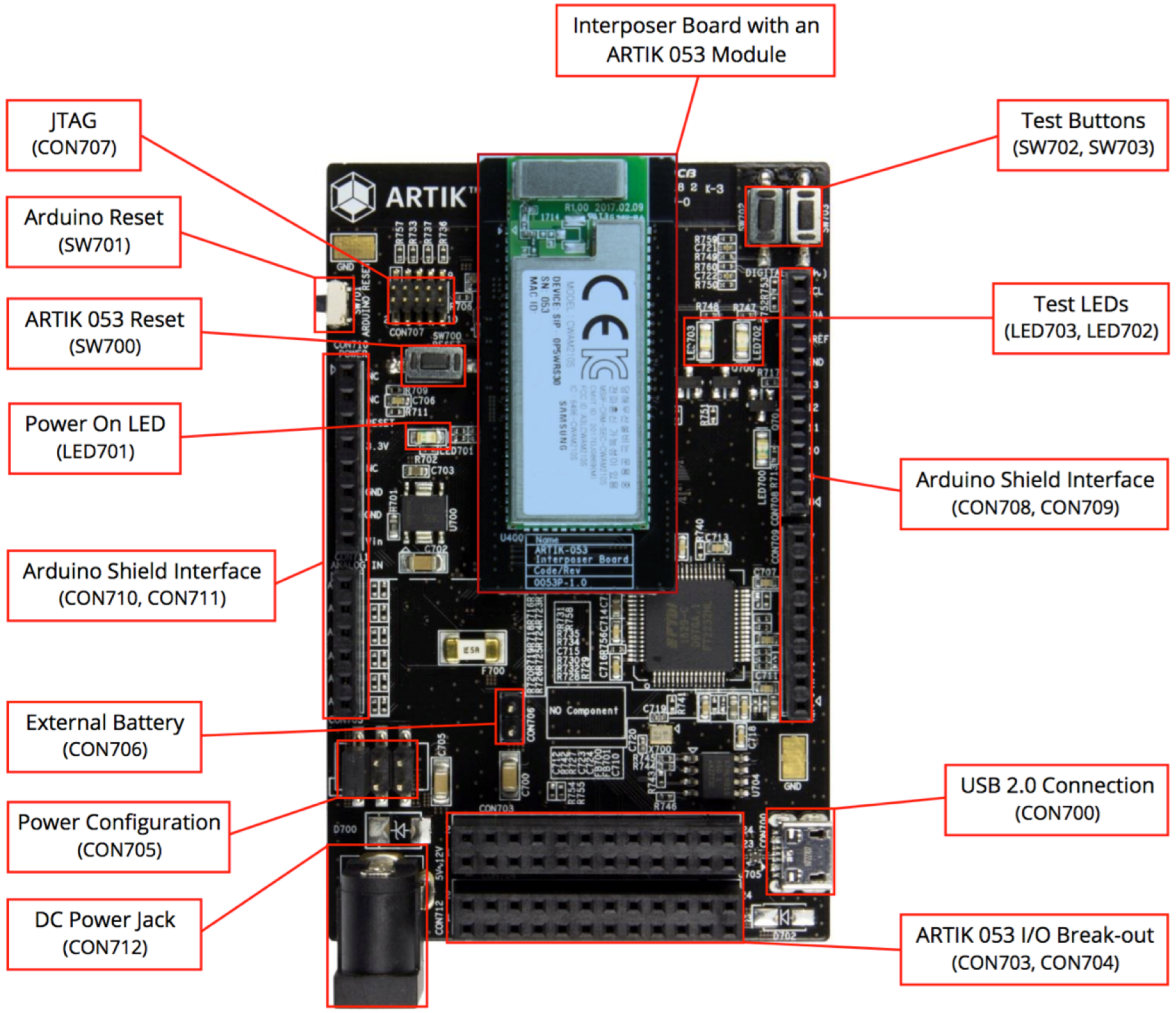
Create secure, next-gen edge products

- 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 Security: ARM Cortex M0
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 Starter Kit



Wi-Fi Subsystem

- ARTIK05x supports 802.11b/g/n Wi-Fi at 2.4GHz
- Dedicated Wi-Fi Processor subsystem with 480MHz 32-bit ARM Cortex R4 supported by 32KB I-Cache and 16KB D-Cache
- WiFi throughput: ~25 Mbps single stream
- WPA/WPA2

Samsung ARTIK™ 05x WiFi – wpa_supplicant

- Supplicant is used in the client stations for key negotiation with a WPA Authenticator.
- wpa_supplicant is designed for Linux, BSD and Windows with support for WPA and WPA2.
- wpa_supplicant was designed to use hardware, driver and OS independent, portable C code for all WPA functionality.
- A daemon program running in the background and acting as the backend component controls the wireless connection.

Samsung ARTIK™ 05x Power Management

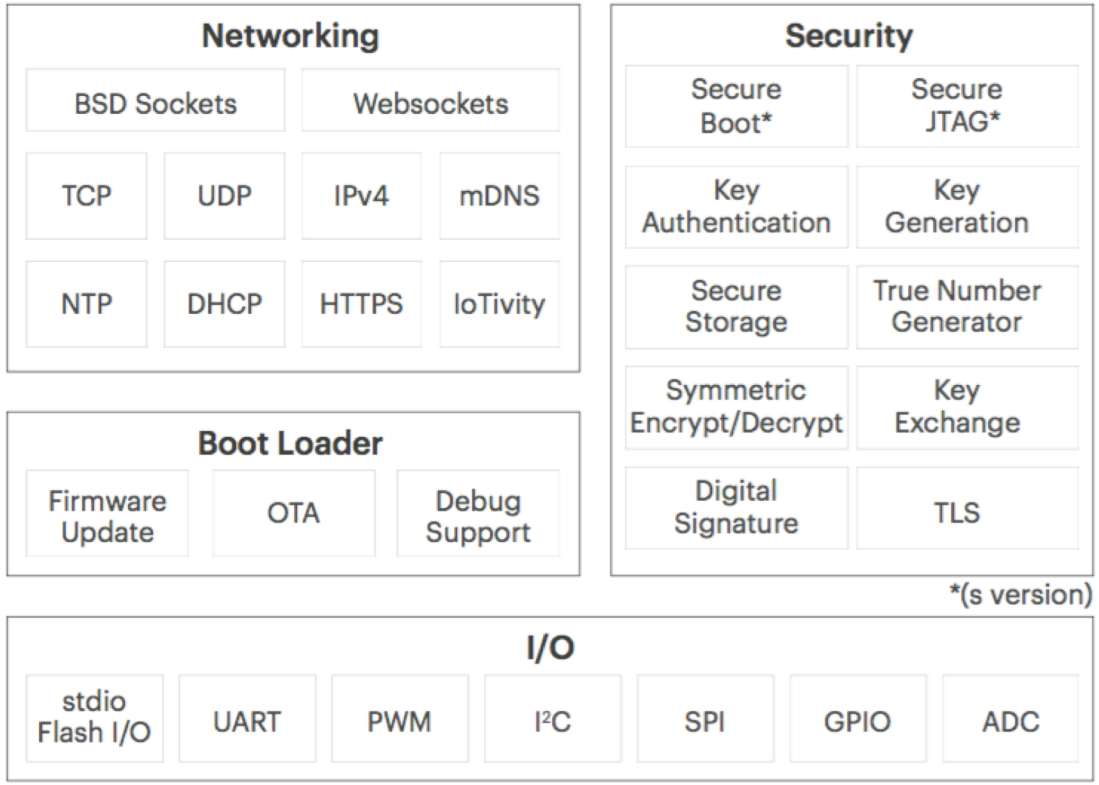
	Description	Power Consumption	Current @ 5V Typical	Current@12V Typical
Normal	Normal states. All components are running.	55mA normal cases	362mA +/- 30	151mA +/- 15
WiFi OFF	In this mode, almost all components are powered down. It consumes low power.	Up to 0.05W	46.5mA+/- 12	23.3mA+/-1.7
Deep Stop (DSTOP)	Almost all components are powered down except PMU (Power Management Unit).This state is similar to Power Off. However, DSTOP can be waken up by events such as external interrupt(Push button), UART or I2C device. And it also maintains their context before going to DSTOP.	Up to 0.05W	0.1mA	0.15mA

TizenRT OS Basics

- ARTIK 05x are powered by TizenRT
- TizenRT is a lightweight RTOS-based platform to support low-end IoT devices, based on Nuttx
- Primary governing standards are POSIX and ANSI standards
- IP Network Stack

TizenRT OS Hierachy

Kernel Services	
Realtime	Tasks, threads, queues, mutex, semaphore, signal
Time	Real-time clock, date/time, timer, sleep
Network Services	
Internet	DHCP, NTP Client, DNS Client, mDNS, BSD Sockets, Websockets
Services	Web client/server, MQTT client, IoTivity, cJSON
libc Services	
Libc Compatibility	Flash based Stdio, Stdlib, String, Unistd, Time
Security Services	
Encryption	AES 128/256, RSA 1024/2048, ECC BP/NIST 192/224/256/384/512
Authentication	HMAC 128/256, certificate
Certificate Storage	Secure Flash storage
Firmware Integrity	Secure boot and JTAG protection



SAMSUNG ARTIK™

IoTBus Framework

- GPIO (General Purpose Input/Output)
- I2C (Inter Integrated Circuit)
- SPI (Serial Peripheral Interface)
- PWM (Pulse Width Modulation)
- UART (Universal Asynchronous Receiver/Transmitter)

Device Management and LWM2M stack

- Lightweight M2M (LWM2M) is a device lifecycle management specification
- Provides a specification for functions like: firmware upgrade, provisioning of certificates, access control policies, connectivity monitoring etc.
- Based on CoAP protocol
- LWM2M allows the use of UDP for communication between client and server
- DTLS security for communication between an LWM2M client and ARTIK Cloud server(an LWM2M server).

ARTIK 05x Development

Developing on ARTIK 05x

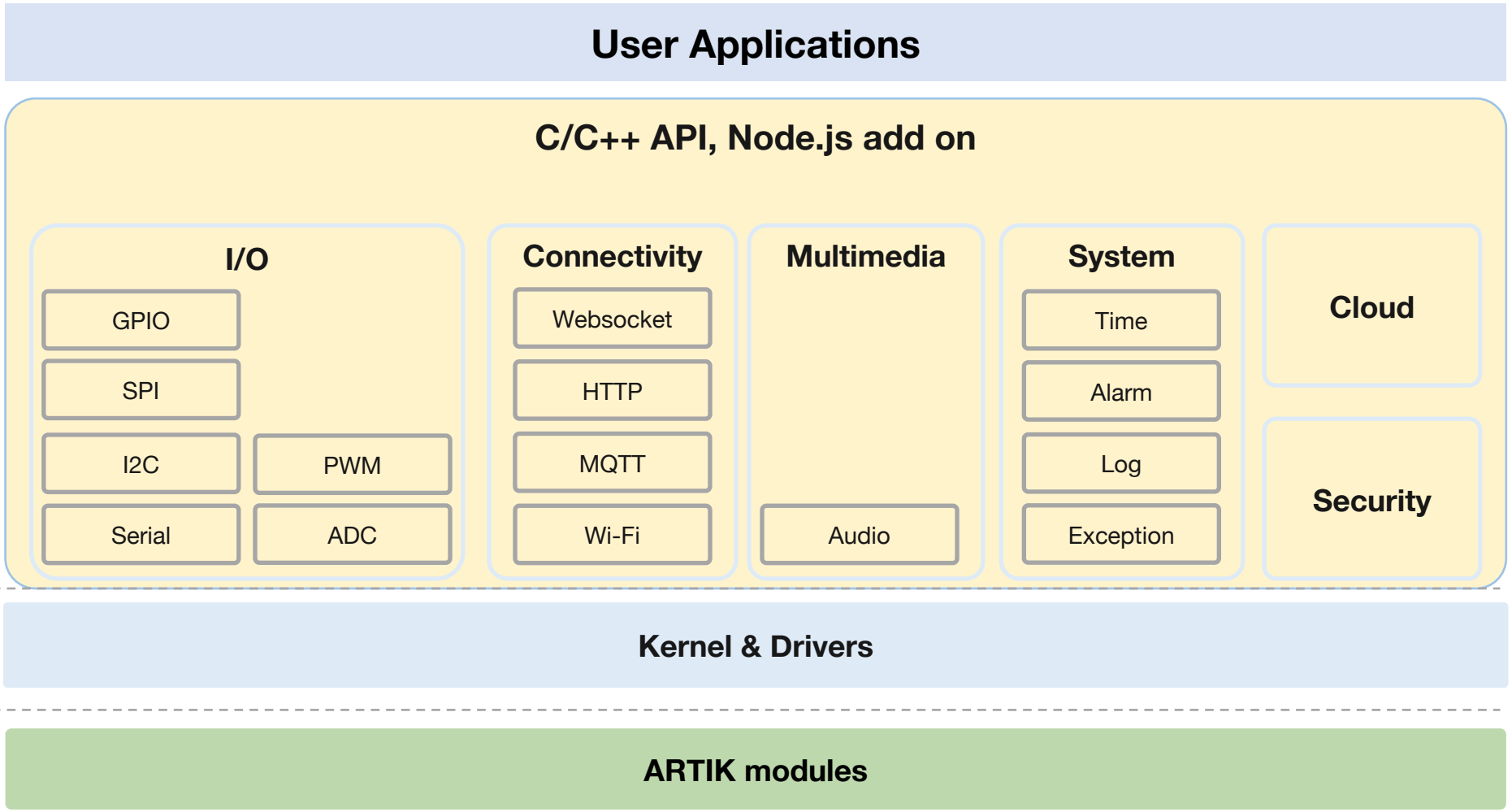
- ARTIK SDK/IDE (C language)
- Cross-compilation for ARM architecture from command line (C language)
- JerryScript(under development, JS)

