ARTIK Security

Wei Xiao

June 2, 2018

SAMSUNG ARTIK™

Agenda

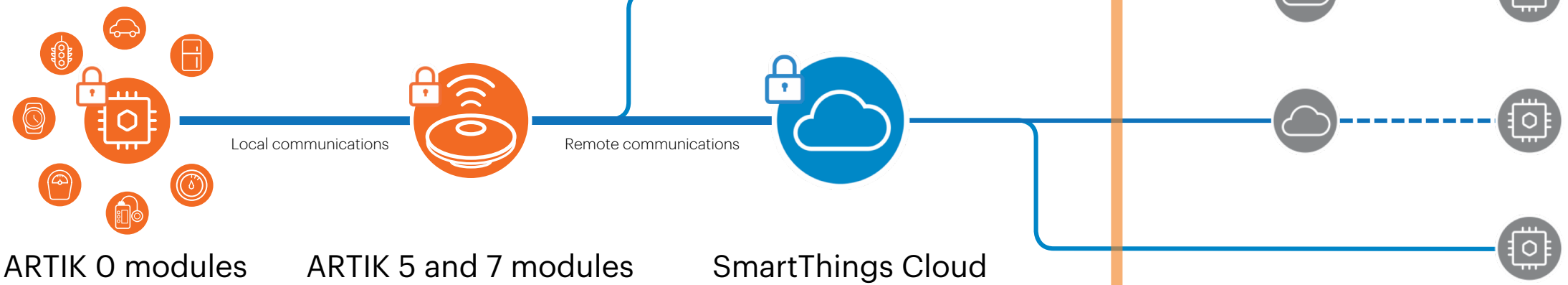
- ARTIK Module Security
- ARTIK Platform Security

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™

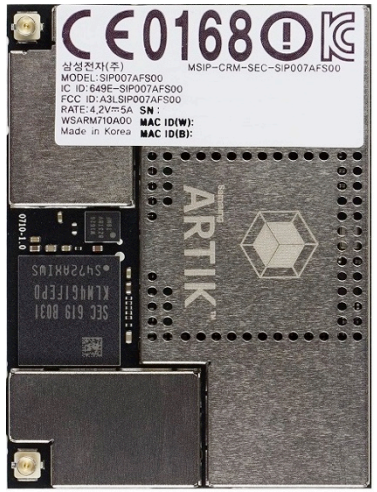
ARTIK Module Security

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

Security Questionnaire

How do you provide security across all attack surfaces?

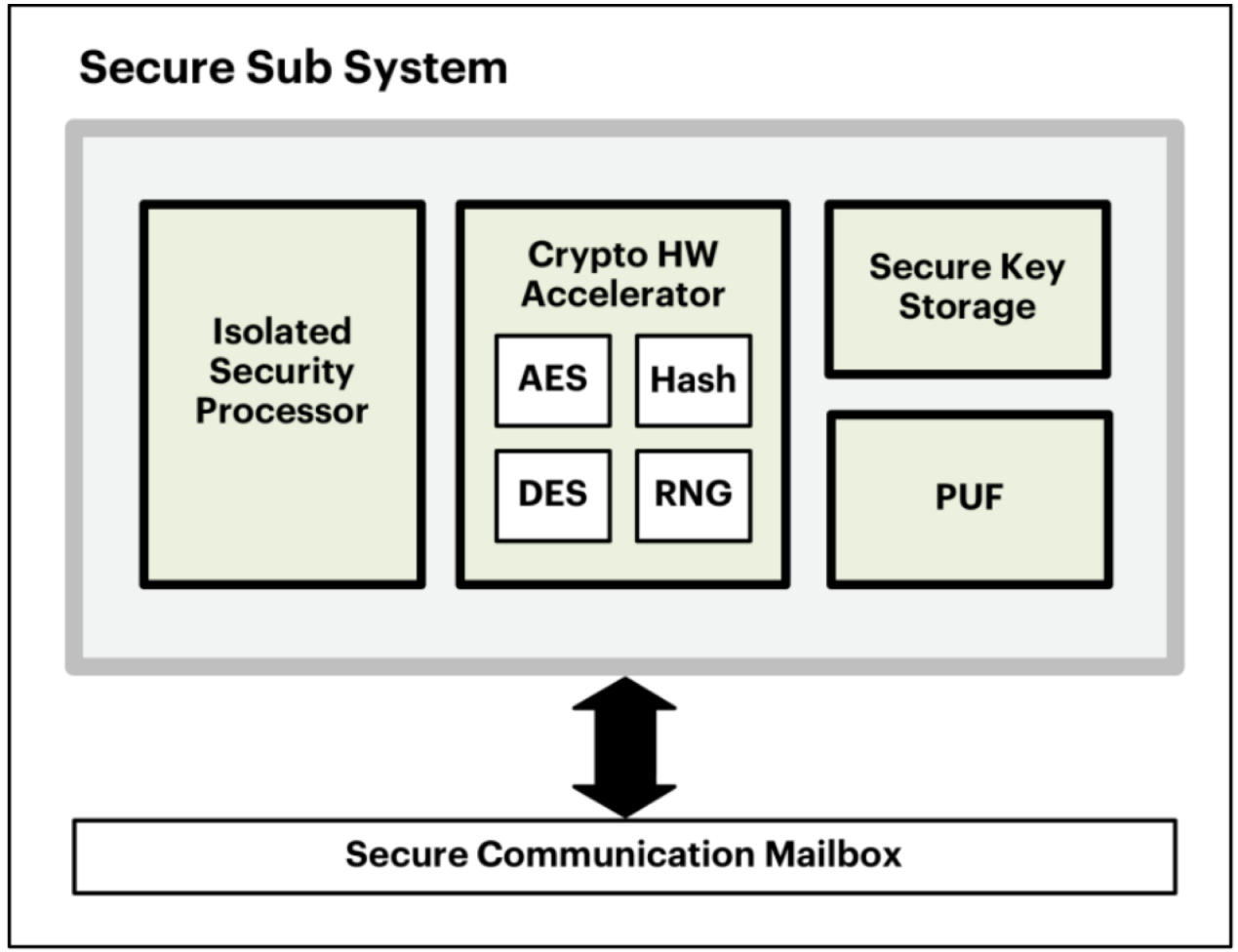
Question	ARTIK 5/7/053
Do you support secure communication from device to device or device to cloud? How do you secure communication? Are you using TLS1.2 or higher?	Yes, HTTPs using TLS 1.2
How do you establish identity of device?	Using unique certificate on each device
How does the device establish 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
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? Are your certificate and keys safe if software is hacked?	Specialized HW on module (secure element)
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)
How do you guarantee your firmware integrity?	Secure Boot

