SAMSUNG
ARTIK™ Modules

ARTIK Security Guide

TABLE OF CONTENTS

List of Figures

List of Tables

VERSION HISTORY

Revision	Date	Description	Maturity
V1.0	5/16/2017	First release.	Release
V1.1	5/29/2017	Minor updates.	Release update

MODULE SECURITY

The ARTIK platform security, while designed to provide end to end security, leverages strong hardware security capabilities and support through the use a Common Criteria EAL5 Secure Element available on most of ARTIK modules. Among important aspects of this design is the ability to:

- Provisioning of X.509 certificates, and corresponding keys and identities inside the secure storage of the Secure Element of the modules and thereby protecting these sensitive assets over the entire device life cycle and in particular during execution of cryptographic algorithm depending on these keys. The X.509 certificates are issued as part of a PKI trust hierarchy that roots back to an ARTIK Root CA operated based on high level of physical security as well as disaster recovery policies
- Provisioning of X.509 certificates in the cloud servers interacting with ARTIK devices. Server certificates are also issued through a chain rooting back to the same ARTIK Root CA
- Establishing a secure channel (TLS/ DTLS) between devices and cloud solutions, and device to device communication with strong authentication via unique keys and certificates

For basic and fundamental security of IoT pipeline protection, the key and certificate enables secure device registration with ARTIK Cloud, which ensures the device is genuine, and messages exchanged are verified.

ARTIK (S) modules are additionally offering support for secure boot, secure JTAG, and full access to the security library. The security library is based on TrustZone and a Secure Element, and provides secure storage and cryptographic algorithms running in a secure environment without exposure to the user execution environment.

Security threats to IoT devices are diverse and real, starting from compromised consumer privacy, up through theft of services and malicious sabotage of connected devices. These security threats can be mitigated if proper security measures are taken in the design and implementation IoT platforms.

Table 1. Module Security

ARTIK Device	PKI	Secure Onboarding	Secure Element	Security API	Secure Boot	KMS	SEE/TEE	SSS	Secure JTAG	PUF
520	X	X	X	X*						
530	X	X	X	X*						
710	X	X	X	X*						
520S	X	X	X	X	X	X	X		X	
710S	X	X	X	X	X	X	X		X	
053	X	X		X	X	X		X		X

* Reduced Security API support. See *Table 2* for details.

COMMUNICATION SECURITY

One of the most basic security measures is to provide communication security. Communication security is intended to prevent unauthorized access of all communication passing between two entities in the IoT system. It prevents 3rd-party listeners from decoding any of the ongoing traffic, and to eliminate the ability to inject unintended traffic into the connection.

Two most important requirements of communication security are:

- **Encryption** - The process of protecting a payload being communicated between any two entities
- **Authentication** - The process that allows one party to validate the identity of another party

Samsung ARTIK provides a full solution for secure communications between ARTIK Module based devices and Samsung ARTIK Cloud. The Samsung ARTIK solution provides all the necessary software stacks and protocols for providing connectivity security to other IoT products and services.

Encryption

A payload is encrypted on one side of the link and decoded on the other side. The two sides need to share a secret key that is used for the encryption process. A non-authorized listener that does not have the key cannot decode the traffic even if the encryption algorithm used for encrypting the traffic is known. ARTIK provides hardware acceleration (Crypto Engine) for AES and RSA encryption and decryption. ARTIK uses Elliptic Curve Diffie–Hellman (ECDH) for encryption key sharing, which provides high level of protection with low power consumption.

Authentication

Authentication is based on the knowledge of a shared secret between the two parties initiating the link or by using public cryptography based signatures and certificates. ARTIK provides a Public Key Infrastructure (PKI), which is used to generate and apply unique certificates and key pairs on each ARTIK Module during manufacturing.

The PKI standard defines a set of roles, policies, and procedures to create, manage, distribute, use, store and revoke digital certificates, and manage public key encryption. This facilitates the secure electronic transfer of information where simple passwords are an inadequate authentication method, and more rigorous identity proof and information validation is required. ARTIK uses Certificate Authorities to validate different levels of certificates. Figure 1 shows the ARTIK Certificate Authority hierarchy for cloud and device certificates.