ARTIK SDK (05x, 5, 7 series)

Software Modules + ARTIK API

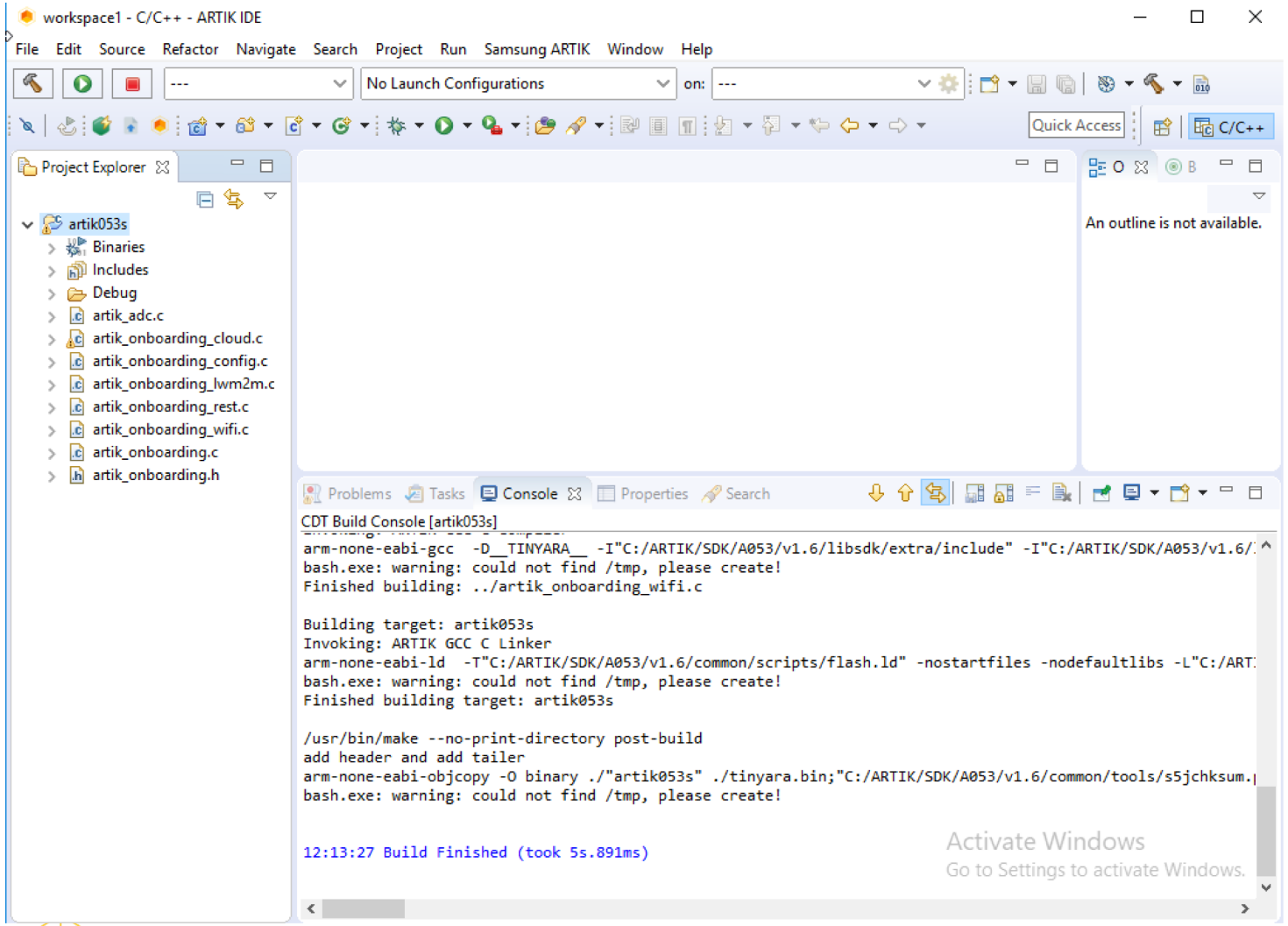
Kernel

HW



SAMSUNG ARTIK™

ARTIK IDE



gcc-arm-none-eabi

Cross Compilation from command line

- Github page: https://github.com/SamsungARTIK/TizenRT
- How to build:

```
$ git clone https://github.com/SamsungARTIK/TizenRT.git
$ cd TizenRT/os
  ….
$ make menuconfig
$ make
```

SAMSUNG ARTIK™

JerryScript

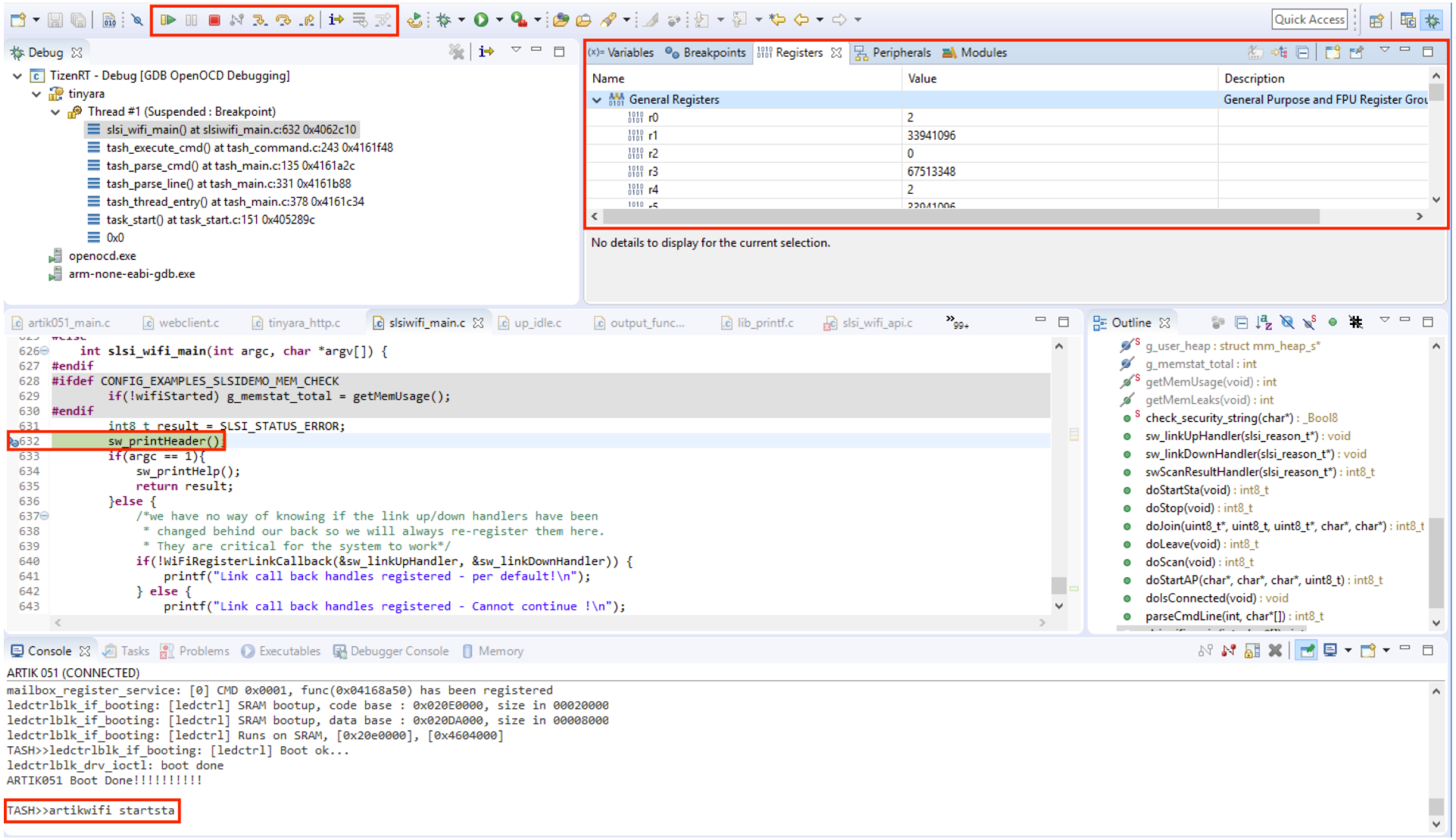
- Light weight JavaScript Engine. Base footprint is only 10KB of RAM
- Optimized for microcontrollers
- Portable, can run on bare-metal
- OS Support: Nuttx, RIOT, mbed OS, Zephyr, Linux, macOS

TASH shell

- Github page: https://github.com/SamsungARTIK/TizenRT/tree/artik/apps/shell

```
TASH>>help

         TASH command list
         --------------------
cat              cd               date             df
dhcpd            exit             free             heapinfo
help             ifconfig         ifdown           ifup
kill             killall          ls               mkdir
mksmartfs        mount            onboard          ping
ps               pwd              reboot           rm
rmdir            security         sh               sleep
stkmon           umount           uptime
```

Debugging on ARTIK 05x



SAMSUNG ARTIK™

Demo: Smart Coffee Machine with ARTIK E2E Solution

ARTIK Security

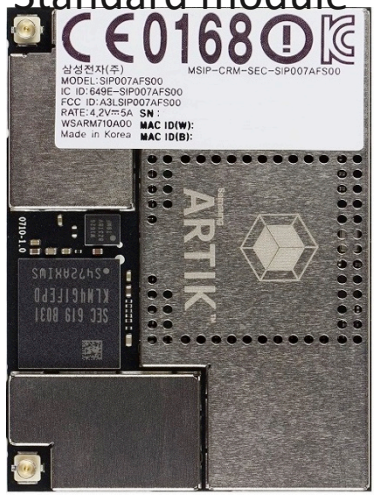
SAMSUNG
ARTIK™

ARTIK 05x Module Security

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

Security Questionnaire

How do you provide security across all attack surfaces?