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™

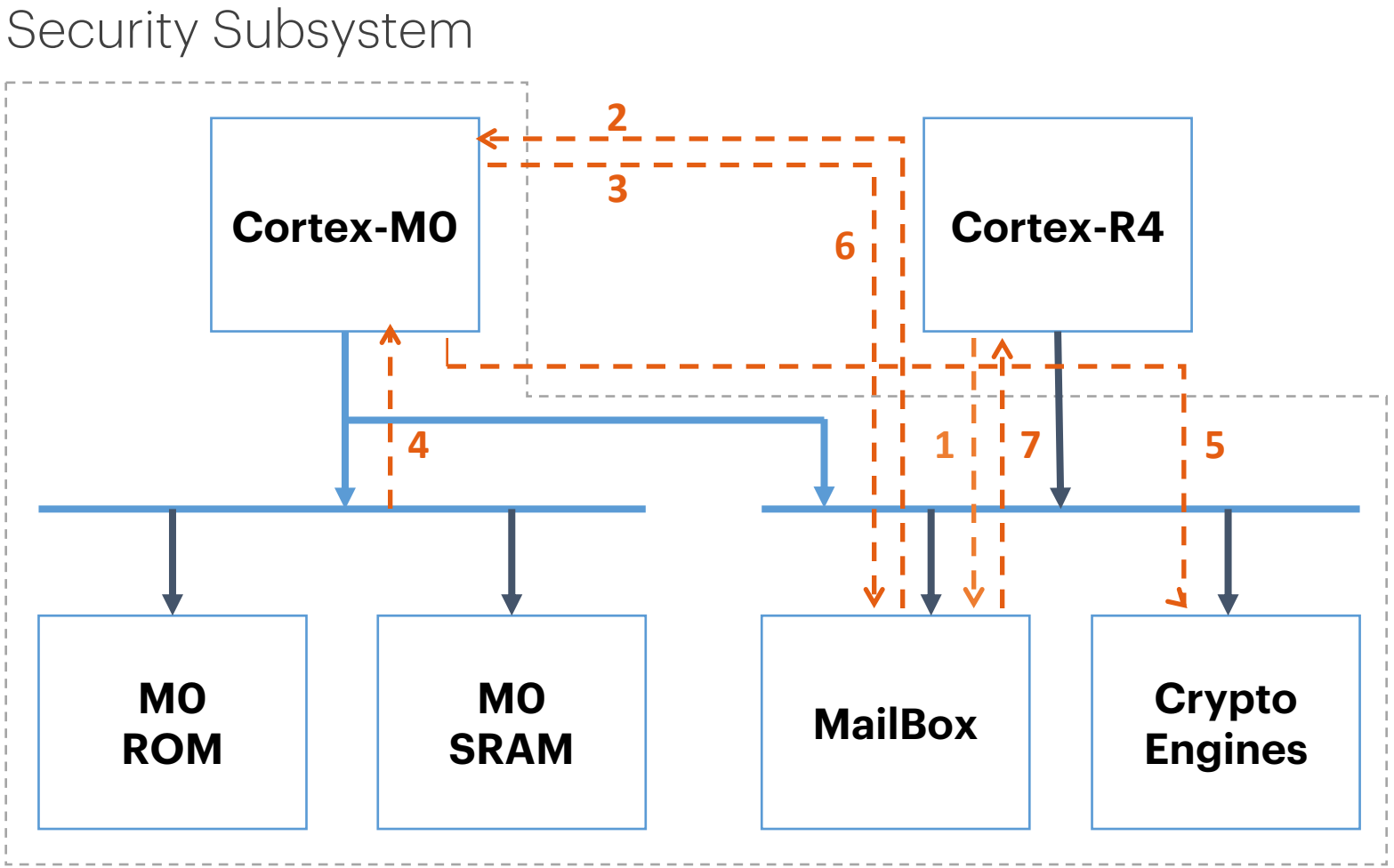
ARTIK 05x Security Subsystem



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

SAMSUNG ARTIK™

Isolated Security Processor



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

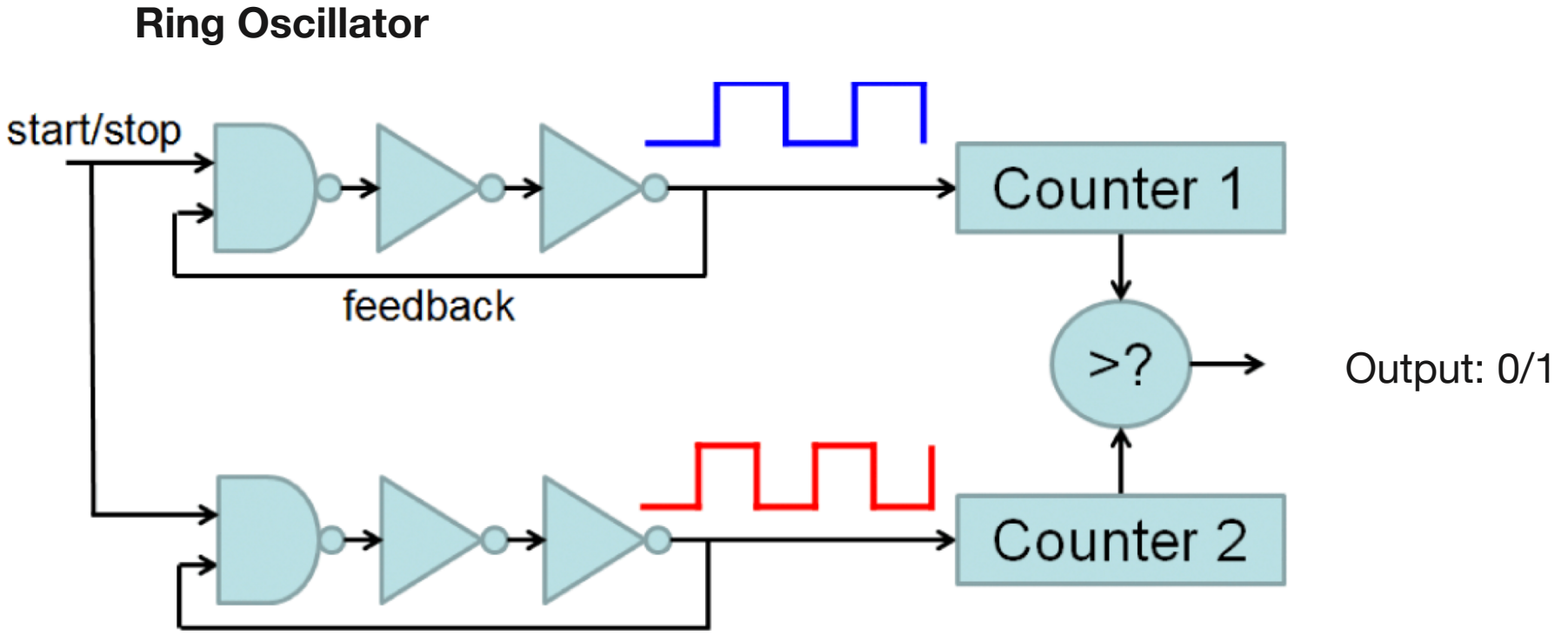
PUF (Physically Unclonable Function)

- 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:
  - Key generation and storage
  - Device identification
  - IP Protection
  - Protocols with challenge-response pairs