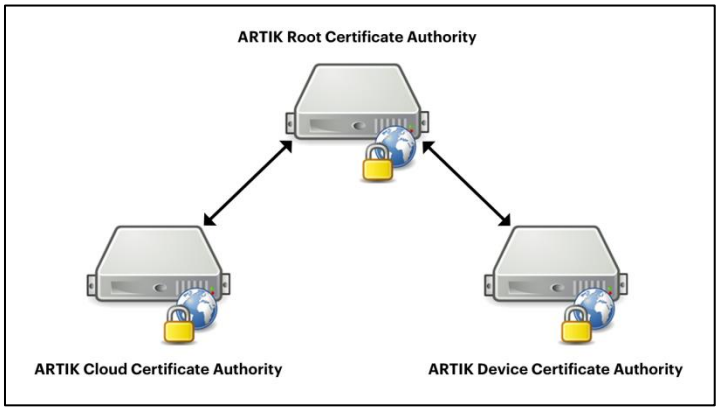

Figure 1. ARTIK Certificate Trust Link

ARTIK Cloud and devices use Transport Layer Security (TLS) and Datagram TLS (DTLS) protocols for a secure communication channels. Over TLS/DTLS, ARTIK Cloud authenticates ARTIK devices using a certificate/key-pair stored on each ARTIK device. The certificate/key-pair is stored in a highly-secure storage, the Secure Element. The certificate/key-pair cannot be altered or tampered with once they have been flashed onto the ARTIK device.

Figure 2 illustrates the process flow of how the certificate/key-pair are created and placed onto ARTIK devices.

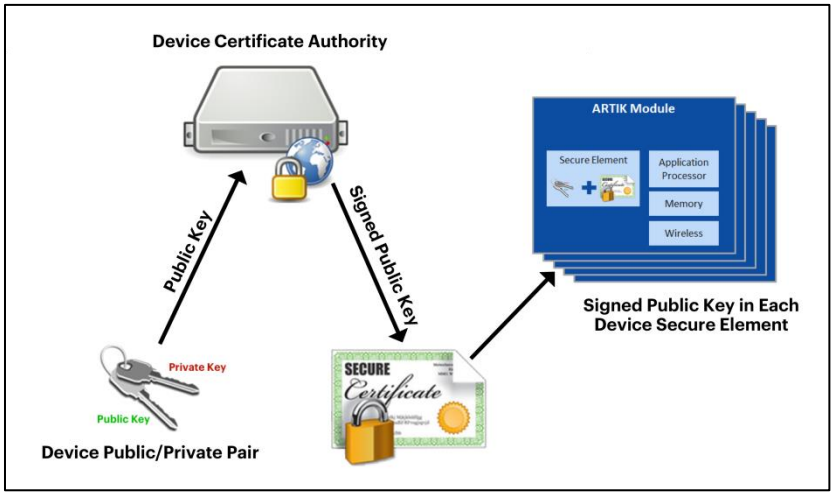

Figure 2. ARTIK Device Key-pair and Certificate Issuance

Also, as part of the authentication process, matching session keys are created to establish a secure session for data transfer between the ARTIK device and ARTIK Cloud, which are then used to encrypt/decrypt the traffic using AES encryption. One may also store an HMAC key and asymmetric key pair into secure storage. This may be used to setup a secure connection with a third party cloud service. For additional information regarding post provisioning, please refer to the ARTIK Security API Guide.

DEVICE SECURITY

Secure Boot

To trust the software running on a hardware platform is one of the most fundamental principles of security. Many attacks on connected devices and systems are based on the attacker's ability to replace or modify the software running on the attacked platform. Thus, it is important to ensure that the software running on a device is from the legitimate and intended source. To ensure authenticity, software needs to be signed by the software provider who owns it, and has verified the software's execution on the target device. This verification starts when the system is brought up from a cold boot. A secure boot process consists of several stages, called bootloader stages, where software is verified and installed at each stage.

A Secure Boot scheme adds cryptographic checks to each stage of the boot process. This process aims to prevent any unauthorized software from running by assuring the integrity of all boot images when each boot loader is called by the previous one. This process eliminates the possibility of unintended images being used on the platform by simple replacement or modification of the code image stored in module flash by either direct access or remote software upgrade. *Figure 3* illustrates one possible secure boot sequence.