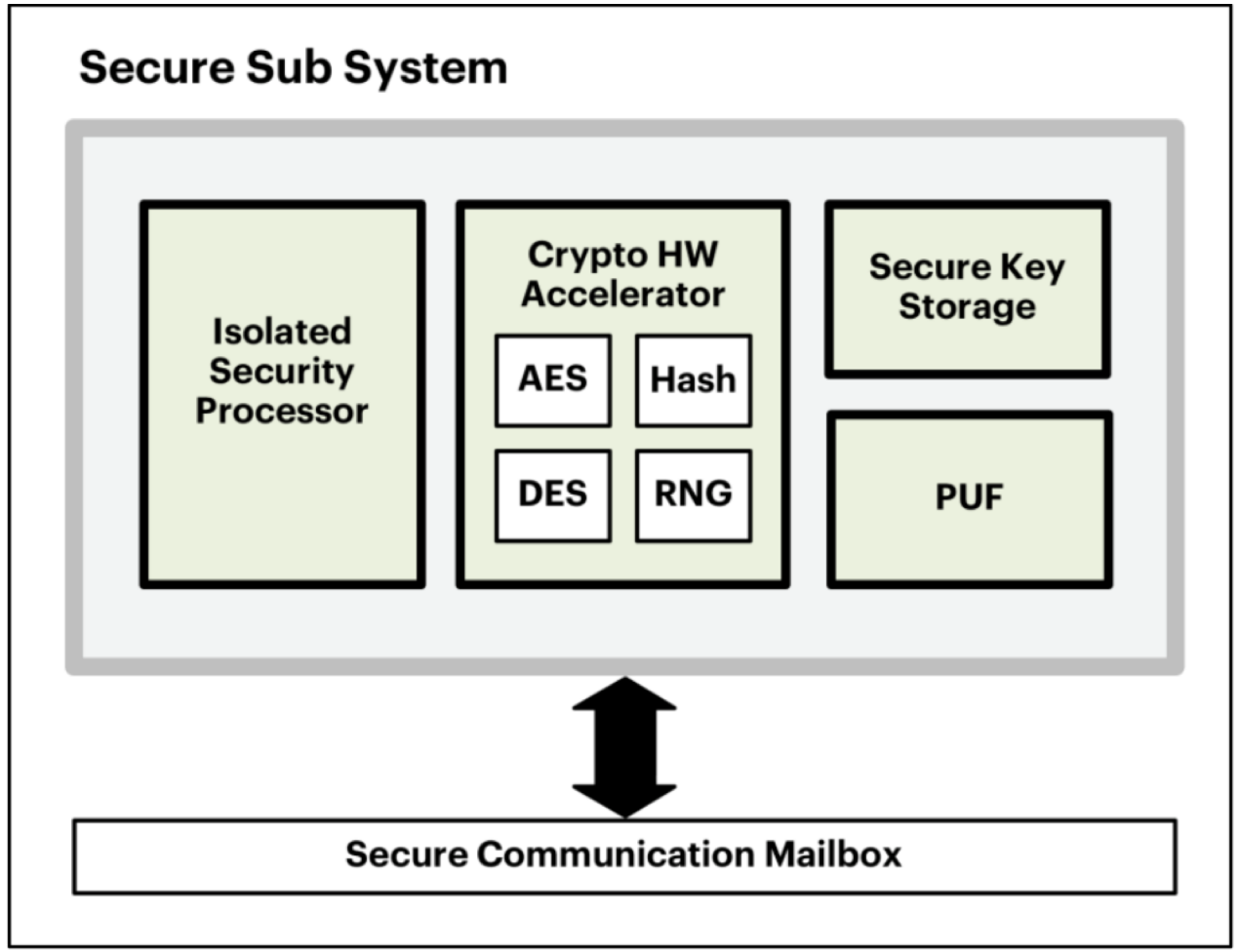
Question	ARTIK 5/7/053
Do you support secure communication from device to device or device to cloud?	Yes
How do you secure communication? Are you using TLS1.2 or higher?	HTTPs using TLS 1.2
How do you establish identity of device?	Using unique certificate on each device
Do you have the infrastructure to inject unique key and certificate in each device to establish unique identity per device? How much does it cost?	Yes (Done at Samsung factory. Cost included in module)
How do you protect your certificate, keys?	Specialized HW on module (secure element)
Are your certificate and keys safe if software is hacked?	Yes (They are protected by HW)
How does the device establish identity of cloud?	Both device and cloud are chained to ARTIK Root CA and can verify each other certificates
Do you have mutual authentication when enabling secure communication?	Yes
Is your certificate infrastructure secure? How do you secure your Root Certificates? How much does it cost?	Yes (Root CA secured by 3rd party security vendor)

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™

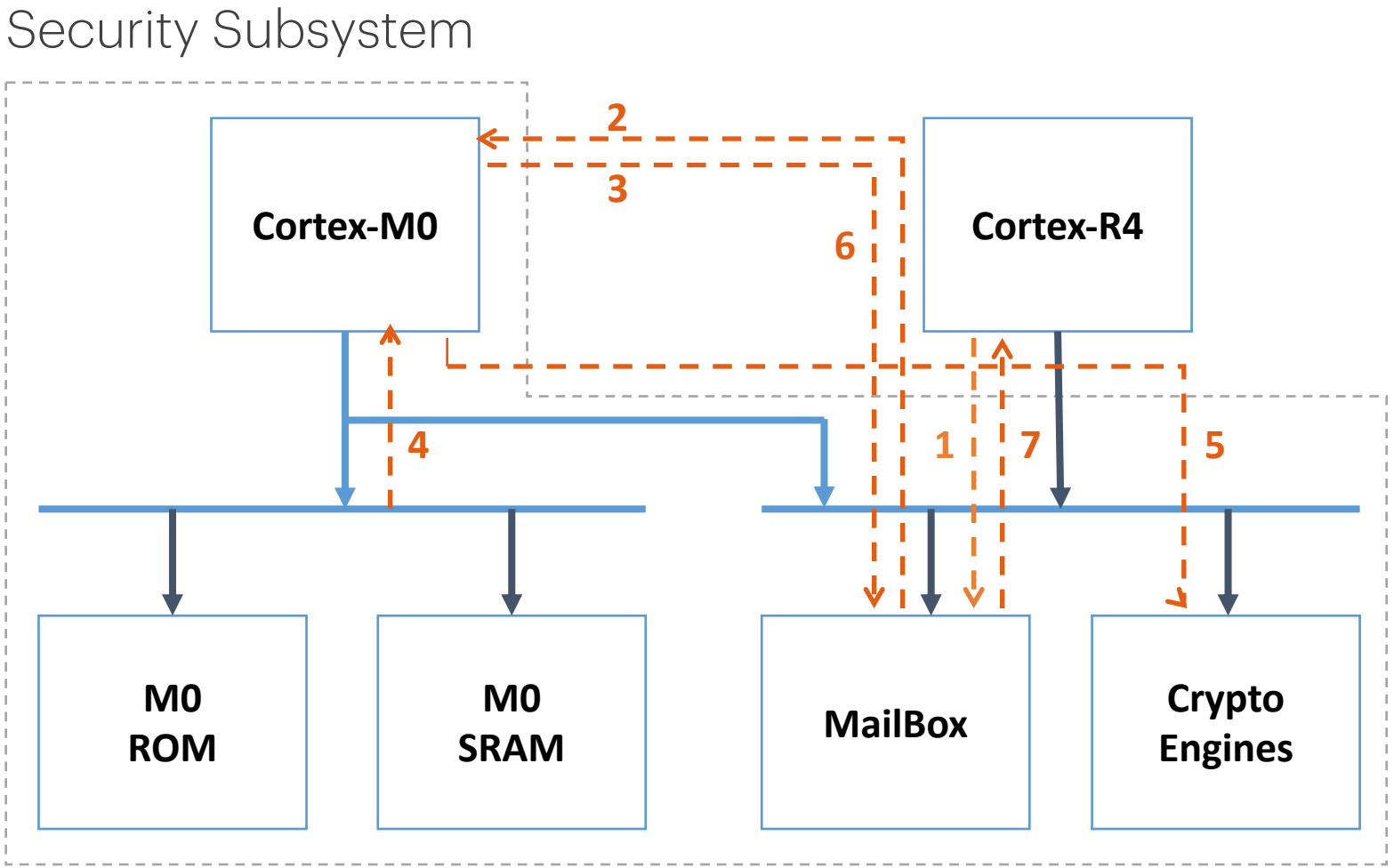
ARTIK 05x Security Subsystem



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

SAMSUNG ARTIK™

Isolated Security Processor



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

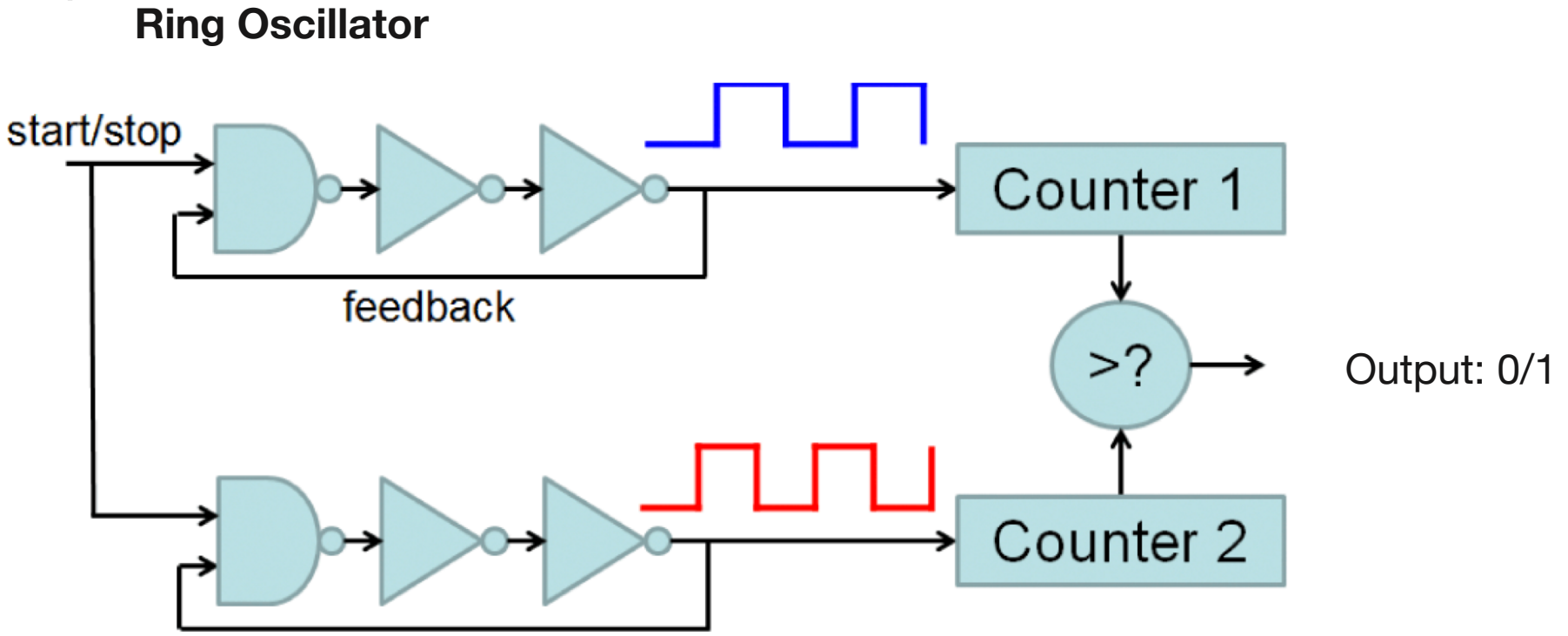
PUF (Physically Unclonable Function)

- 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:
  - **Key generation and storage (seed key)**
  - Device identification
  - IP Protection
  - Protocols with challenge-response pairs