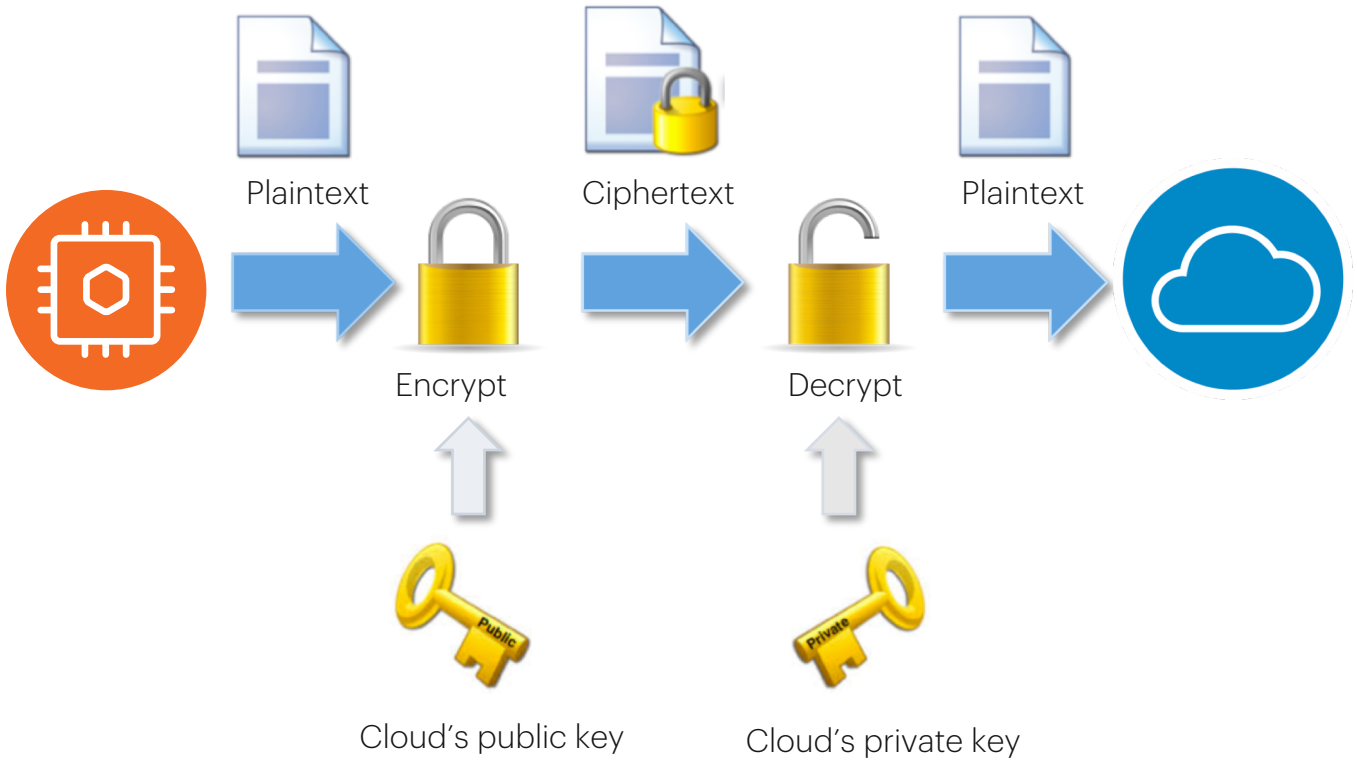
SAMSUNG ARTIK™

RO Frequency PUF

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

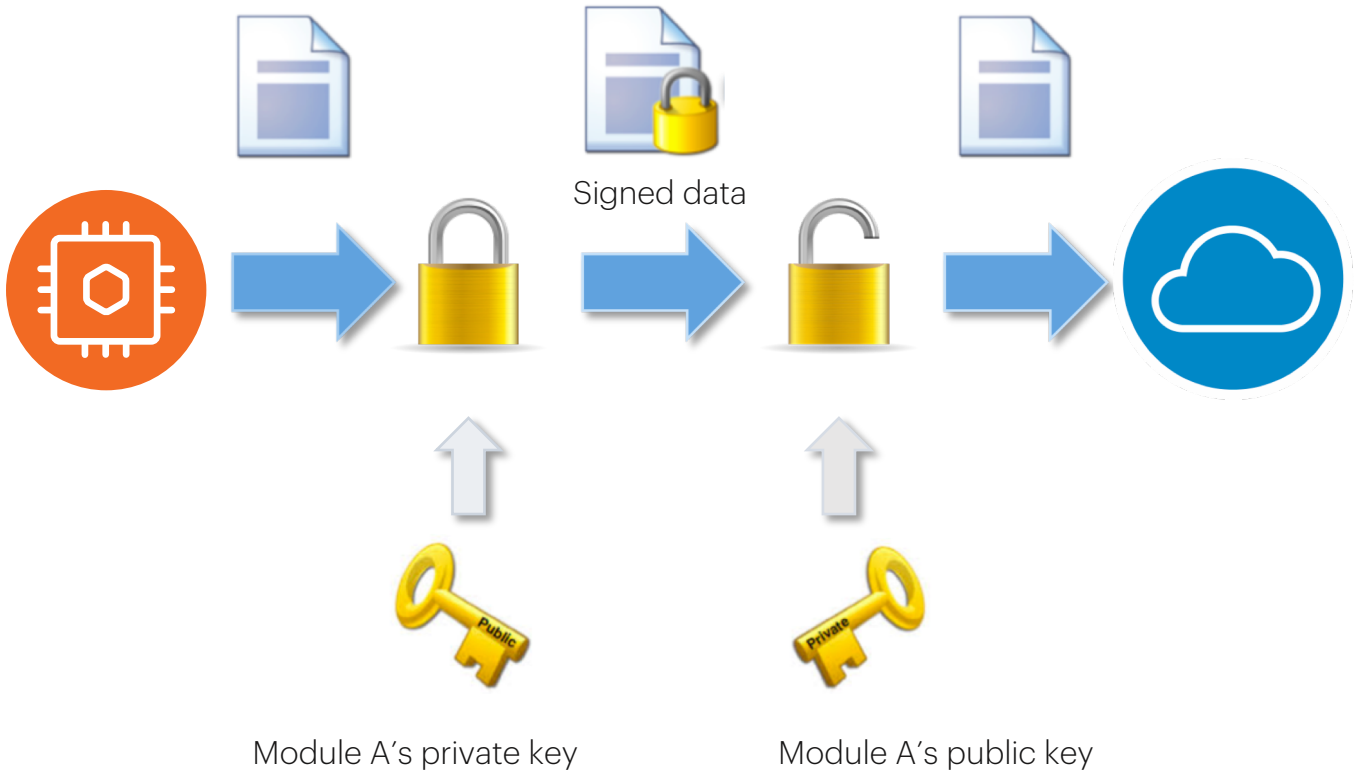


Encryption and Decryption



Different keys are used to encrypt and decrypt messages

Signature

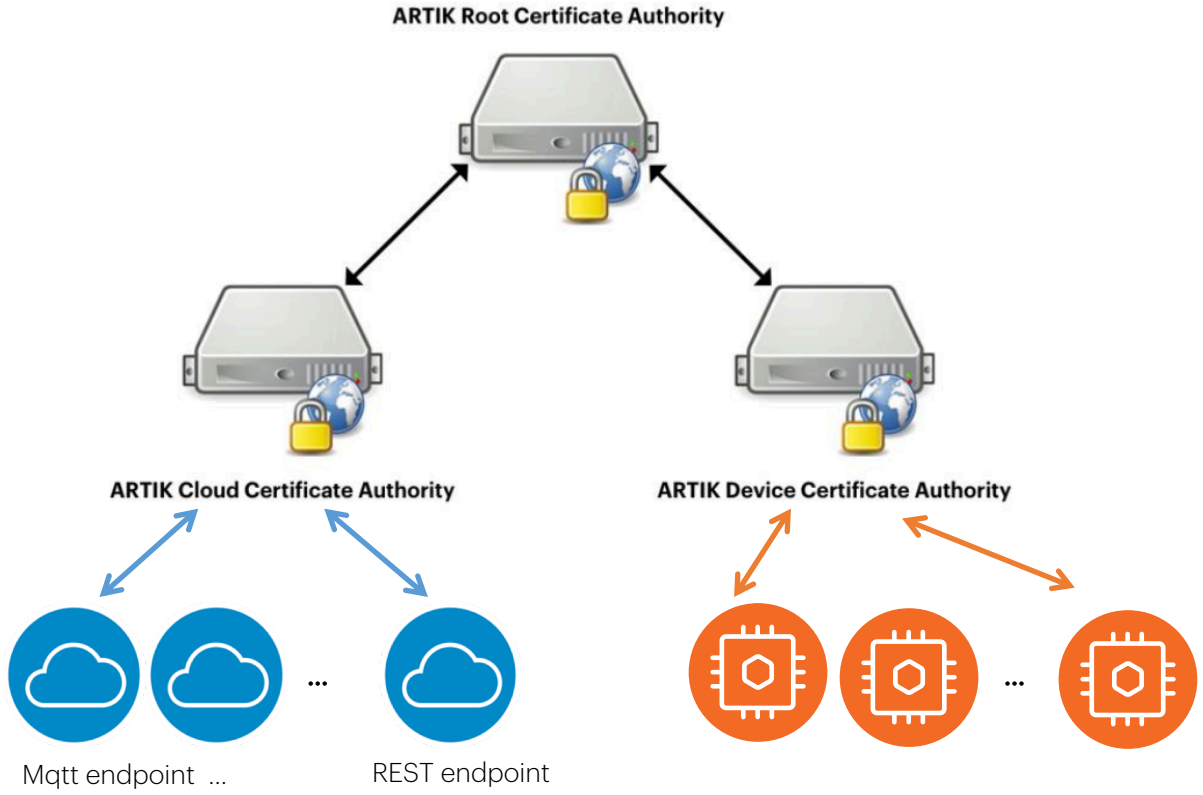

Signed data
Public
Private
Module A's private key
Module A's public key

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 its own PKI, which is used to generate and apply unique certificates and key pairs to each ARTIK Module during manufacturing.

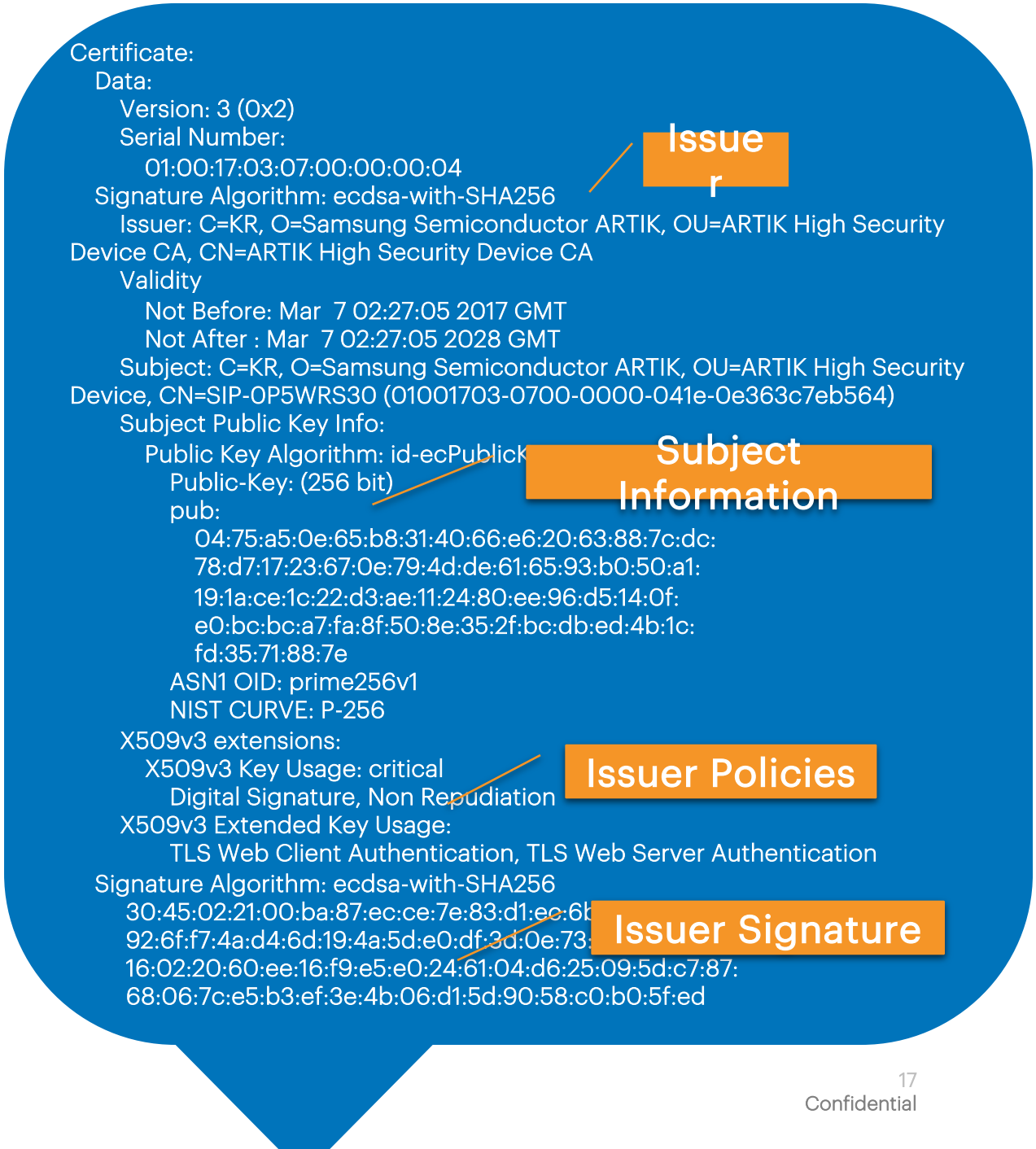
ARTIK Root CA

- PKI's core concept is (Digital) Certificate. Issued by a **Certificate Authority**, e.g, GlobalSign, Symantec
- ARTIK Root CA



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 ARTIK modules, you need to generate your own certificate/key-pair
- We can use Post Provisioning to post provision customer credentials(key, certificate) to Secure Element

SSL/TLS/DTLS

- Transport Layer Security(TLS) and its predecessor, Secure Socket Layer(SSL) are cryptographic protocols designed to provide communication security.
- Use X.509 certificates(asymmetric) cryptography to authenticate the counterparty
- Negotiate a symmetric session key, which is to be used for data encryption
- DTLS is an implementation of TLS over UDP

Secure Communication

ARTIK Modules support:

- A unique pair of key and cert from ARTIK PKI
- True random number generator
- Cryptographic Accelerator, Encoding and decoding of packages
- TLS/DTLS library for creating the channel
- OpenSSL Engine which takes advantage of the hardware accelerated ARTIK security library to get keys from the secure element, encrypt and decrypt, encode and decode.. (Supported OpenSSL Ciphers: ECB, CBC, CTR etc.)