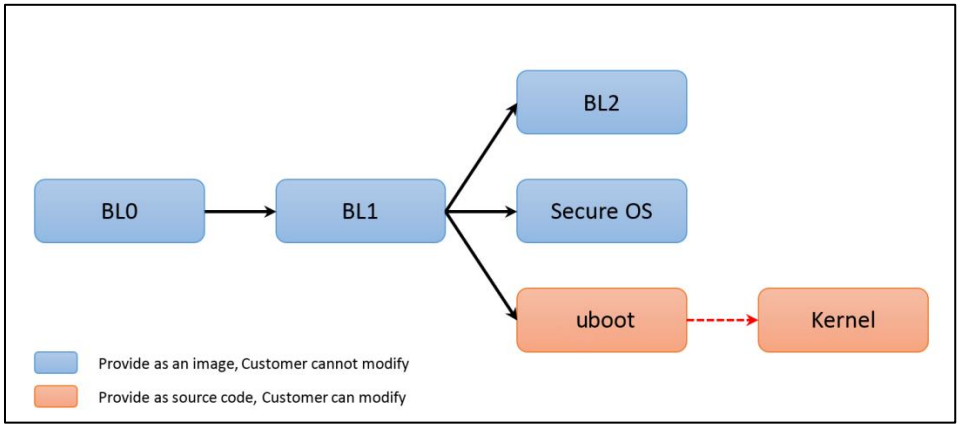

Figure 3. Cryptographic Check Sequence Overview

The Samsung ARTIK platform provides a Secure Boot functionality to mitigate threats to the booting process. To ensure resilience against mass-compromises, an asymmetric key signature algorithm is used for signing and verification. Images are signed through a highly secure code signing system, referred to as Key Management System (KMS), where signing keys are stored and operated within Federal Information Processing Standards (FIPS) 140-2 certified Hardware Security Modules (HSM) based on strict access control policies. Samsung provides access to signing services to its customers for performing the signing at their own convenience, while relying on the operational and physical security provided by Samsung. See the KMS section for further details.

KMS

A Secure Boot solution is only effective if the private key is secure and safe. This requires the use of specific business practices to securely store and control access to the private key. In order to provide a secure and easy to use signing process, Samsung ARTIK provides a Key Management Server (ARTIK CodeSigner service). KMS is used to sign packages using highly secure cryptography standards (SHA256wRSA2048). At the same time, signing keys are protected using highly secure signing servers equipped with FIPS certified HSMs with proper administrator controls. ARTIK offers the use of its highly secure signing infrastructure for customers and partners via ARTIK CodeSigner Portal for the task of secure key management and code signing. The ARTIK CodeSigner Portal system is hosted by Samsung and allows for remote secured connection via internet. *Figure 4* illustrates the package signing process.

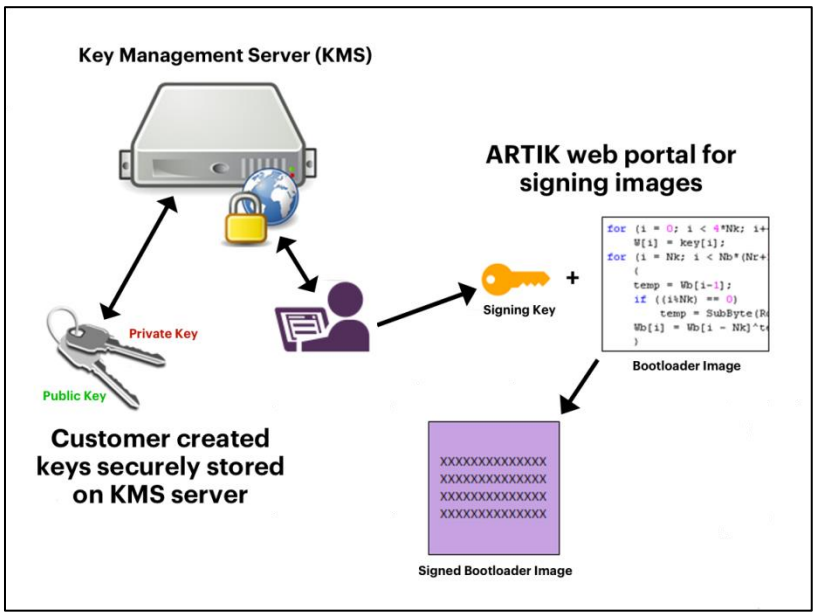

Figure 4. Key Management Server (KMS)

Using the Samsung ARTIK KMS solution, one can generate signing keys and share the public key with Samsung. The public key gets added to the first bootloader and the private key is used to sign the other secondary bootloader binaries. This way verification of secondary bootloader is based on the key pair that is unique to the customer, allowing them to fully own and protect their firmware.