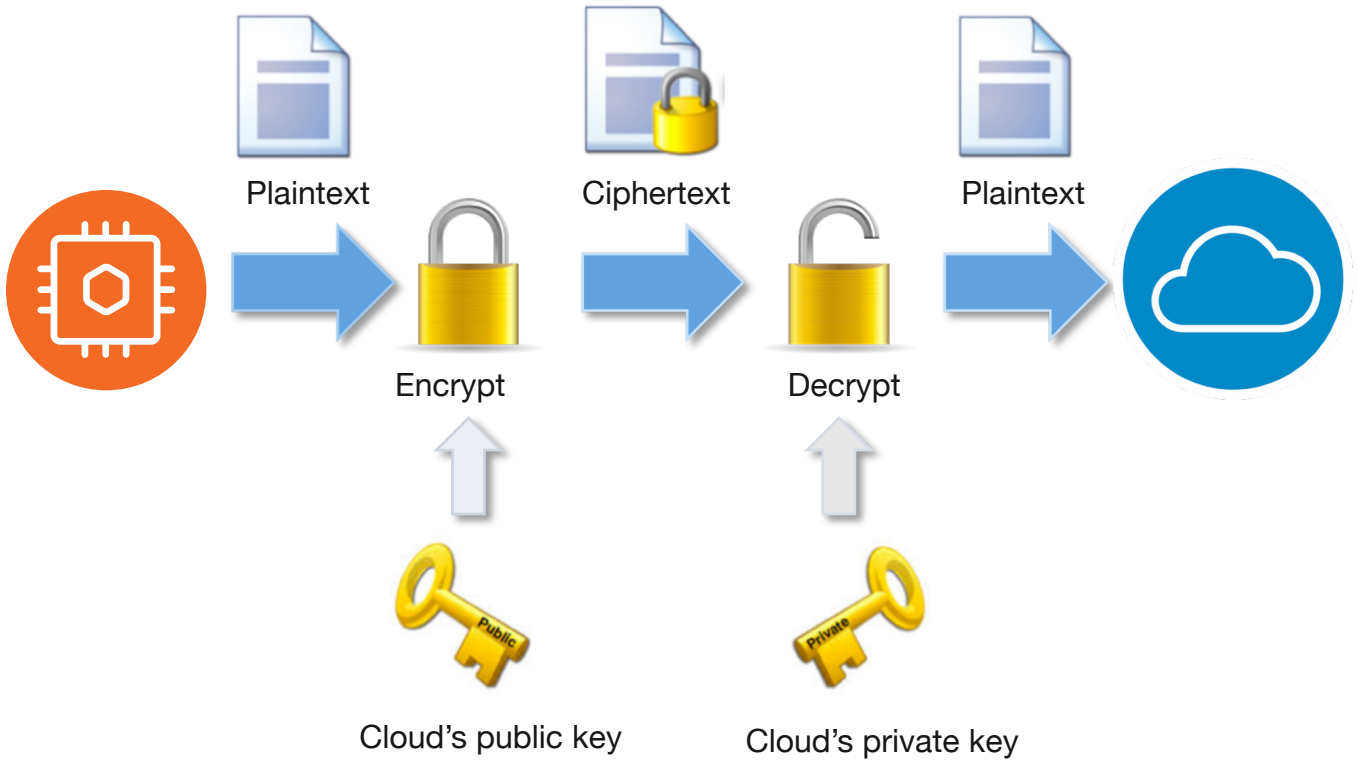
SAMSUNG ARTIK™

RO Frequency PUF

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

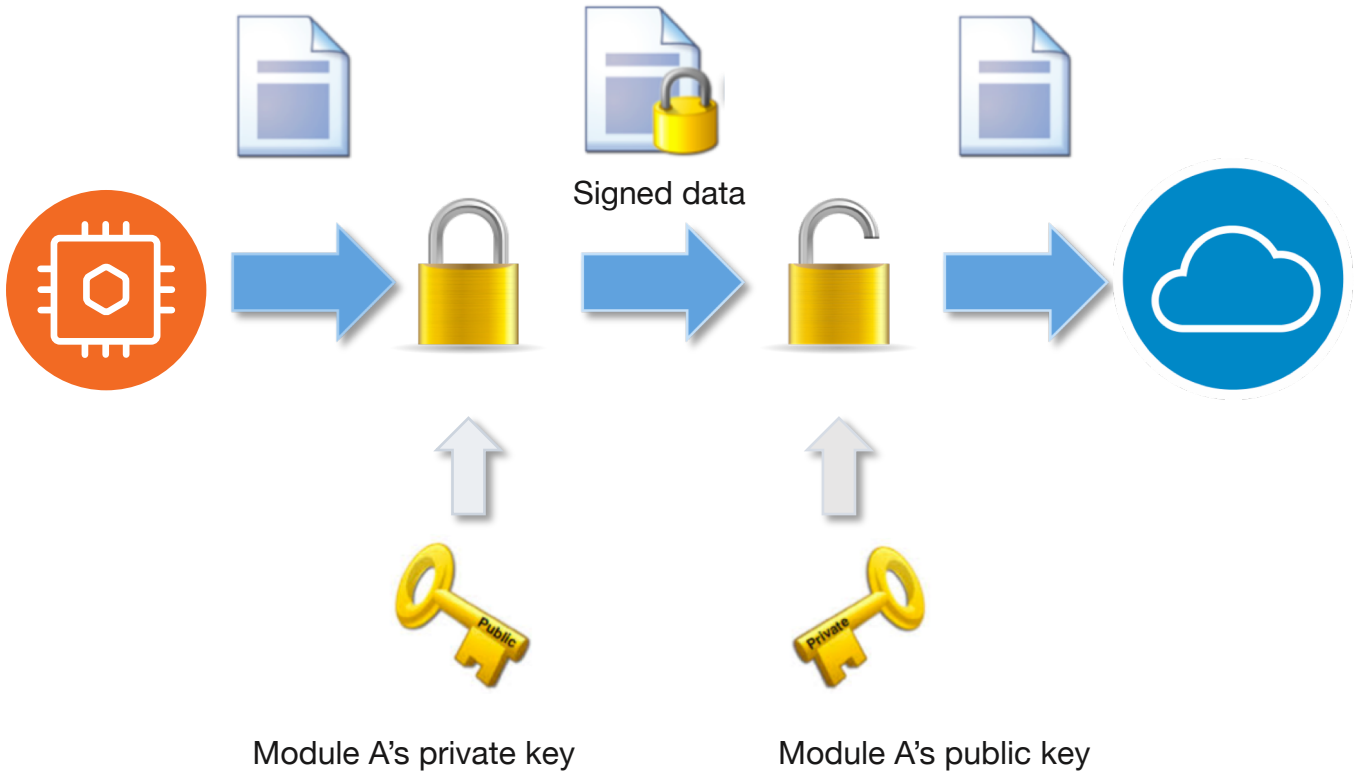


Encryption and Decryption



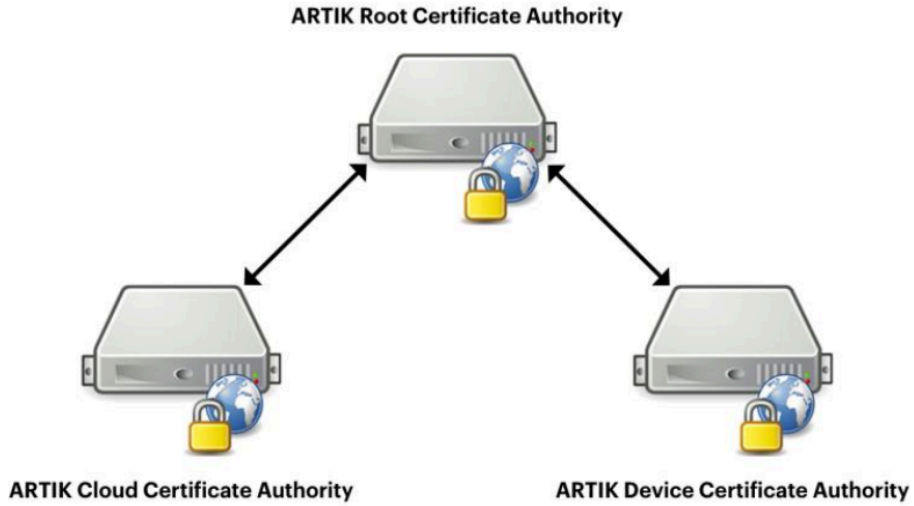
Different keys are used to encrypt and decrypt messages

Signature


Signed data
Public
Private
Module A's private key
Module A's public key

Public Key Infrastructure (PKI)

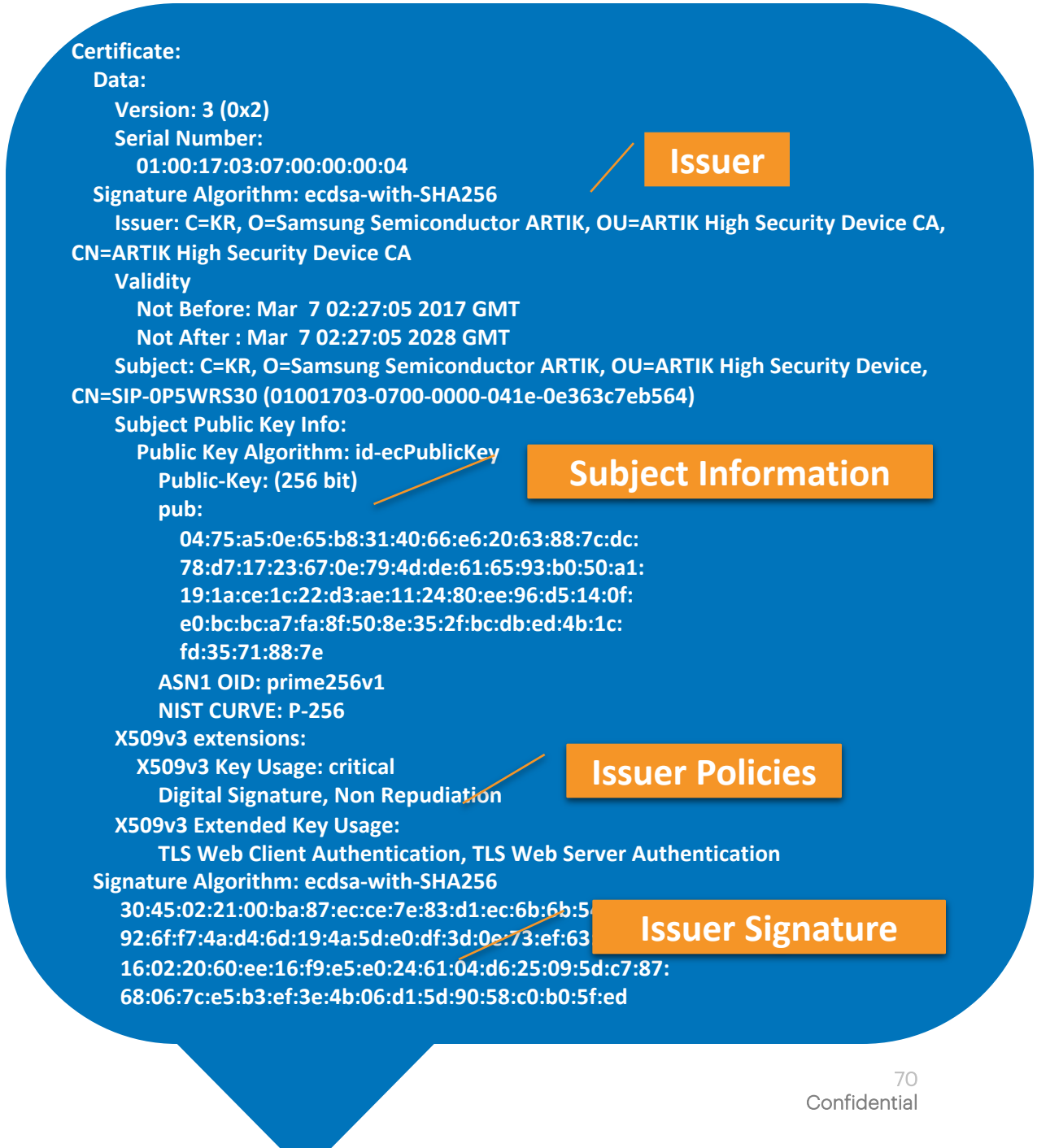
- A Public Key Infrastructure (PKI) supports the distribution and identification of public encryption keys, establishing authenticity and trust in a system.
- ARTIK provides PKI, which is used to generate and apply unique certificates and key pairs to each ARTIK Module during manufacturing.
- PKI's core concept is (Digital) Certificate. Issued by a **Certificate Authority,** e.g, GlobalSign, Symantec
- ARTIK Root CA



SAMSUNG ARTIK™

Certificate

- A Certificate contains an identity (a hostname, or an organization, or an individual), a public key, signature etc.
- X.509 is a standard that defines the format of public key certificates.



Mutual Authentication

- Each ARTIK module is provisioned with:
  - An unique private key
  - Its associated certificate containing a public version of the key.
  - An ARTIK Root CA certificate
- ARTIK Cloud's server certificate is also rooted to the ARTIK Root CA certificate
- At connect time, server and client exchange certificates for mutual authentication

Post Provisioning

- If you want to connect your ARTIK Module to a 3rd party Cloud service or implement a link between two ARTIK modules, you need to generate your own certificate/key-pair
- We can use Post Provisioning APIs to post provision customer credentials(key, certificate) to Secure Element

Secure Communication

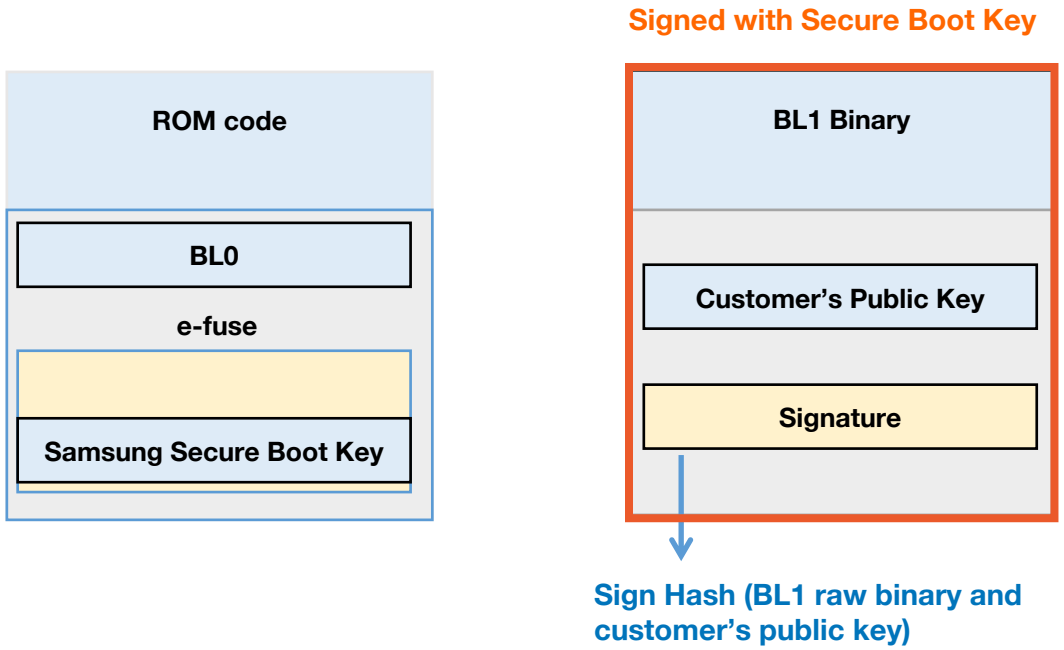
		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	Comments
Secure communication	**Per device unique key & certificate**	✓	✓	**Uniquely identifies device**
	Key stored in HW secure element	✓	✓	**Secure key storage**
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	**Device 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™

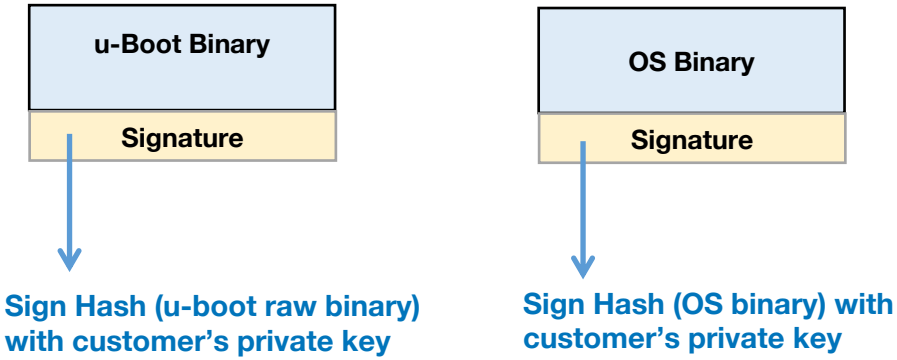
Secure Boot

- Secure Boot adds cryptographic checks to each stage of the boot process.
- The first element in the boot process authenticates the second, the second verifies the third.
- Authentication is based on digital signature verification.
- **Chain of Trust:** Every component can be authenticated before being executed.