Secure Communication

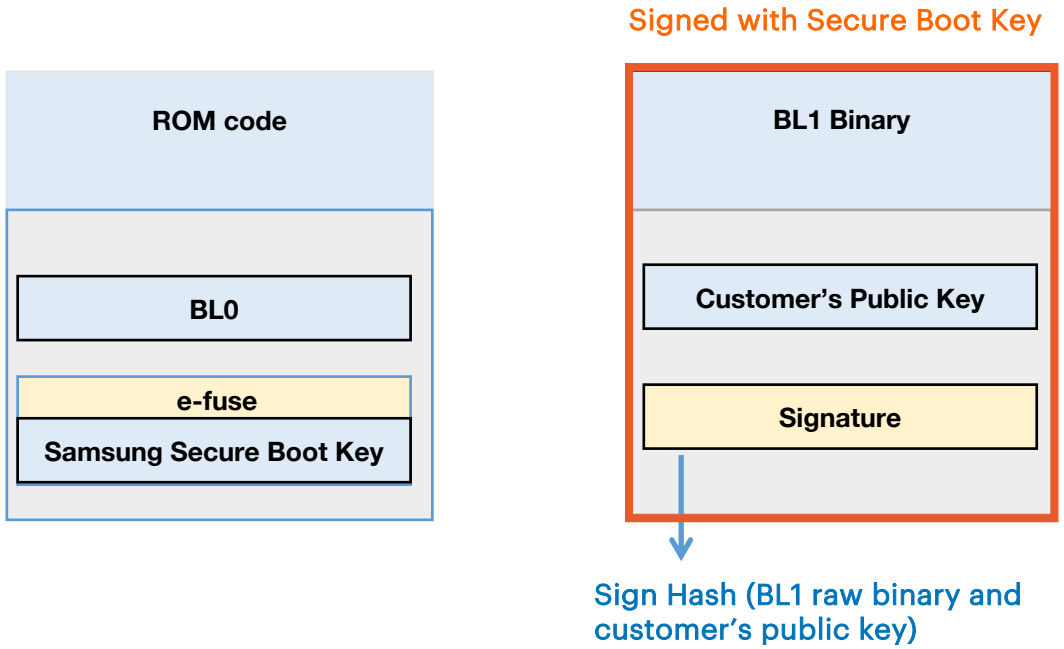
		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to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