Samsung implements the required practices and infrastructure to support this process so the user doesn't have to. The Samsung ARTIK KMS service has been customized to operate with the ARTIK development flow to provide a streamlined, seamless experience that enables customers to concentrate on their code development and not on the custom implementation of security services. ARTIK provides chain of trust starting from Boot-Loader-0 (ROM) until u-boot (bootloader). One can enable the "verified boot" feature provided in the ARTIK Board Support Package (BSP) to enable verification of the binaries for kernel and subsequent stages.

Figure 5. Samsung CodeSigner service web interface

To gaining access to the Samsung ARTIK KMS server, send to request to Samsung ARTIK Sales team. After obtaining the account information from the Samsung ARTIK Team, portal users are allowed to login to the portal and perform tasks related to code signing. Such tasks available are:

- Requesting a new key
- Uploading a code image
- Signing the code image
- Downloading the signed code image

For more details, please refer to the ARTIK CoderSigner Portal Guide.

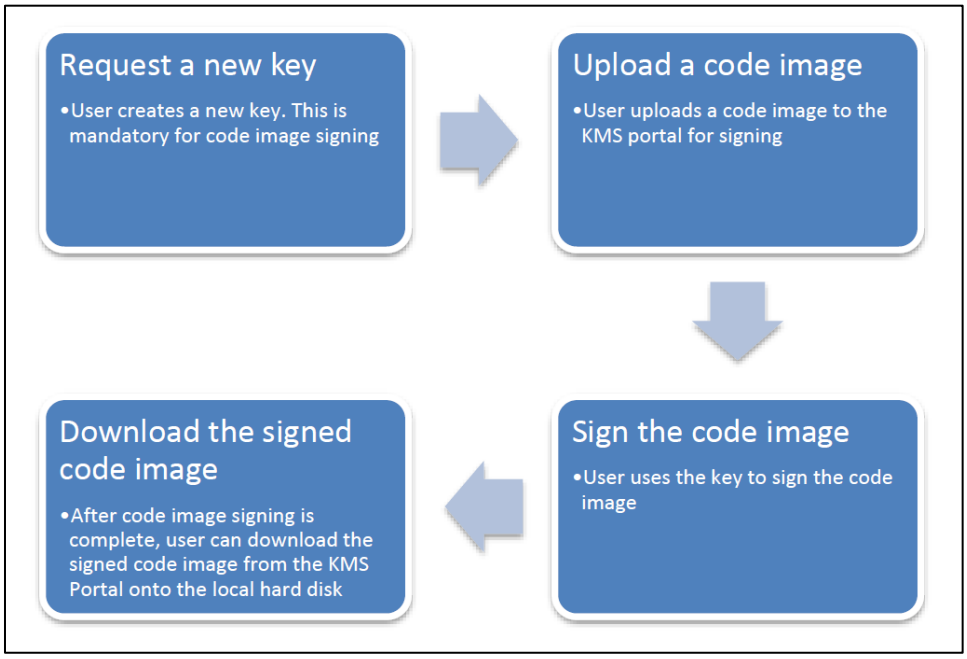

Figure 6. Code Signing Flow Overview

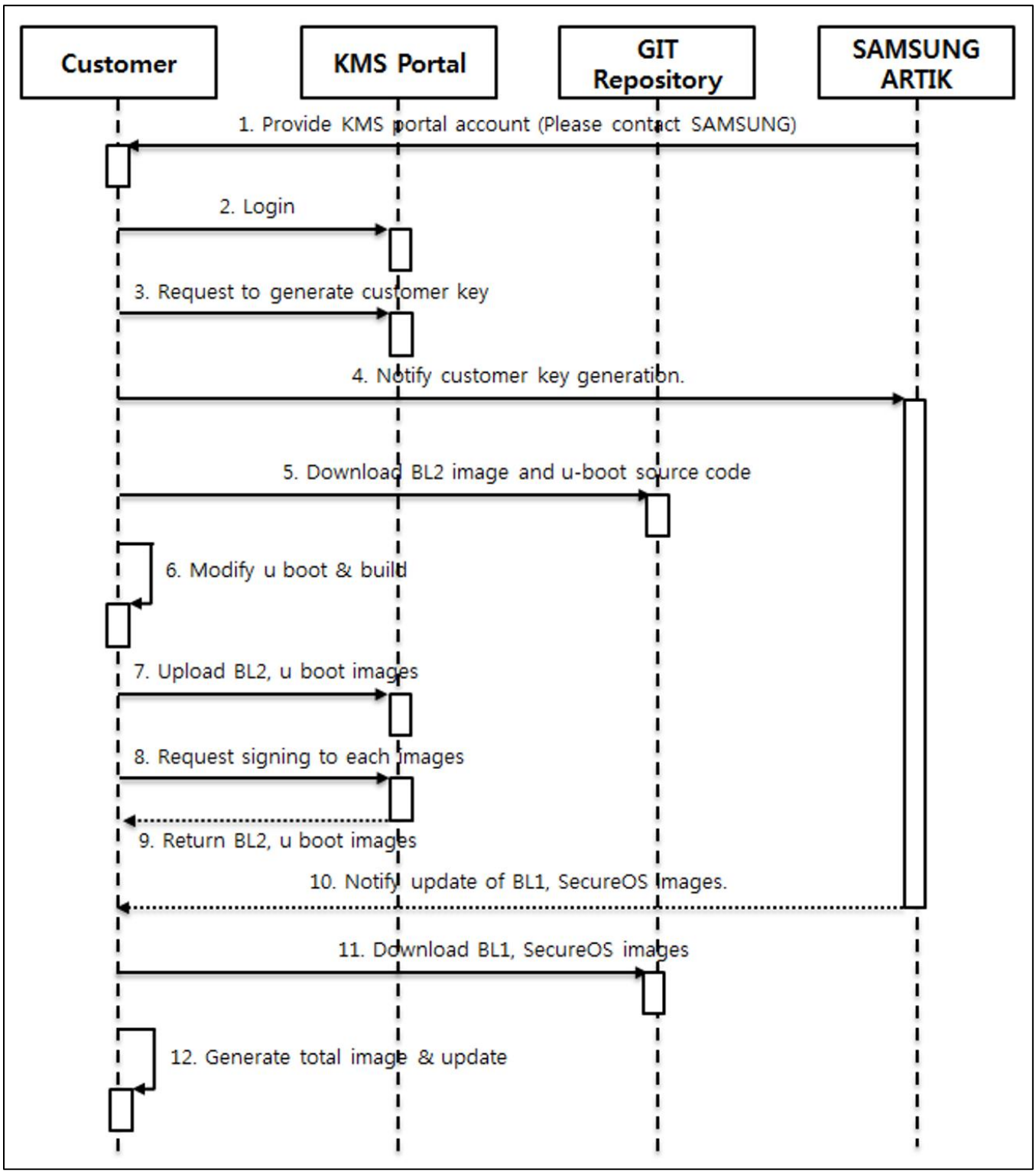

Figure 7. Code Signing Flow Details

Secure JTAG

The Samsung ARTIK devices provide JTAG for debugging of the platform. However, JTAG is a known vulnerability since access via JTAG opens up methods to bypass internally defined security mechanisms. Samsung ARTIK (S) devices support Secure JTAG to protect the device from unauthorized access.

Secure JTAG requires the use of a password, specific to a particular manufacturing lot of modules, to gain access the JTAG chain. The password is based on the serial number of module, which is provided on special request to Samsung ARTIK. Contact Samsung ARTIK Sales for more details.