Secure Boot for ARTIK 05x S-Module



For ARTIK 05Xs, BL stage 1 and stage 2 files are located under *build/configs/artik05x/bin* directory: `bl1.bin`, `bl2.bin`, `tinyara_head.bin`



BL0:
1. Decrypt BL1
2. Verify signature using BL1 Hash(BL1 binary and customer's public key) and hash

BL1:
1. Verify signature using u-boot Hash (u-boot binary and customer's public key)
2. Load to DRAM

u-boot:
1. Verify signature using (OS binary and customer's public key)
2. Load to DRAM

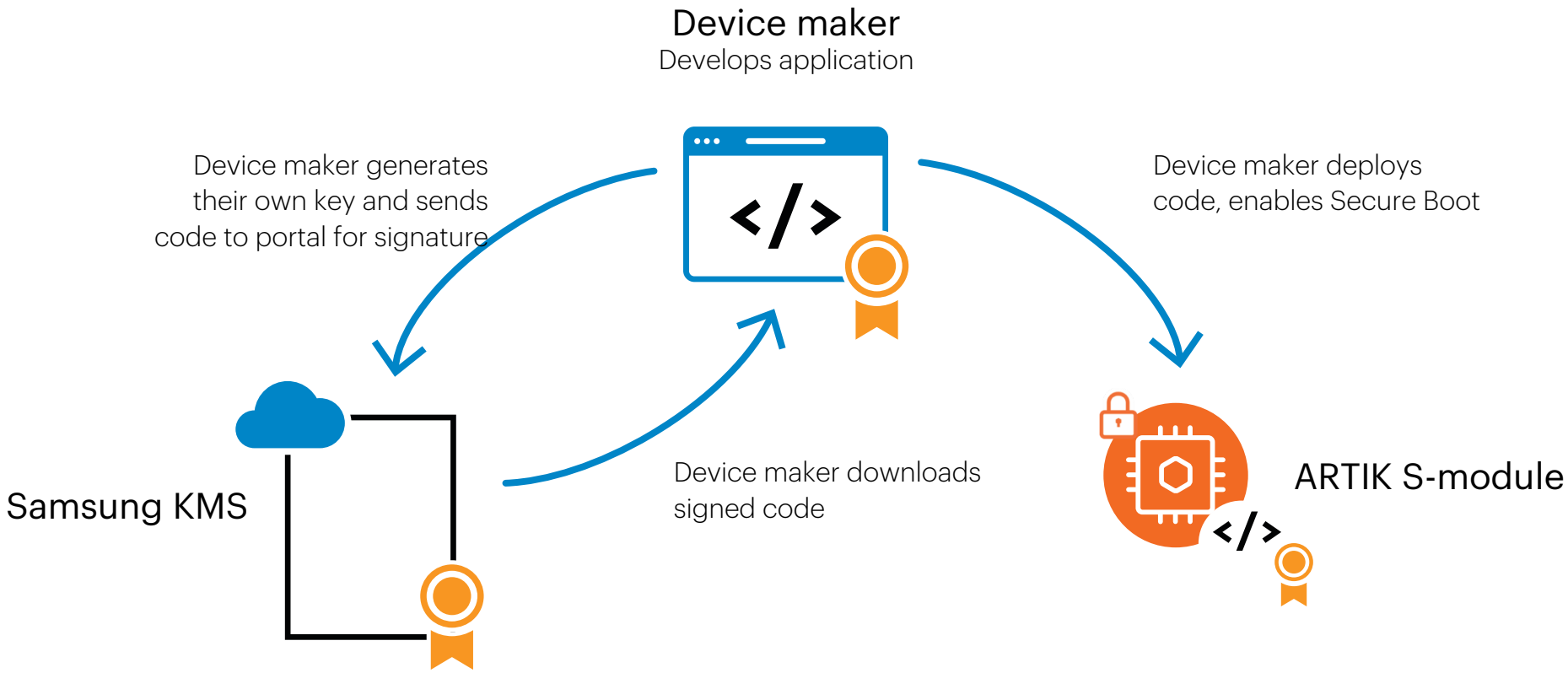
SAMSUNG ARTIK™

Code Signer (Development Stage)

```
Invoking: ARTIK GCC Create Head Bin
C:/ARTIK/SDK/A055s/v1.7.1/common/tools/s5jchksum.py     "tinyara.bin"
"tinyara_head.bin"
Finished building: tinyara_head.bin


Invoking: ARTIK GCC Create Head Sign
C:/ARTIK/SDK/A055s/v1.7.1/common/codesigner/artik05x_AppCodesigner
C:/ARTIK/SDK/A055s/v1.7.1/common/codesigner/rsa_private.key
"tinyara_head.bin"


  . Seeding the random number generator...
  . Reading private key from
 'C:/ARTIK/SDK/A055s/v1.7.1/common/codesigner/rsa_private.key'
  . Generating the RSA/SHA-256 signature
  . Done (created "tinyara_head.bin-signed")


  + Press Enter to exit this program.
Finished building: tinyara_head.bin-signed
```

NEW Samsung ARTIK™ Key Management System(KMS)

Code signing portal manages key signing

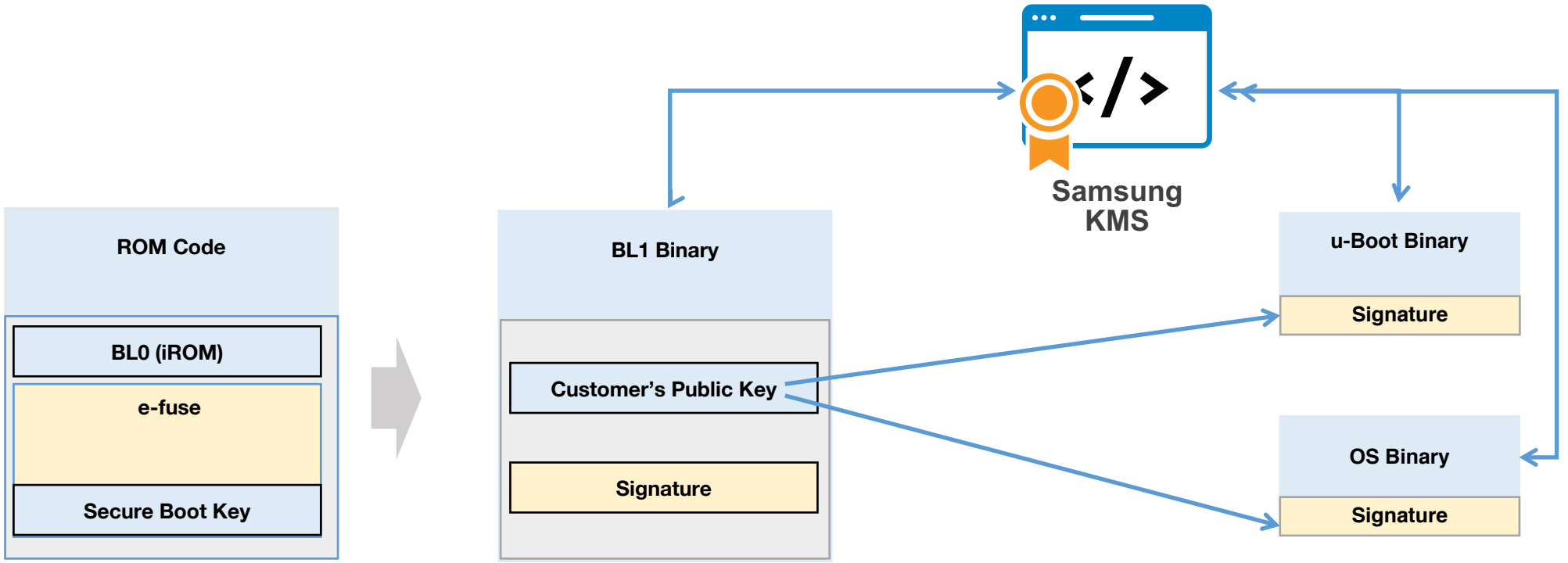


SAMSUNG ARTIK™

Key Management System

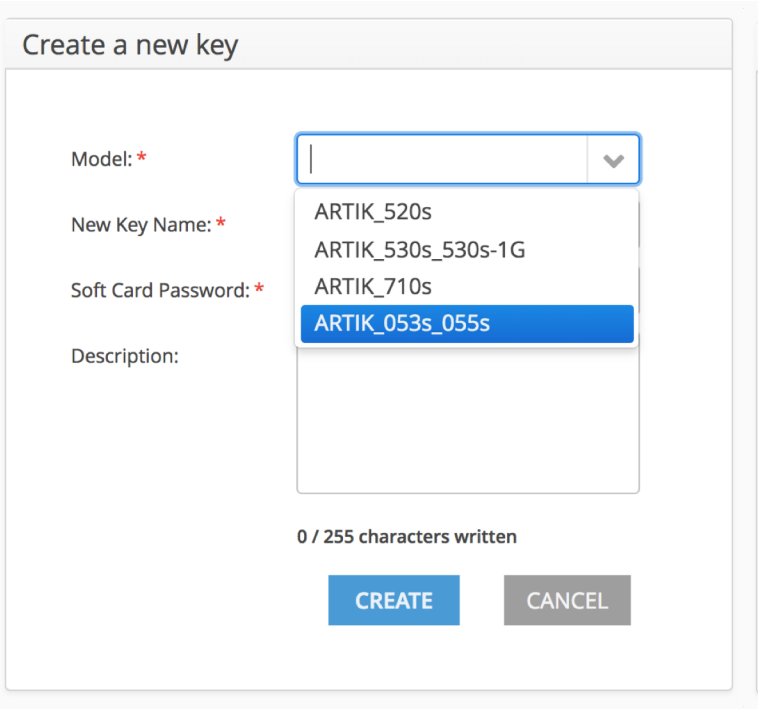
- Signing keys are stored and operated within FIPS 140-2 certified Hardware security modules (HSM)
- Images are signed through a highly secure cryptography standard (SHA-256 w/ RSA2048 encryption)
- Strict access control policies
- Only accessible through whitelisted IPs