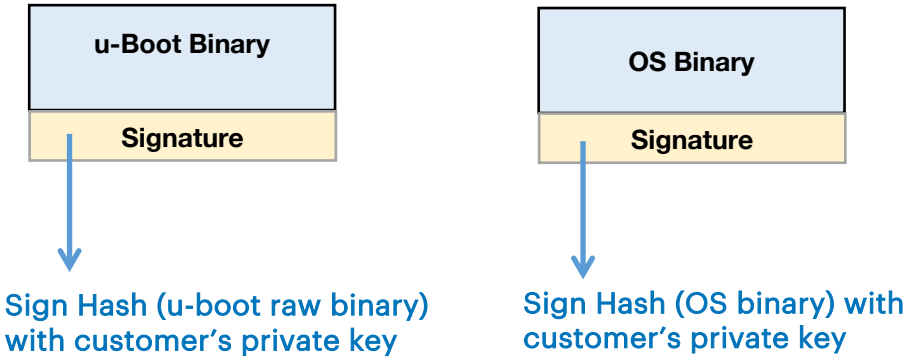
Secure Boot

- 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

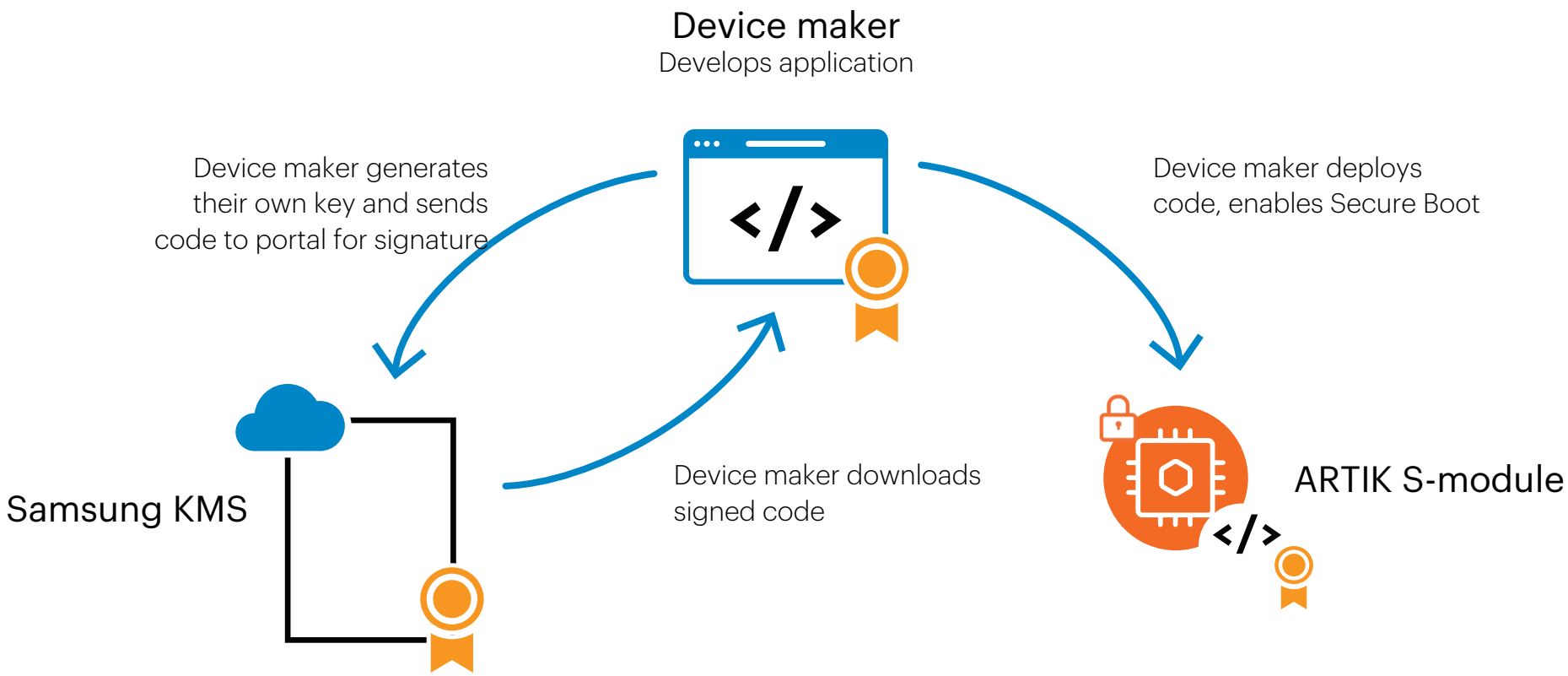
SAMSUNG ARTIK™

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

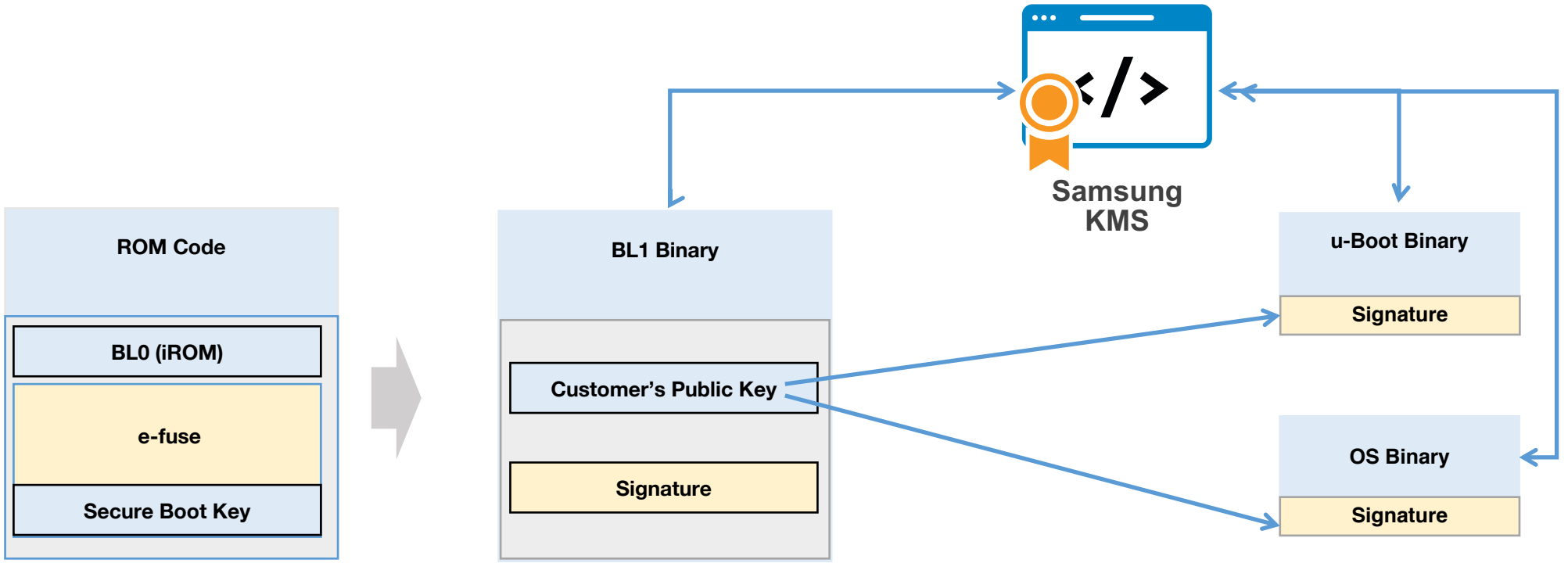


SAMSUNG ARTIK™

Key Management System

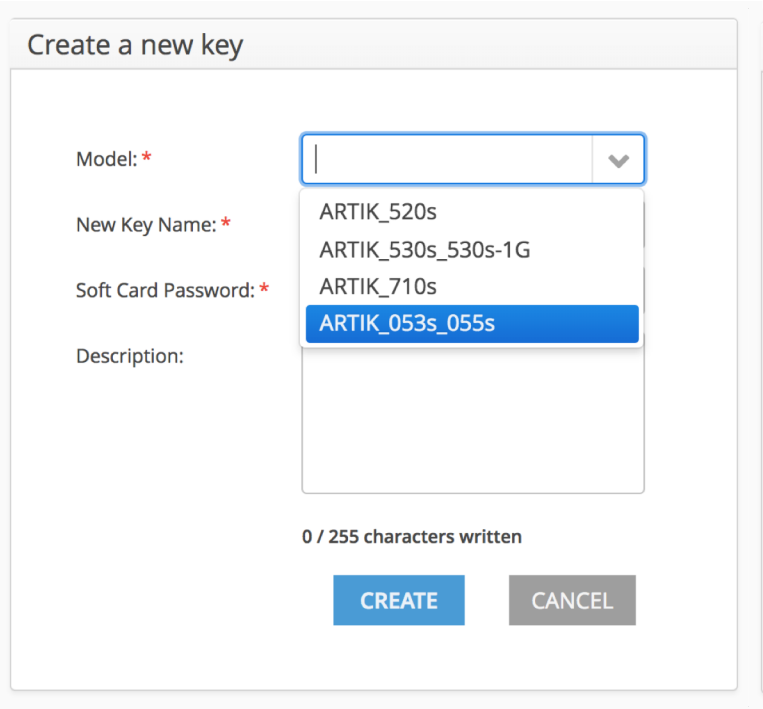
- Signing keys are stored and operated within FIPS 140-2 certified Hardware security modules (HSM)
- Images are signed through a highly secure cryptography standard (SHA-256 w/ RSA2048 encryption)
- Strict access control policies
- Only accessible through whitelisted IP addresses

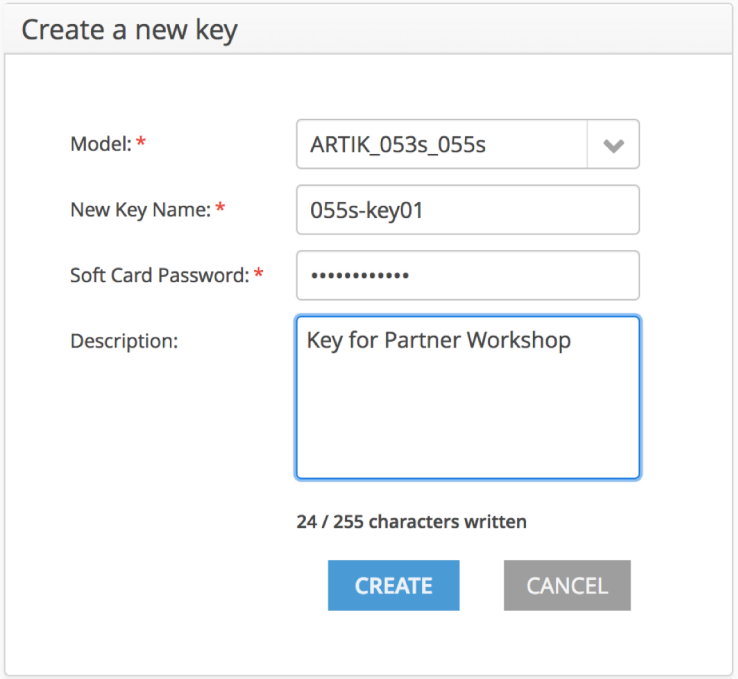
Key Management System Role

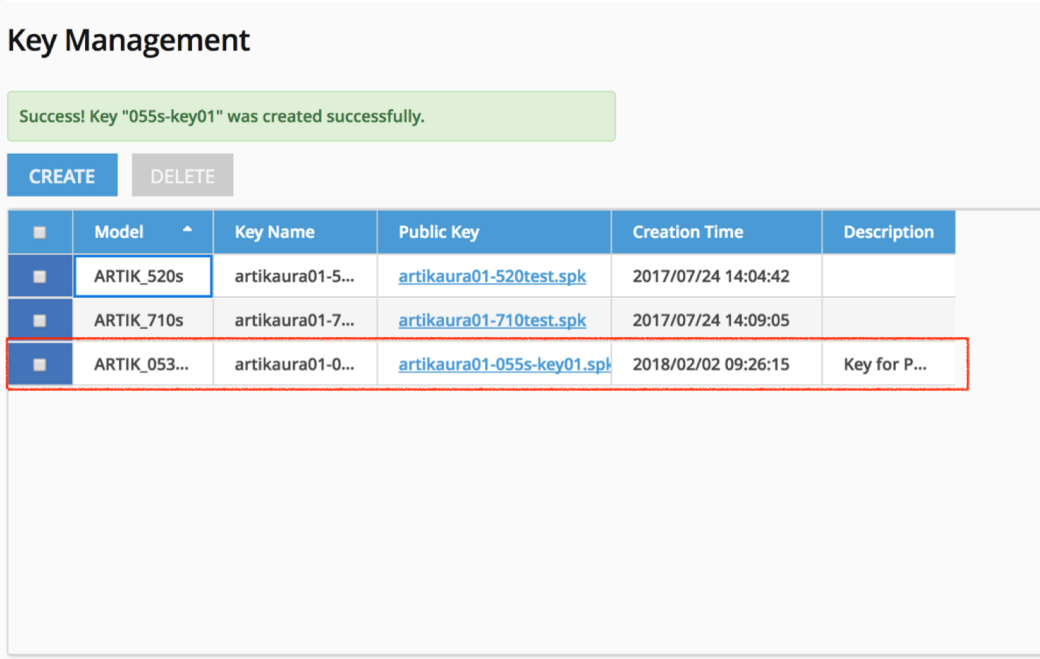


- BL1 image is provided by chip vendor

KMS Key Management







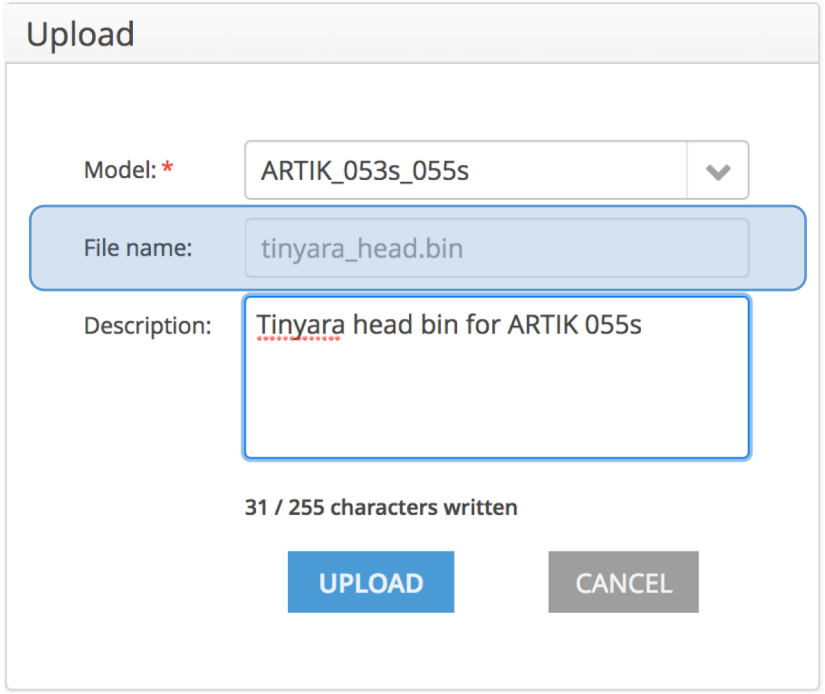
Stage 1:

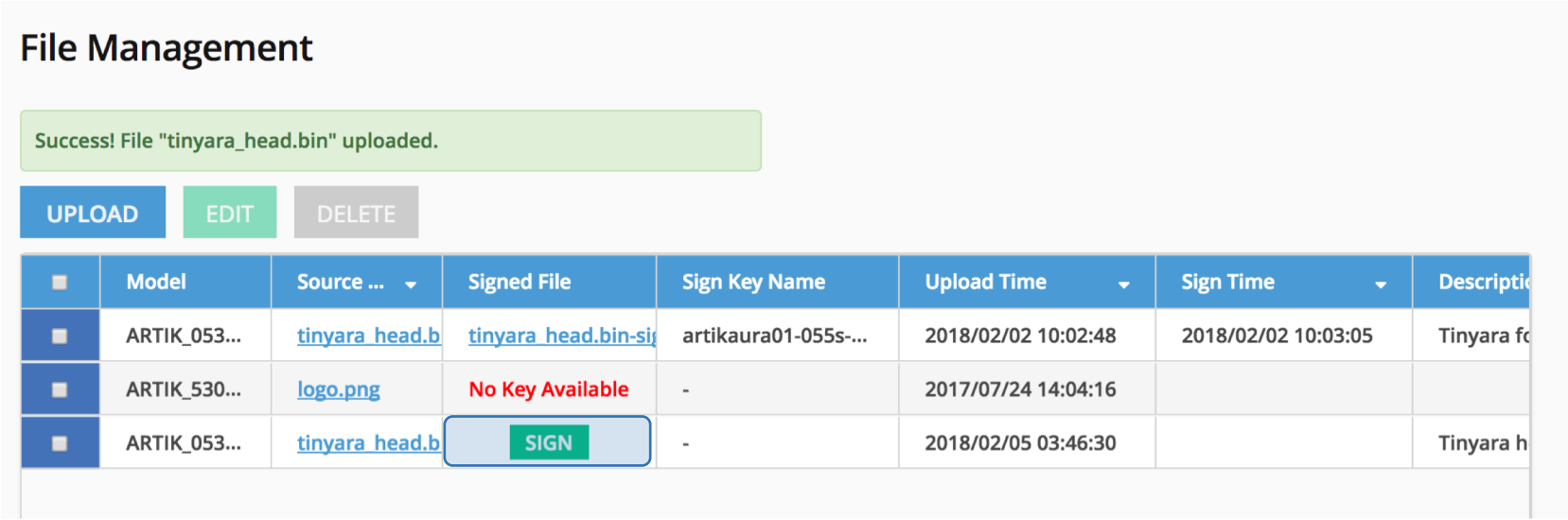
- Public key is immediately available on KMS portal
- Send ARTIK team the resulting public key.
- ARTIK team signs the bootloader stage 1 (BL1) image and deliver it to you by e-mail.

SAMSUNG ARTIK™

KMS File Management (Stage 2 Images)