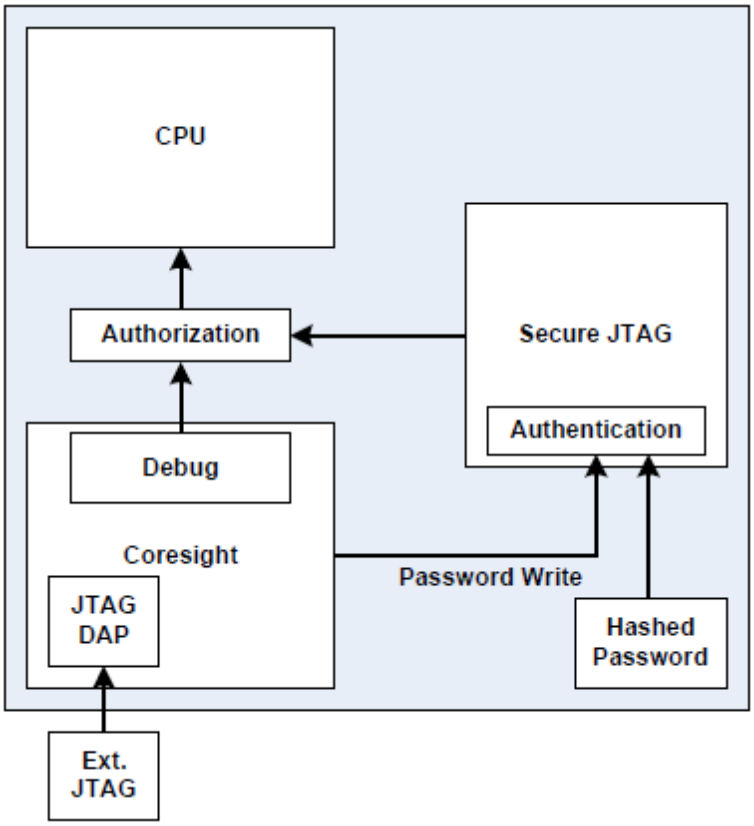

Figure 8. Secure JTAG Block Diagram

DATA SECURITY

Trusted Execution Environment

The Samsung ARTIK 5 and 7 family modules support the Trusted Execution Environment (TEE). TEE provides a fully-isolated and secured operation environment to applications requiring a high degree of security, as well as the full capabilities and power of the application processor environment.

TrustZone®

The Samsung TEE implementation is based on the ARM® TrustZone® hardware architecture. TrustZone allows for the complete separation of the Trusted Execution thread from the regular operation. Using a well-proven and widely-deployed architecture implemented in hardware provides for improved security assurance. In comparison, implementations that use just software-based virtualization techniques for TEE implementation can be circumvented. *Figure 9* shows this comparison.

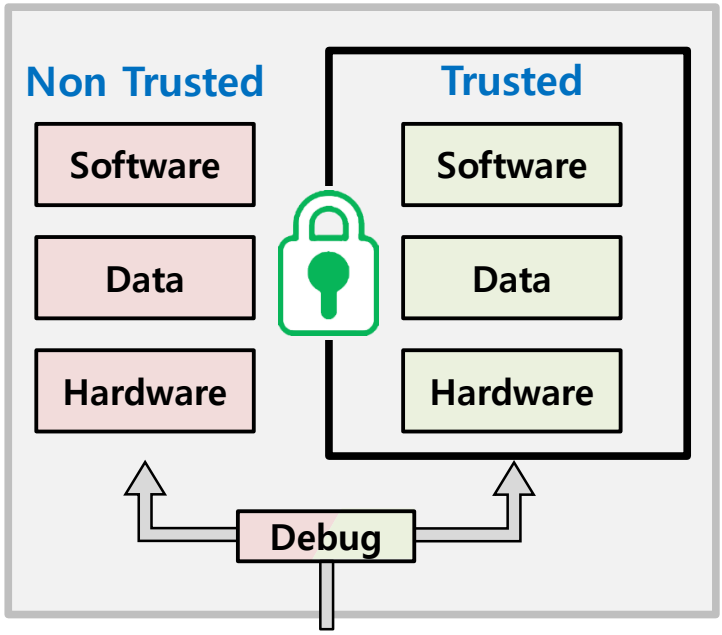

Figure 9. ARM® TrustZone® Separation Concept

The TrustZone hardware enables the isolation of system resources such as specific memory sections and specific peripherals so they are only accessible to the CPU's trusted operation thread. A TrustZone CPU enables the operation of two completely-separate threads, one which is secure and has full privileges to access all system resources, and another that is used for general applications and is restricted from accessing the specific resources designated for secure operation.

Inclusion of the basic TrustZone hardware support is a requirement for the implementation of a proper TEE environment. However, operating systems and applications that utilize this hardware capability and are coded with the proper methodologies to guarantee their security are not commonly deployed. In fact, many systems that are based on platforms that include mechanisms such as TrustZone have not implemented true TEE functionality due to the complexity and required expertise.

Secure Processing

The Samsung ARTIK platform offers all of the required software support for a hardware-based TEE implementation pre-integrated into its firmware support. The TEE software included in the ARTIK solution includes two separate offerings to meet varied customer needs.