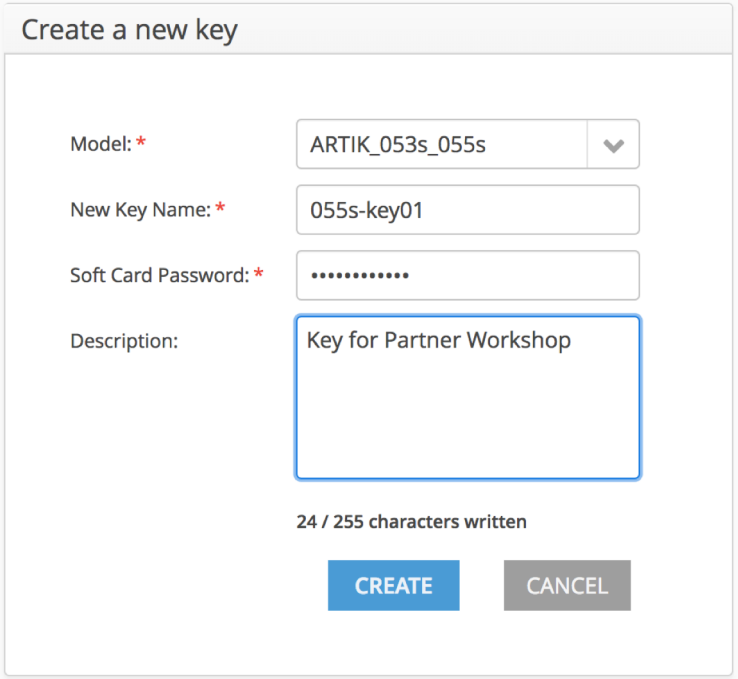
Key Management System Role

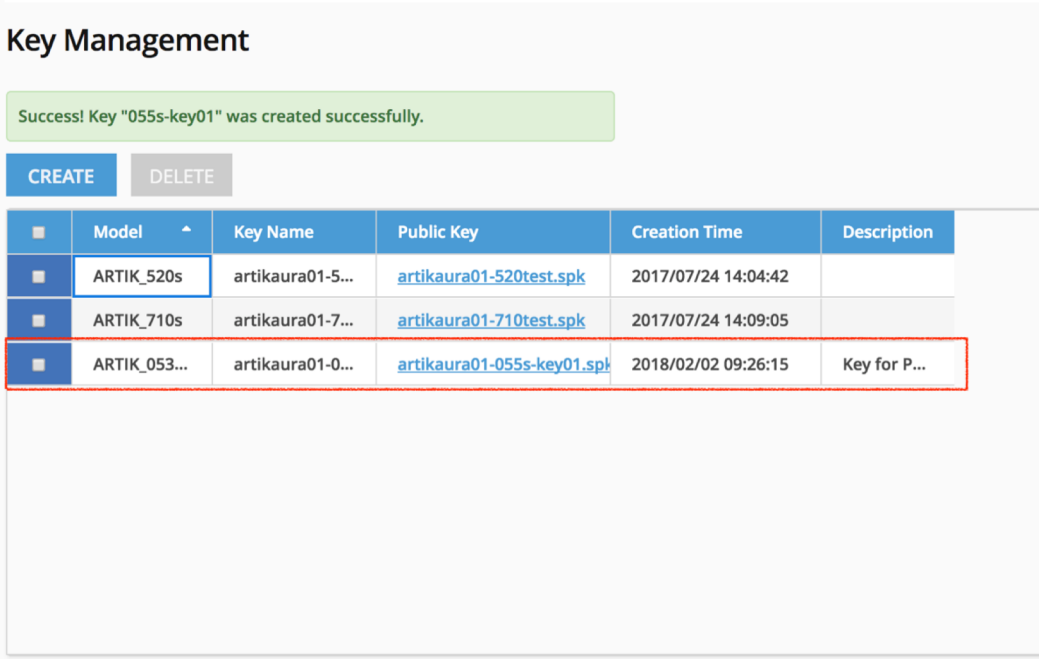


- BL1 image is provided by chip vendor

KMS Key Management







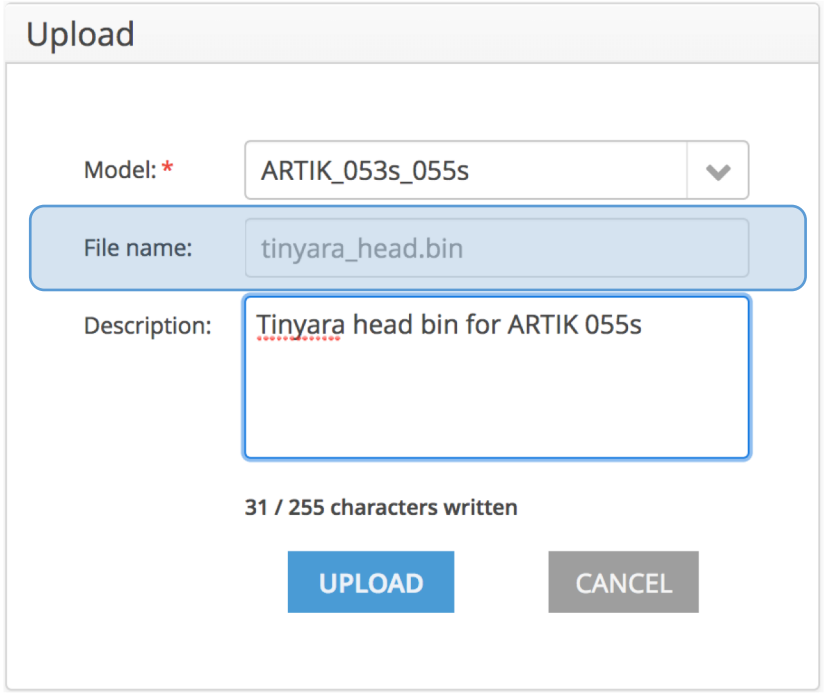
Stage 1:

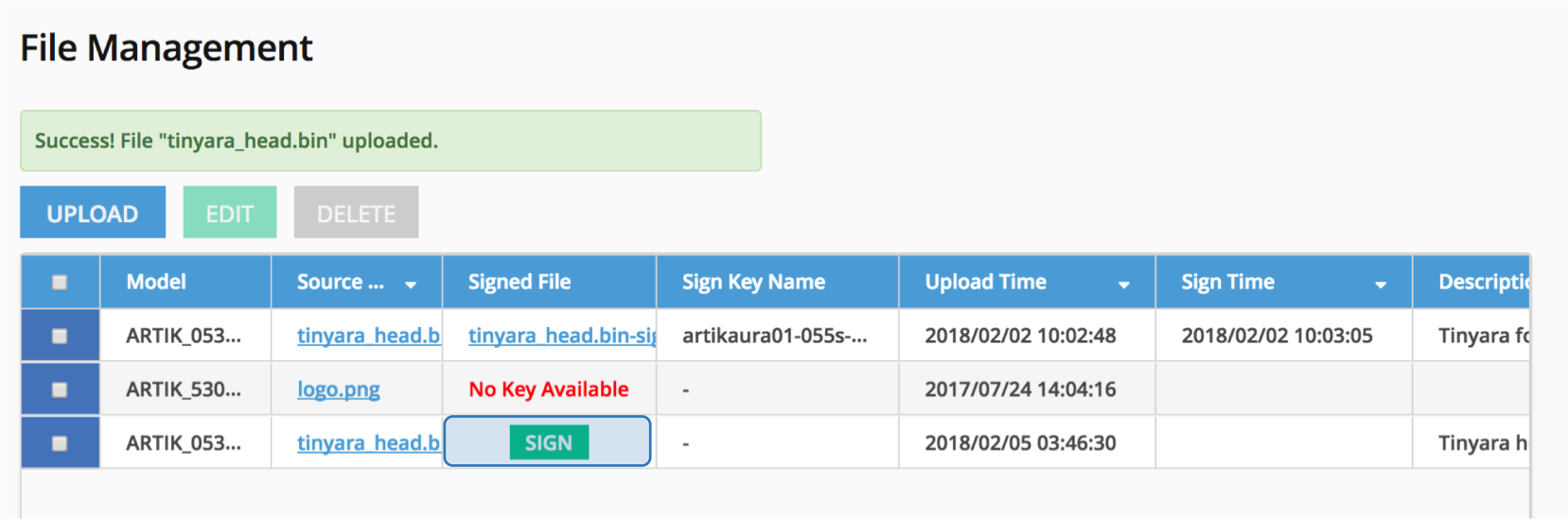
- Public key is immediately available on KMS portal
- Send ARTIK team the resulting public key.
- ARTIK team signs the bootloader stage 1 (BL1) image and deliver it to you by e-mail.

SAMSUNG ARTIK™

KMS File Management (Stage 2 Images)

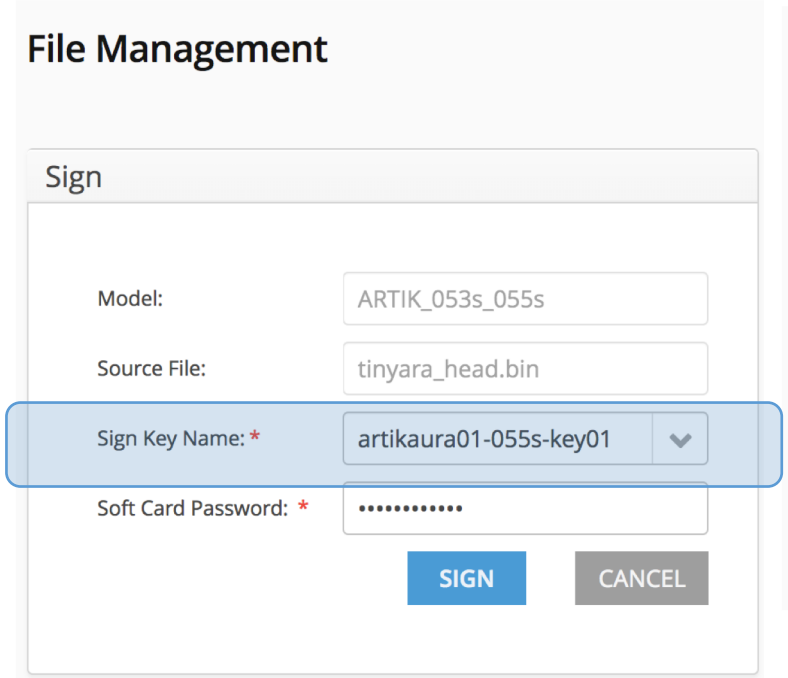
Upload bootloader stage 2(BL2) and OS files for self-signing

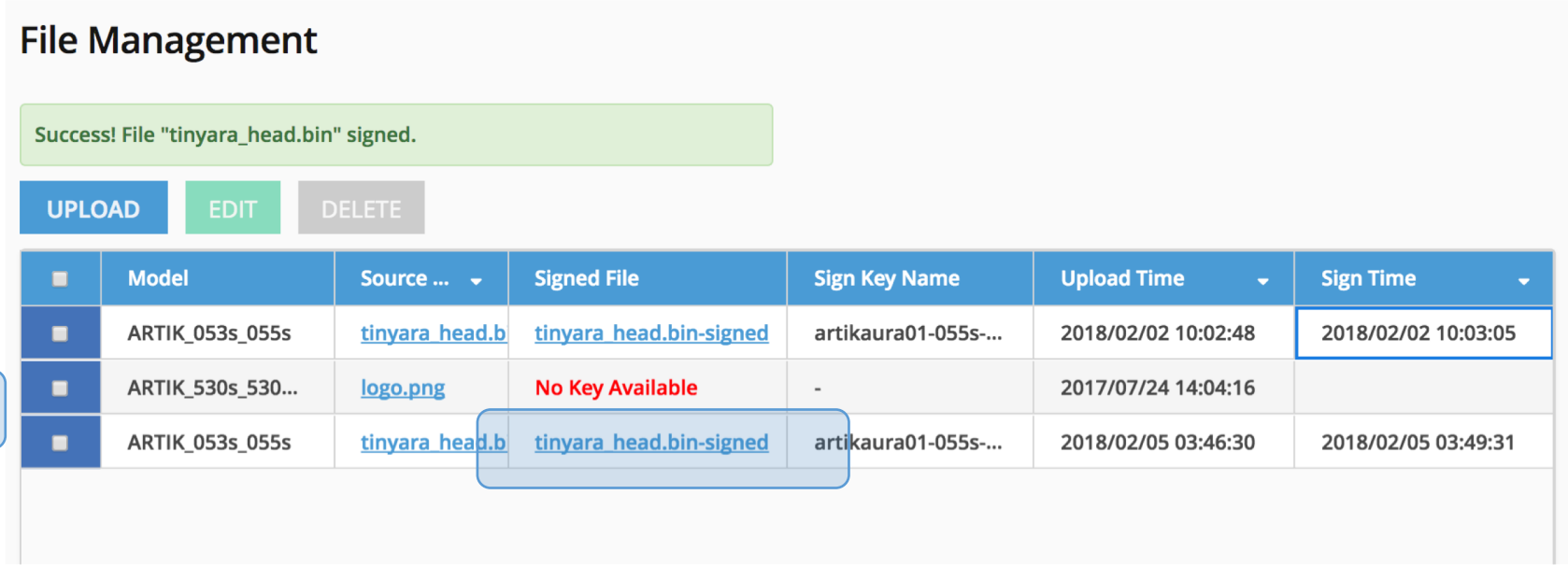




KMS File Management (Stage 2 Images)

Sign BL2/OS image with generated key, and download the signed BL2/OS images.