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

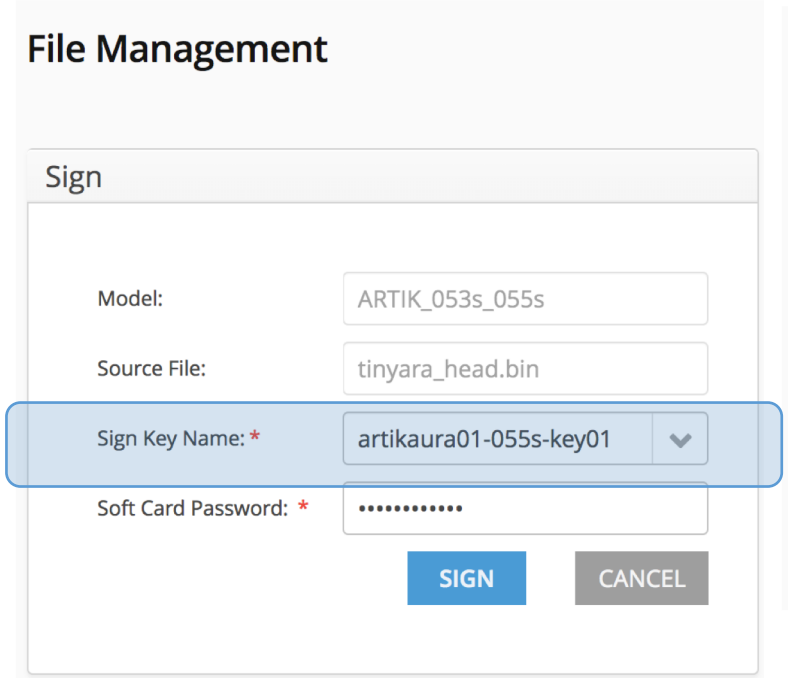


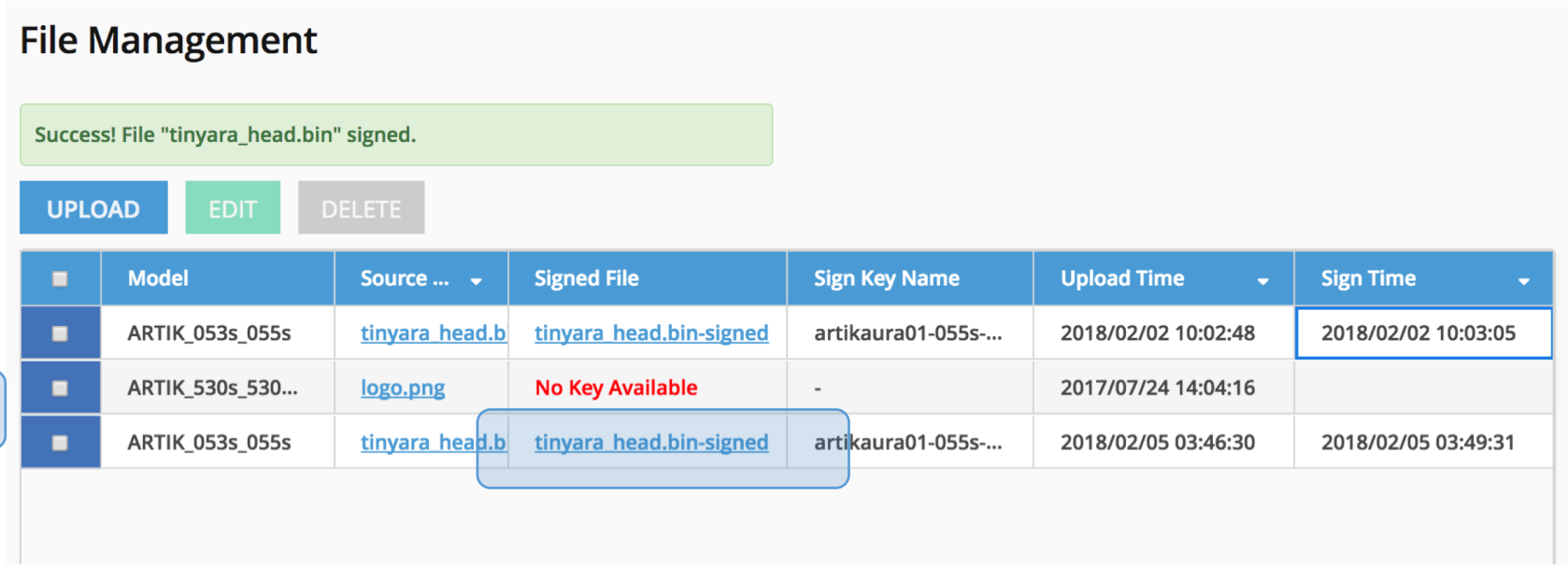


SAMSUNG ARTIK™

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

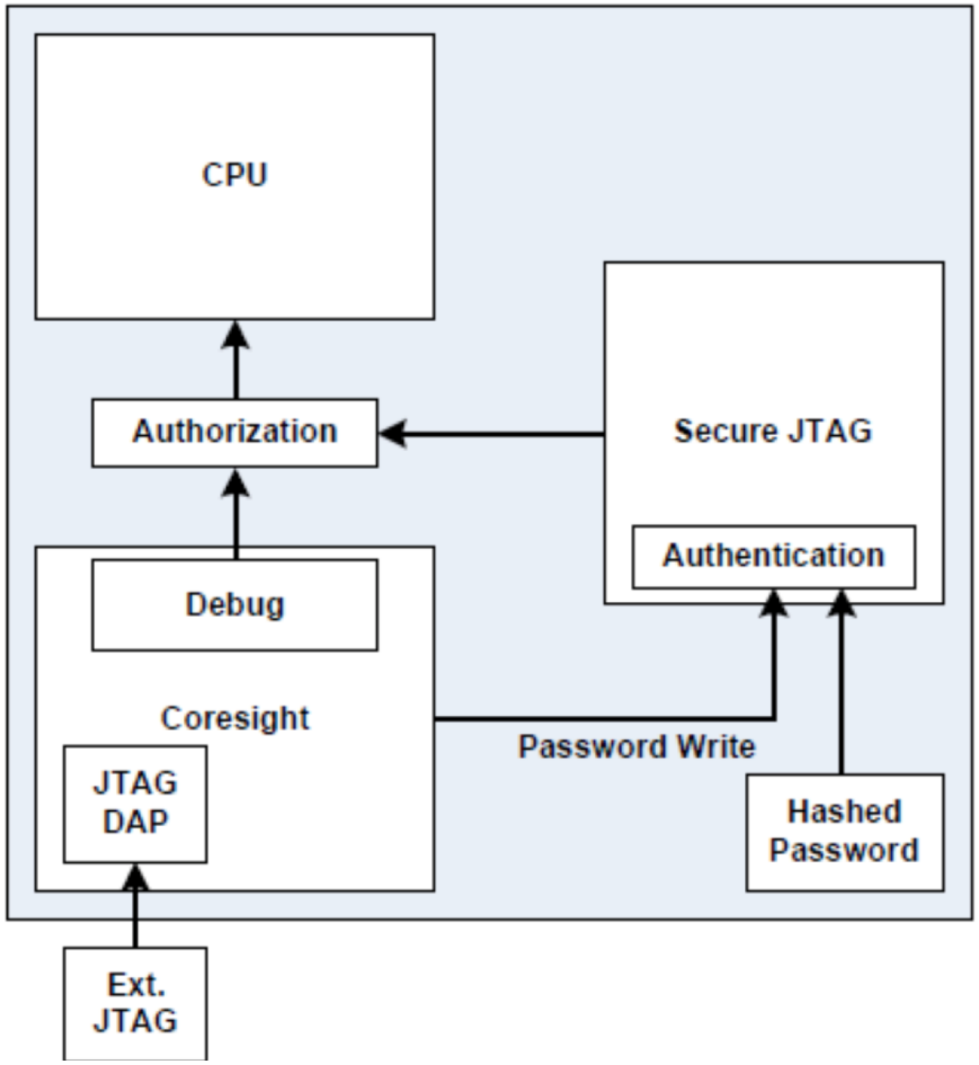
CUSTOMER

	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

- JTAG is disabled by default.
- Secure JTAG can be enabled to an OEM, where it requires a password to authenticates and authorizes JTAG access. The password is based on the serial number of module.
- The information is only made available through an authorized request to Samsung.



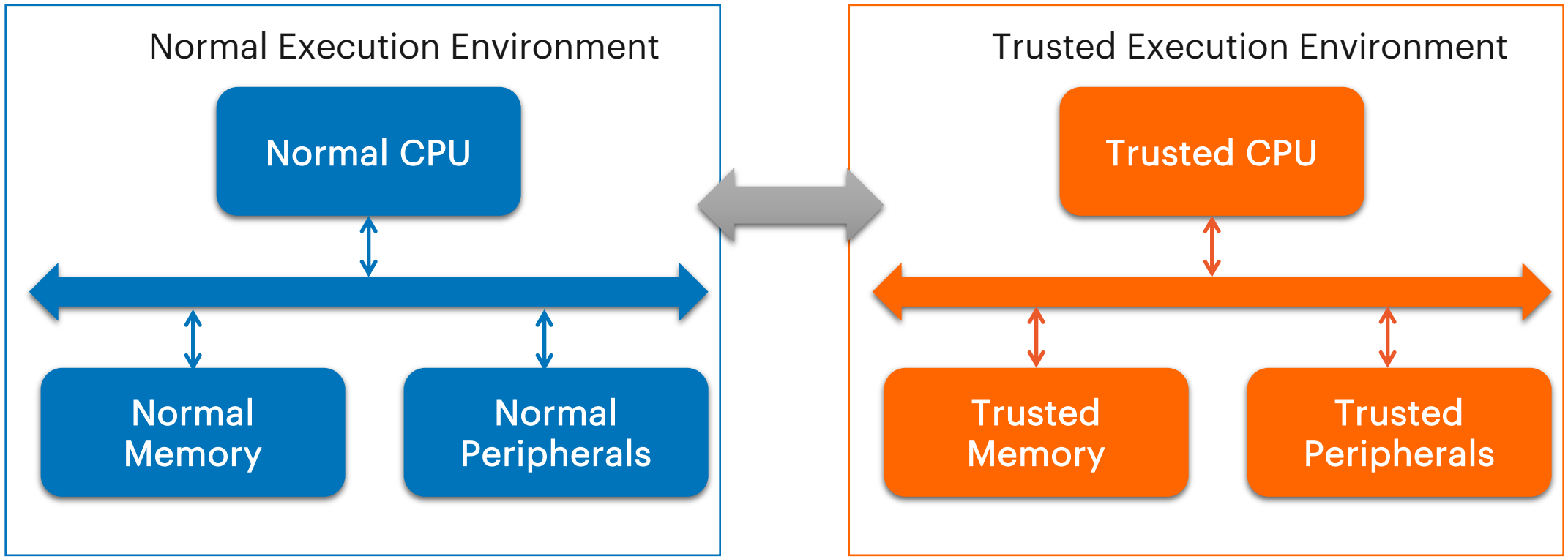
SAMSUNG ARTIK™

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™

Trusted Execution Environment on 5/7x (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

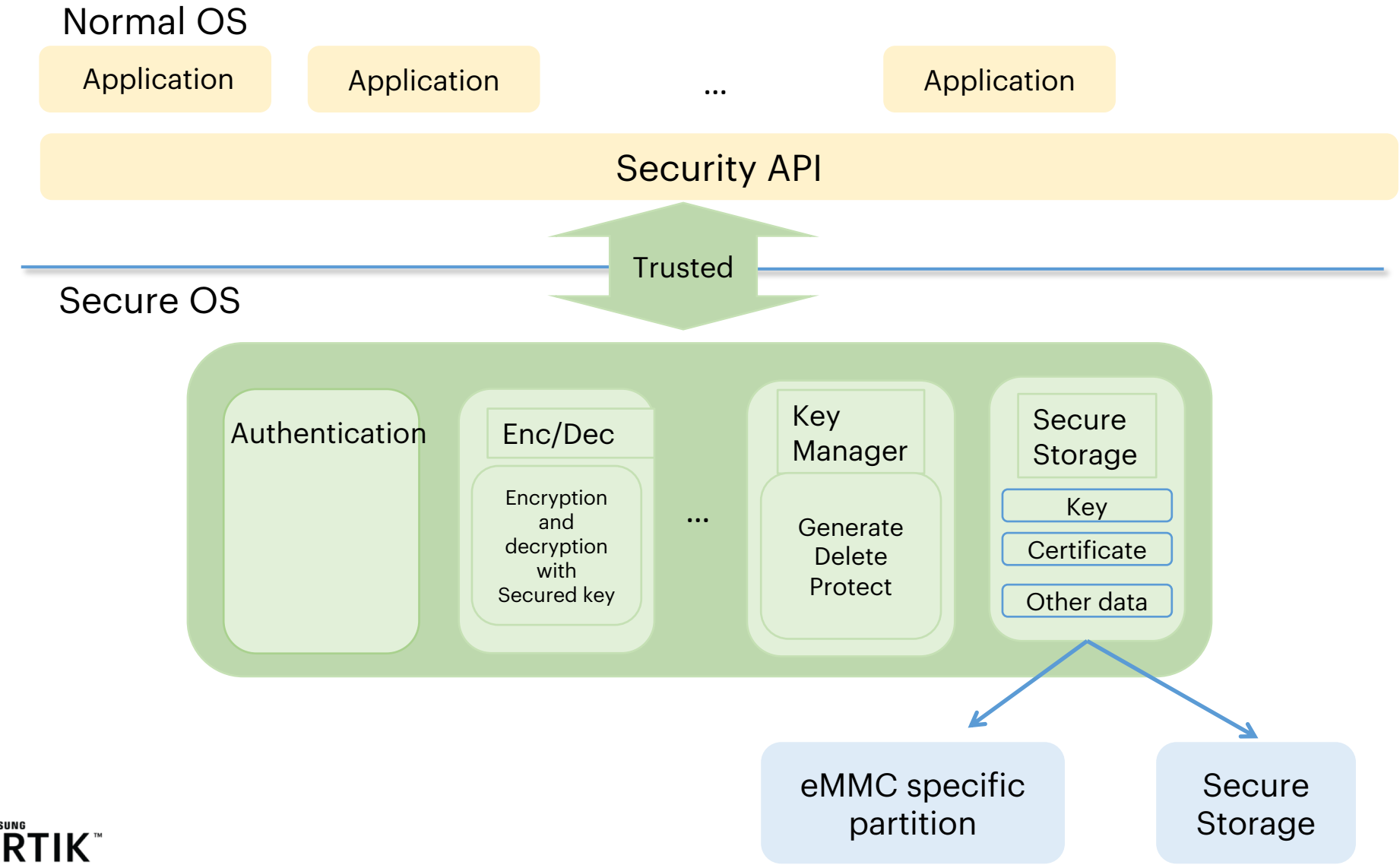
- eMMC file system (Flash-based)
  - Uses the same storage as the normal operating system. However, a specific partition is managed by Secure OS.
  - All data in this partition is encrypted with a unique key generated at run time, and is stored as a file unit of 32KB with a maximum of 1024 files that may be stored.
  - Applies to ARTIK 05x and 5/7 modules.

Secure Storage – Secure Element

Secure Element – an isolated storage device that supports 2 slots of ECDSA key pairs (16 AES 128-bit keys).