Samsung SEE: Samsung Secure Execution Environment (SEE) provides a full TEE implementation of a Secure-OS which provides a set of APIs for access and communication from a non-secure operating system. The SEE environment supports the implementation of basic security APIs for key generation and storage, certificate handling, and provides secured access to the secure storage and its services described later in the document. The SEE environment includes all the key and certification security services required for the implementation of full access to ARTIK Cloud.

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

Trustonic TEE: The Samsung ARTIK TEE solution is provided by Trustonic. It offers pre-integration of the Trustonic TEE environment (named Kinibi). Users who require developing custom TEE applications or require operating multiple, isolated TEE applications may leverage the pre-integration reference of the Trustonic TEE environment. Target applications for the Trustonic TEE environment include home insurance and monitoring services, medical insurance and services, and utility-management service providers, among others. These applications require strict isolation from each other, strong authentication and identify verification, as well as controlled access to resources.

Secure Storage

A Secure Storage feature allows the Samsung ARTIK module to securely store data. Secure Storage uses two storage types, the eMMC file system (flash based), and the Secure Element.

The eMMC file system 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 runtime and is stored as a file unit of 32KB with a maximum number of files that may be stored is 1024.

NOTE: *A consequence of this key storage solution is if the eMMC flash space is formatted or cleared, the data in the secure storage partition will also be deleted.*

The Secure Element is an isolated storage device that supports the storage of up to 16 AES 128 bits keys. The Secure Element provides high levels of security as hardware with anti-temper measures. Also, a secured software environment is provided which allows for the highest level of security offered on consumer devices. All communication from the Secure Element to the processor is secured and encrypted. Customers can access and use the secure storage via the APIs provided by the ARTIK security library, and each storage type can be selected via API argument.

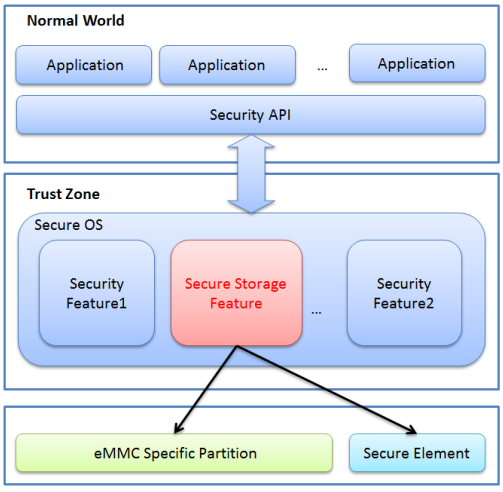

Figure 10. TEE Functionality Overview

ARTIK Security Library

The Samsung ARTIK solution includes a Security Library which consists of APIs to communicate with the Samsung SEE from the non-secure OS (Linux). The Security Library offers specific functions related to key management, authentication, secure storage, and post provisioning.

The following table lists the descriptions of the APIs available as part of the Samsung ARTIK Security Library. For Samsung ARTIK (S) modules, access to all the APIs of ARTIK Security Library is available. For non-(S) modules, only three APIs are available for use in authentication. The three supported Security Library API that is supported on all ARTIK modules are highlighted in bold.

Table 2. Security Library API Support

Category	ARTIK API	Description
Initialize	see_init	For Initializing a new SEE session.
	see_deinit	
Key Manager	see_generate_key	For management of symmetric and asymmetric keys that are not exposed to non-secure operating system user space.
	see_set_key	
	see_get_pubkey	
	see_remove_key	
Authentication	**see_generate_random**	For use with the TLS library with callback functions to generate a digital true random number, generate or get certificates, get signatures and verify, and to generate or compute DHM parameters.
	see_generate_certificate	
	see_set_certificate	
	see_get_certificate	
	see_remove_certificate	
	see_get_rsa_signature	
	see_verify_rsa_signature	
	see_get_ecdsa_signature	
	see_verifiy_ecdsa_signature	
	see_get_hash	
	see_get_hmac	
Secure Storage	see_write_secure_storage	For access to the secure storage for data, credentials, and keys.
	see_read_secure_storage	
	see_list_secure_storage	
	see_delete_secure_storage	
Post Provision	see_post_provision	For inject a HMAC key or asymmetric key pair (ECC/RSA) into the secure element.
	see_post_provision_lock	
Encryption/Decryption	see_rsa_decryption	For Data encryption and decryption using a key in secure storage.
	see_rsa_encryption	
	see_aes_decryption	
	see_aes_encryption	

ARTIK 053 Security Subsystem

A Security Sub System (SSS) provides secure code execution, secure storage, an isolated security processor, cryptographic hardware acceleration, and a Physically Uncloneable Function (PUF). In addition, the Security Subsystem contains unique keys and certificates created during the ARTIK 053 module manufacturing process. An ARTIK 053 module uses these unique keys and certificates and ARTIK PKI to authenticate with the Samsung ARTIK Cloud. Refer to *Table 2* for module support.