SAMSUNG ARTIK™

Samsung ARTIK™ Module development

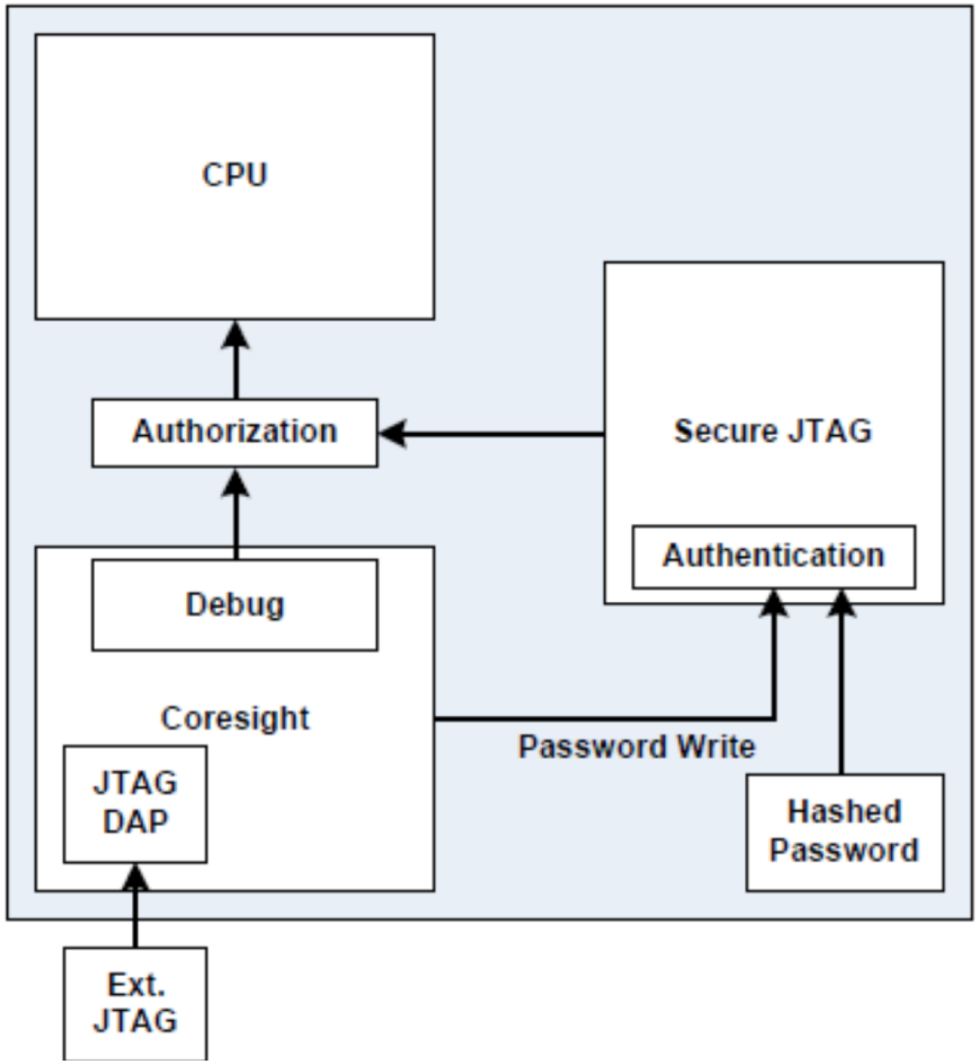
CUSTOMER

	STANDARD MODULES	s-MODULES
	BUYS ARTIK IoT module OR	**BUYS** ARTIK IoT s-module
Download	**DOWNLOADS** SDK from github.com	**DOWNLOADS** SDK from github.com
		LOGS ON artik.io
		DOWNLOADS, SIGNS SLA
	DOWNLOADS OS, libraries	**DOWNLOADS** secure OS, libraries, code signer
Modify and develop	**MODIFIES** downloaded software	**MODIFIES** downloaded software
	DEVELOPS custom application	**DEVELOPS** custom application
		RE-SIGN using code signer
	COMPILE development code	**COMPILE** development code
	LOAD DEV CODE on SoM and validate	**LOAD DEV CODE** on SoM and validate
		SETUP KMS ACCOUNT
		CREATE KEY
		SIGN, DOWNLOAD CODE
	LOAD PRODUCTION CODE on SoM and validate	**LOAD PRODUCTION CODE** on SoM and validate
	PRODUCTIZE	**PRODUCTIZE**
OTA update	**BUILDS** OTA image	
	SIGN, DOWNLOAD IMAGE	
	UPLOAD to artik.cloud	
	DELIVER OTA to devices	
	STATUS UPDATES confirmations sent to cloud	

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.



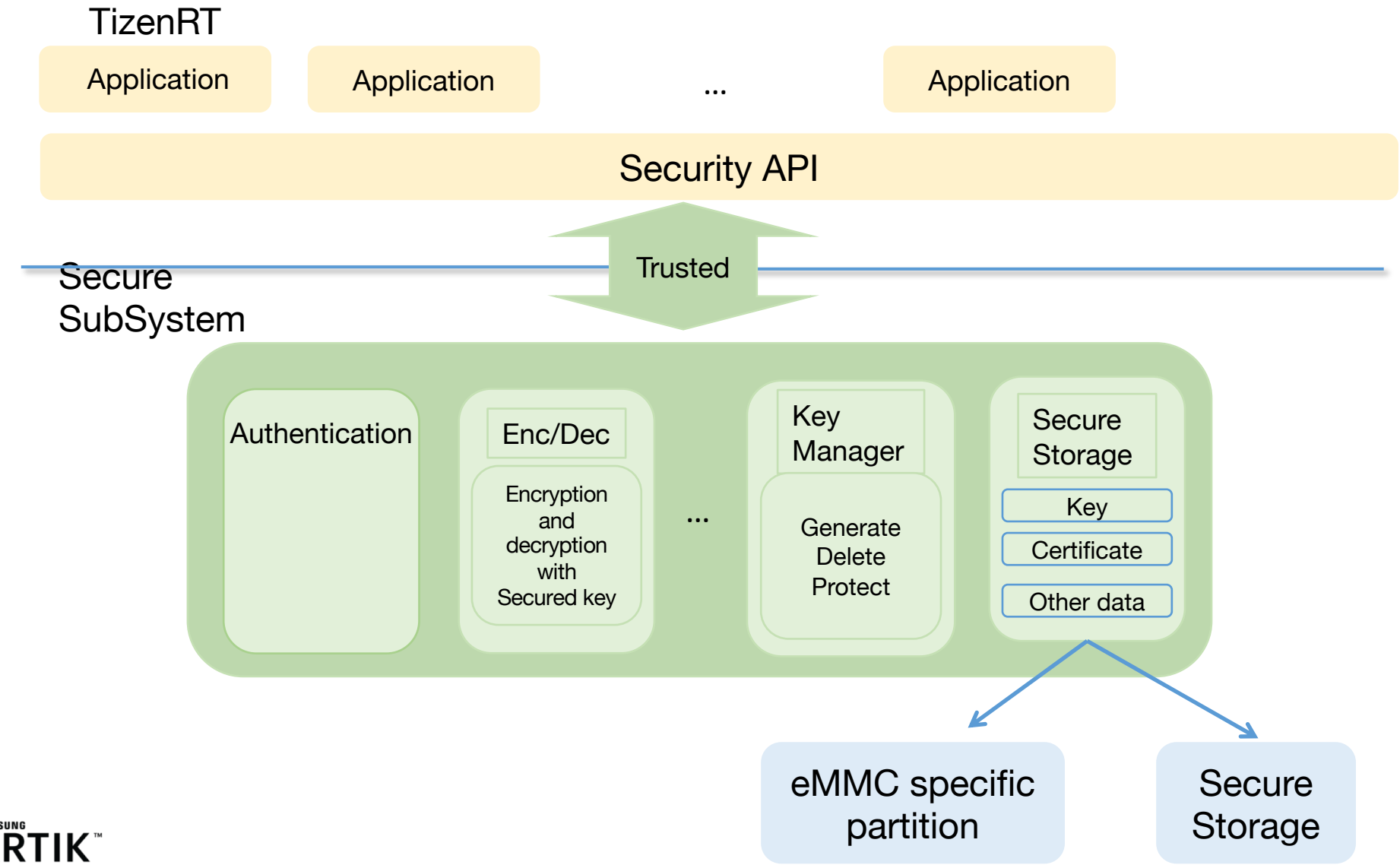
SAMSUNG ARTIK™

Device Protection

		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	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™

ARTIK SEE Architecture



ARTIK SEE 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)	

ARTIK SEE 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

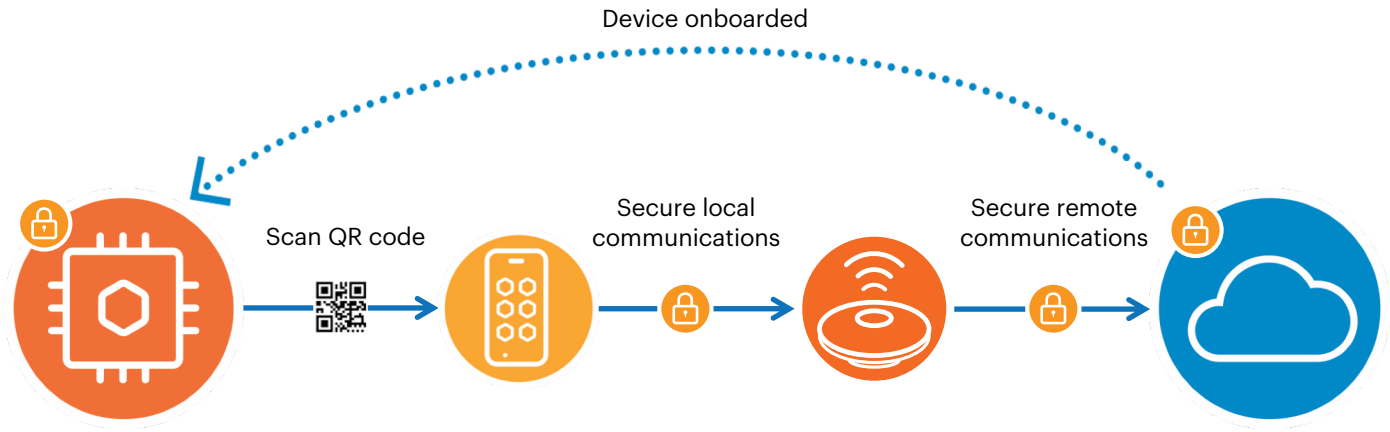
Device Protection

		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	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™

Platform Security

Secure Device Registration



ARTIK-based device

- Hardware root of trust
- Pre-injected certificates and keys
- Secure element/PUF
- Data encryption
- Secure storage

ARTIK mobile app

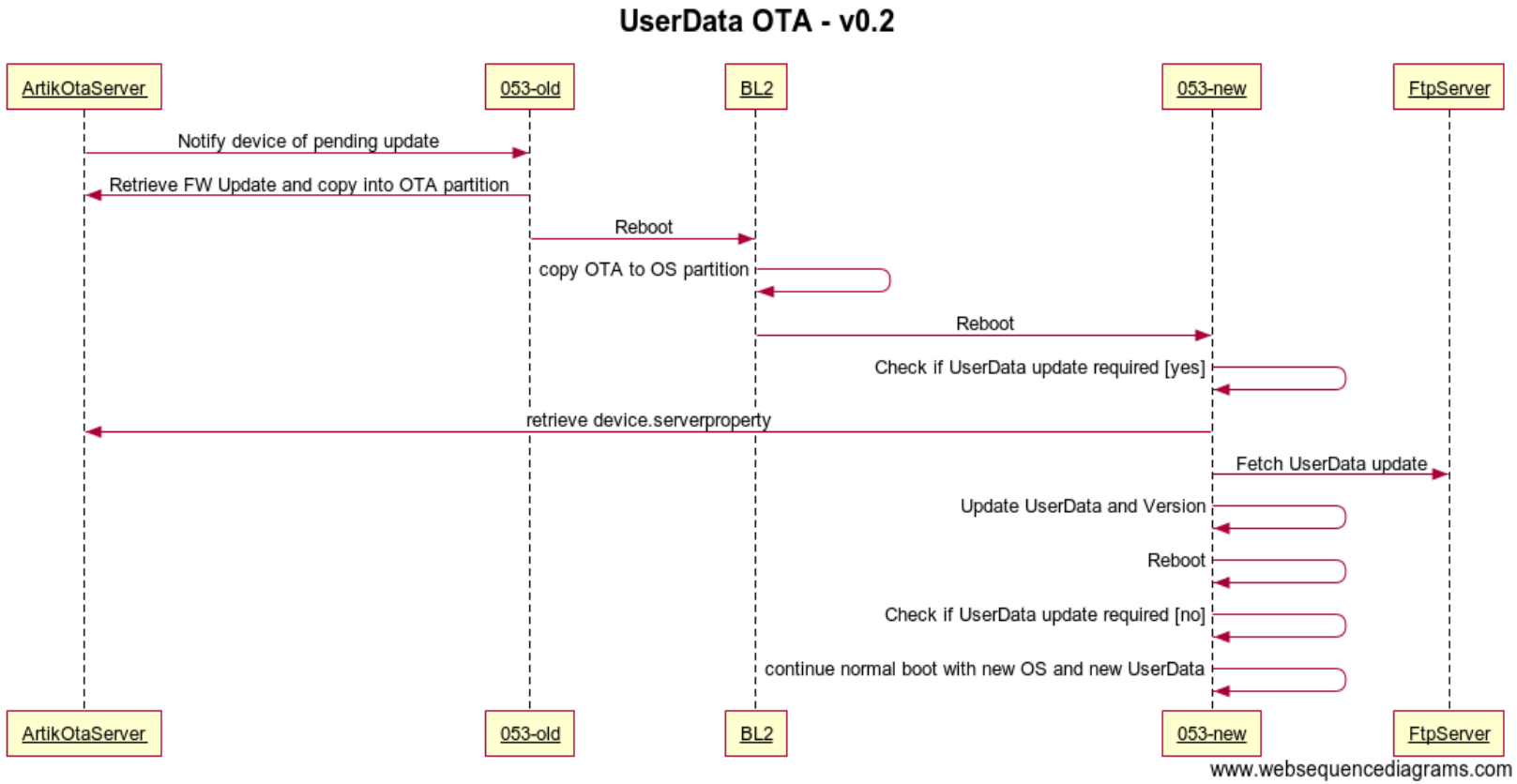
SmartThings Cloud

ARTIK cloud services

- Authentication
- Authorization
- Device whitelisting
- Data encryption

SAMSUNG ARTIK™

Secure OTA



SSS R/W Key(512KB)	Secure Storage
Wi-Fi NVRAM(8KB)	WiFi RAM
User R/W (1400KB)	SmartFS
OTA download (1536KB)	OTA Image
Factory Reset (1536KB)	Factory Reset OS Image(compressed image)
OS AREA TizenRT (2400KB)	TizenRT Tinyara_head.bin
Wi-Fi F/W (512KB)	WiFi firmware wlanfw.bin
SSS F/W (32KB)	sssfw.bin
BL2 (192KB)	2nd stage bootloader, bl2.bin
SSS R/O Key (48KB)	secure boot key
BL1 (16KB)	1st stage bootloader, bl1.bin