- The Secure Element provides high levels of security as hardware with anti-tamper measures.
- It includes cryptographic services such as random-number generation, key/data secure storage, and certificates handling and processing.
- All communication from the Secure Element to the processor is secured and encrypted.
- Uses Power glitch detector, Active Shield removal detector etc. 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 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)	

SAMSUNG ARTIK™

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

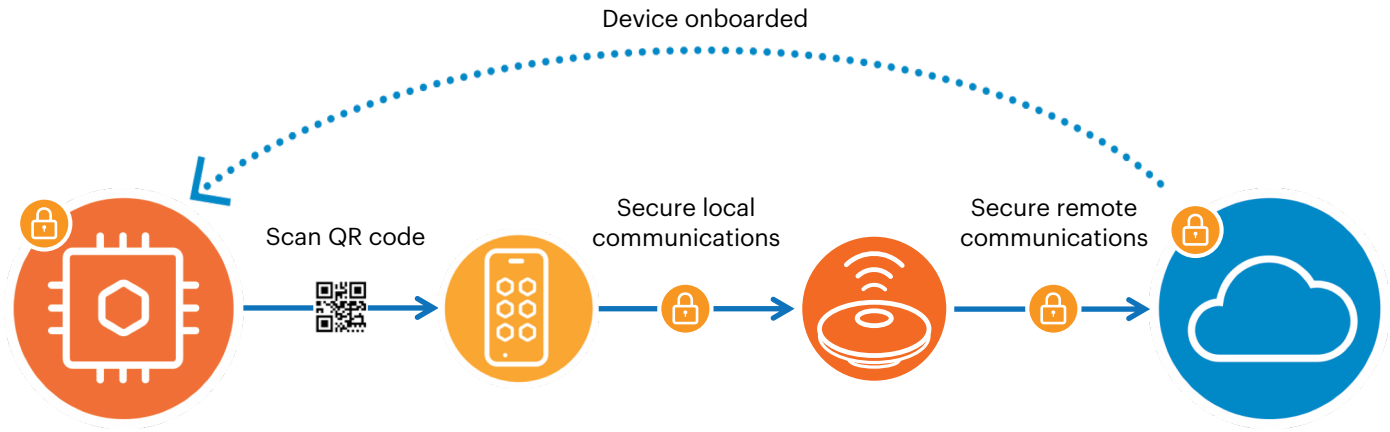
		ARTIK module (05x, 5, 7)	ARTIK S-module (053s, 055s, 530s, 710s)	Comments
Secure communication	Per device unique key & certificate	✓	✓	Uniquely identifies device
	Key stored in HW secure element	✓	✓	Secure key storage
	PKI infrastructure: Mutual authentication of device and cloud	✓	✓	Device talks to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

ARTIK Platform Security

SAMSUNG
ARTIK™

Secure Device Registration



ARTIK-based device

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

ARTIK mobile app

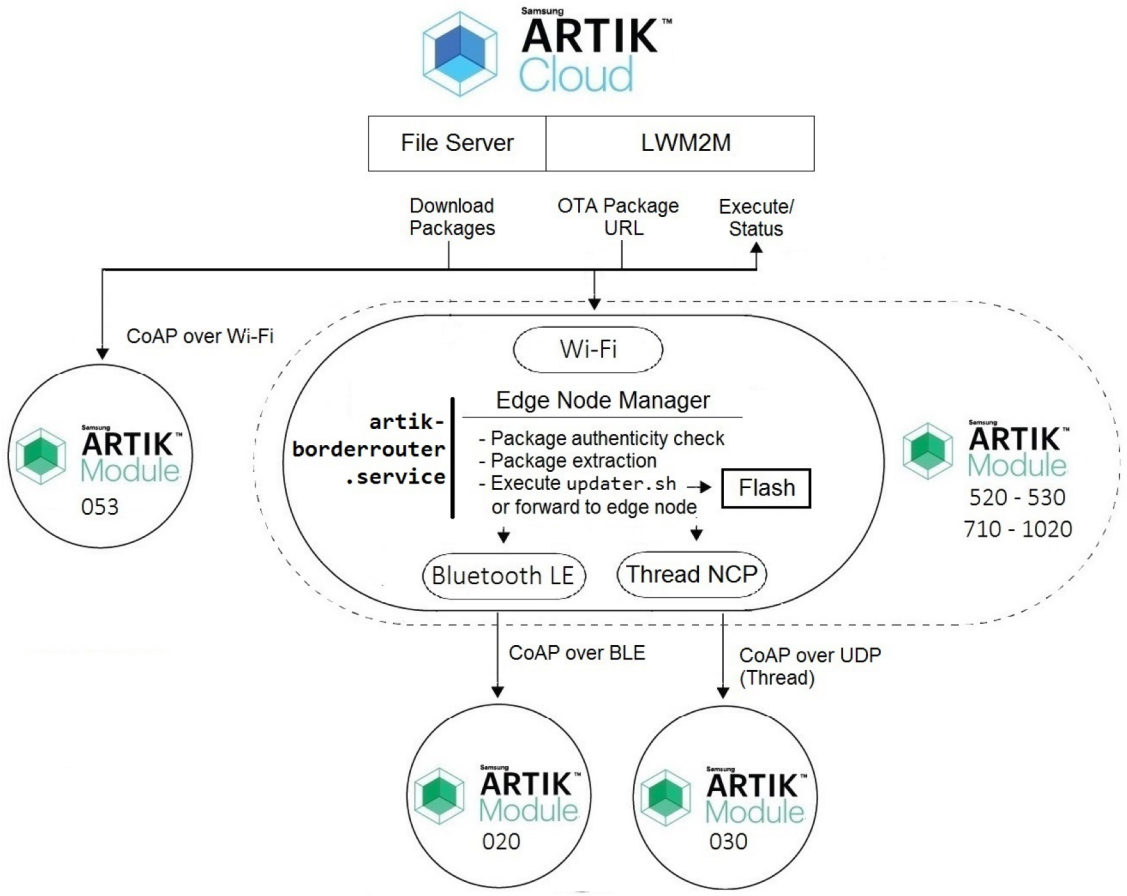
SmartThings Cloud

ARTIK cloud services

- Authentication
- Authorization
- Device whitelisting
- Data encryption

SAMSUNG ARTIK™

Secure OTA



- LWM2M payload delivered over a TLS-secured link
- Protection against DDOS attacks against the image stored. Only registered and authorized device can access
- A unique single-URL for every OTA update
- For 02x, 03x, Edge Node Manager is able to receive firmware updates for the known edge nodes and perform integrity validation

ARTIK Edge Node Manager

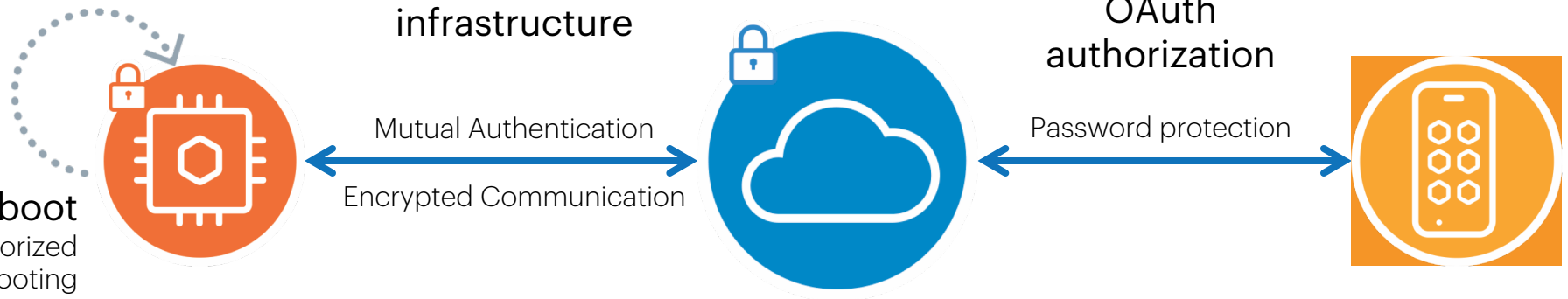
Samsung ARTIK™ End-to-end Platform Security

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™

Praetorian determined that Samsung's ARTIK IoT Platform has adequate security controls in place to defend against prevalent application security vulnerabilities whose existence poses moderate-to-serious risk.

Guided by OWASP Application Security Verification Standard (ASVS)

OWASP Application Security Verification Standard (ASVS)

OWASP ASVS is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to define what a secure application is. Evaluation ratings compare information gathered during the course of the engagement to the OWASP ASVS version 3.1[1] criteria for security standards.

The grade below is a representation of the ARTIK IoT Platform's current, post-remediation security posture. Praetorian calculates grades based on the "Existing Vulnerability Measure" (EVM) formula described in the reference below[2]. EVM is used to quantify the collective risk of the findings identified during this assessment. The letter grade leverages EVM to benchmark risk posture against Praetorian's client-base.

Product	Security	Grade
Samsung ARTIK IoT Platform	Excellent	A

Grade	Security	Criteria Description
A	Excellent	The EVM of the assessed components placed within the top 5-10% of Praetorian's client-base. The overall security posture was found to be excellent with a minimal amount of low and informational risk findings identified.
B	Good	The EVM of the assessed components was above average when benchmarked against Praetorian's client-base. Only a handful of low/informational risk shortcomings were identified in the testing time period.
C	Fair	The EVM of the assessed components was aligned closely to the average EVM of Praetorian's client-base. The current solutions protect some areas of the target from security issues, but moderate changes are required to elevate the discussed areas to acceptable standards.
D	Poor	The EVM of the assessed components fell below the average EVM, with significant security deficiencies present. Immediate attention should be given to the discussed issues to address exposures identified.
F	Inadequate	Serious security deficiencies were present in the assessed components and the EVM placed within the bottom 5-10% of Praetorian's client-base. Shortcomings were identified throughout most of the security controls examined and improved security will require significant resources.

[1] https://github.com/OWASP/ASVS/blob/master/OWASP Application Security Verification Standard 3.1.pdf

[2] https://dl.acm.org/citation.cfm?id=1179505

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

Appendix