SAMSUNG ARTIK™

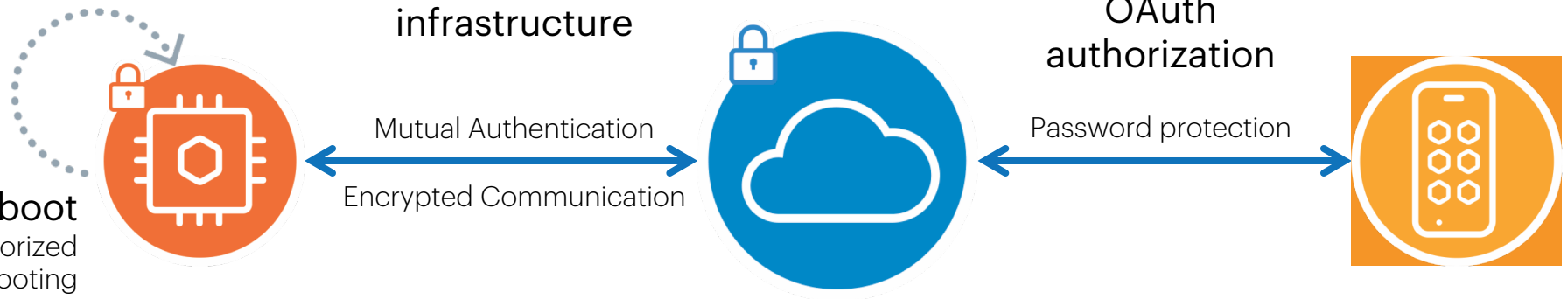
Samsung ARTIK™ End-to-end Platform Security

End-to-end protection for you and your customers

ARTIK Modules

SmartThings Cloud

Mobile apps



Secure boot
Prevents unauthorized software from booting and running on device

Secure OS
Hardware-enforced secure applications

Secure storage
Data encryption

Authentication and authorization, Secure OTA
Cloud services are protected

User data encryption
Protects sensitive info on mobile devices

SAMSUNG ARTIK™

Samsung ARTIK™ End-to-end Platform Security*

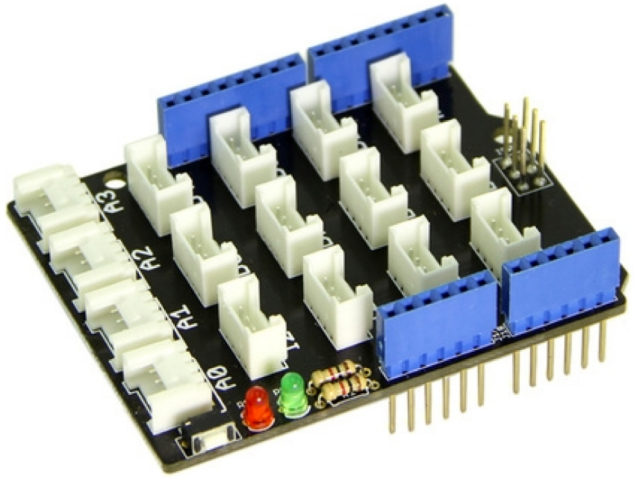
	Feature	ARTIK
Modules	Secure element key storage, secure boot	**Included**
	Security infrastructure: PKI and KMS	**Included**
	Unique device ID and certificate	**Included**
	Secure data storage with data encryption	**Included**
Platform software	Secure device registration	**Included**
	Secure OTA updates	**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; OAuth2; client side certificates	**Included**

SAMSUNG ARTIK™

* Feature list is not exhaustive

ARTIK 05x Ecosystem

Grove Base Shield and Modules Support



Grove - Digital Light Sensor

Grove - Light Sensor

Grove - Temperature and Humidity Sensor

Grove - Barometer Sensor

Grove - Dust Sensor

Grove - Gas Sensor

Grove - Temperature Sensor

Grove - Air Quality Sensor

Grove - Temperature and Humidity Sensor Pro

Grove - Gas Sensor(O_2)

Grove - HCHO Sensor

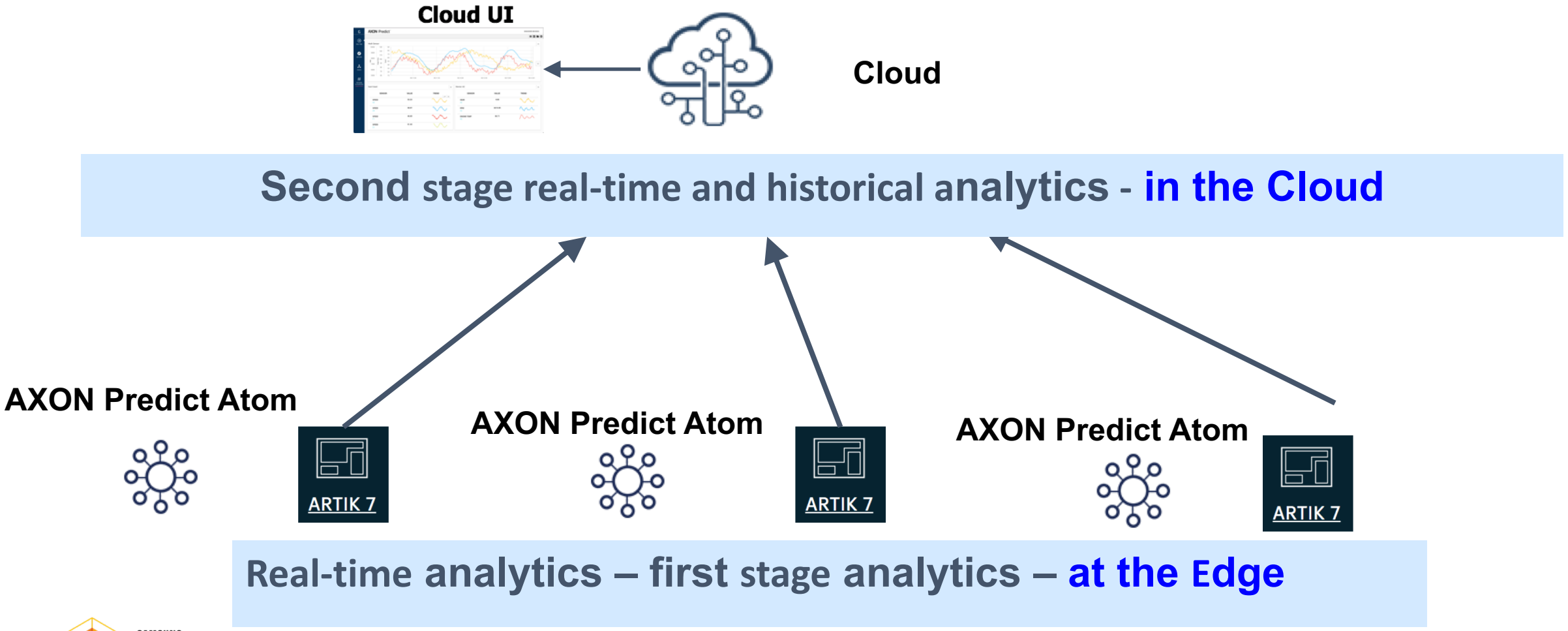
SAMSUNG ARTIK™

Use Case: iCast 2

- ARTIK 05x Module
- Wi-Fi 2.4GHz, BLE 5.0 including 802.15.4 Radio and Thread SW stack
- Analog I/O, GPIO, I2C etc.
- Isolated RS485 serial port
- Supports ARTIK Cloud, AWS IoT, PTC ThingWorx

SAMSUNG ARTIK™

Use Case: Edge Analytics



SAMSUNG ARTIK™ • Real-time analytics, pattern and anomaly detection on device and for connected devices

Use Case: Location Service

SAMSUNG ARTIK™

3rd Party Cloud Support

1. AWS IoT: `https://github.com/Samsung/TizenRT/tree/master/external/aws`
2. Microsoft Azure:
3. PTC ThingWorx: `https://developer.artik.io/documentation/artik-05x/tutorials/thingworx.html`
4. Other Cloud services that support REST API, MQTT etc.

Samsung ARTIK™

Helpful web resources

Web Documentation	https://developer.artik.io/documentation/
Document Library	https://www.artik.io/library/
Forums	https://developer.artik.io/forums/
Blog	https://www.artik.io/blog/
File Tickets	https://support.artik.io
Github Repository	https://github.com/SamsungARTIK
YouTube Channel	https://www.youtube.com/channel/UC4rolvSm8ikmnymdbbznNJw

Samsung ARTIK™ IoT Platform

Enterprise-grade technology for your IoT business

End-to-end security
Integrated security features span ARTIK cloud, modules, and software

Reduces development time, costs, and risks
Integrated, fully-tested, production-ready, secure components speed time-to-market, minimize the need for in-house IoT expertise

Open and interoperable
No lock-in; ARTIK works with existing products and infrastructure to share information, orchestrate complex interactions, and support business growth

Serviceability
Provision, manage, and update devices and services over-the-air and on-the-fly throughout the product lifespan

SAMSUNG ARTIK™

Appendix

Samsung ARTIK™ Edge-node Portfolio

New products

NDA

		020	030	053	053s	055s
Processor		Cortex M4 @ 40MHz	Cortex M4 @ 40MHz	Cortex R4 @ 320MHz	Cortex R4 @ 320MHz	Cortex R4 @3 20MHz
Memory	RAM	32 KB	32 KB	1.4 MB	1.4 MB	1.4 MB
	Flash	256 KB	256 KB	8 MB	8 MB	8 MB
Connectivity		BLE 4.2	ZigBee / Thread	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11 b/g/n
Security	Per device unique key & certificate			✓	✓	✓
	Key stored in HW secure element			✓	✓	✓
	PKI infrastructure			✓	✓	✓
	KMS, secure boot, secure JTAG				✓	✓
	Secure OS, Security Lib APIs, Secure Storage				✓	✓
Operating Voltage		3.3V	3.3V	5-12V	5-12V	3.3V
Temperature Range		-40º to 85°C Ambient	-40º to 85°C Ambient	-20º to 85°C Tcase	-20º to 85°C Tcase	-20º to 85°C Tcase
Size (mm)		15 x 12.9 x 2	15 x 12.9 x 2	15 x 40 x 3.9	15 x 40 x 3.9	15 x 26 x 3.9
Availability	Samples					
	Production	Now	Now	Now	Nov. 30th 2017	Nov. 30th 2017

Samsung ARTIK™ Gateway Portfolio

New products

NDA

		520	530	710	530s	710s
Processor	CPU	Dual Cortex-A7 @ 1.0 GHz	Quad Cortex-A9 @ 1.2 GHz	Octa Cortex-A53 @ 1.4 GHz	Quad Cortex-A9 @ 1.2 GHz	Octa Cortex-A53 @ 1.4 GHz
	GPU	3D graphics accelerator	3D graphics accelerator	3D graphics accelerator	3D graphics accelerator	3D graphics accelerator
Memory	RAM	512 MB	512 MB	1 GB	512 MB/1 GB	1 GB
	Flash	4 GB	4 GB	4 GB	4 GB	4 GB
Connectivity	Wi-Fi	802.11 b/g/n/ac	802.11 b/g/n	802.11 a/b/g/n	802.11 b/g/n	802.11 a/b/g/n/ac
	Bluetooth	4.x	4.x	4.x	4.x	4.x
	Zigbee, Thread	✓	✓	✓	✓	✓
	Ethernet		1 channel (10/100/1000 x1)	1 channel (10/100/1000 x1)	1 channel (10/100/1000 x1)	1 channel (10/100/1000 x1)
	CAN					
Temperature Range (T_J)		-25º to 85º C	-25º to 85º C	0º to 70º C	-25º to 85º C	0º to 70º C
Size (mm)		30 x 25 x 3.4	36 x 49 x 3.4	36 x 49 x 3.4	36 x 49 x 3.4	36 x 49 x 3.4
Availability	Samples					
	Production	Now	Now	Now	Nov. 30, 2017	Nov. 30, 2017

Q & A