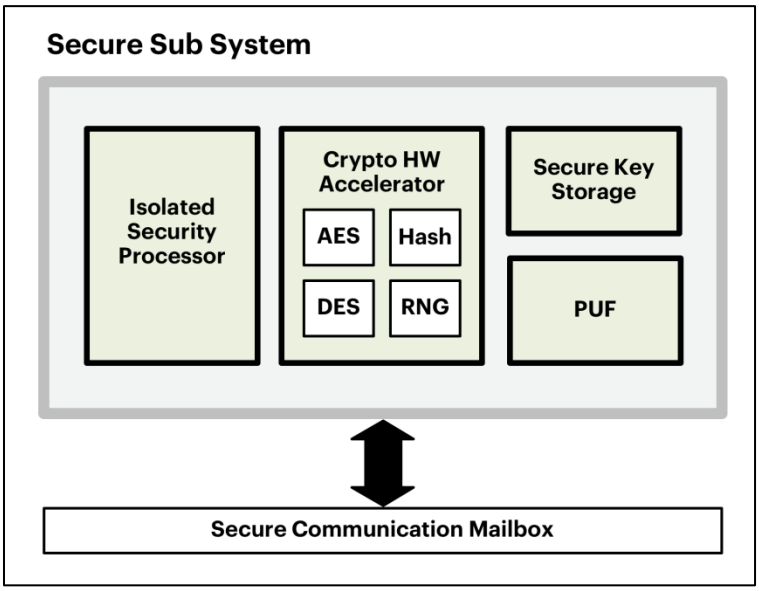

Figure 11. Security Subsystem Block Overview

Isolated Security Processor: A physically isolated security processor with its own dedicated memory and firmware, in a protected execution environment. It is connected to a secure communication bridge between the Secure Subsystem and user execution environment.

Cryptographic Hardware Acceleration: Dedicated cryptographic acceleration hardware which provides support for random number generation, block cipher (AES/DES), Hash functions (SHA[1/2/3] with HMAC), and public key cryptosystem (RSA, ECDSA, DH, ECDH)

Physically Uncloneable Function: Each ARTIK 053 comes with a unique Physically Uncloneable Function (PUF) key generator that is created during device manufacturing. A PUF uses a well-known frequency ring oscillator design that changes for each device by virtue of the manufacturing process itself. This means that each device gets a unique key generator in hardware that is untamperable and uncloneable, and unique to that device. The PUF is therefore used to uniquely fingerprint a device over the device's entire lifetime.

ARTIK (S) Module Secure Element

ARTIK (S) modules include a hardware-based Secure Element. Refer to *Table 2* for module support. The Secure Element provides full services for the secure storage of cryptographic material and other protected content. It includes cryptographic services for cryptographic random-number generation, key/data secure storage, and certificates handling and processing. The Secure Element meets the Common Criteria (CC) certification for computer security and for Evaluation Assurance Level (EAL) 5/6+.

The Secure Element fully integrates with the ARTIK platform and with the Samsung ARTIK Cloud. This relieves the developer from the complex tasks of managing with private/public key-pair generation, certificate issuing and managing, plus provisioning across their production and supply chain. The Secure Element comes pre-loaded with an individual device certificate and private/public key pairs which has been pre-registered with ARTIK Cloud. It uses the following key technologies to achieve highest level of security and protection:

- **Smart Shield:** Custom random layout including memory encryption
- **Smart Sensor:** Digital fault detection including protection against fault-injection attacks
- **Smart Core:** High speed secure cryptography engines with a secure low power CPU

PLATFORM SECURITY

ARTIK is a secure IoT solution, and provides security across the entire IoT pipeline. The ARTIK Platform Software solution includes many applications and features to extend the module security offering for your own application. The software suite offers an onboarding service using secure device registration, edge node device management from the gateway, over the air update protocol, and an easy to use API library.

SECURE DEVICE REGISTRATION

ARTIK Cloud Secure Device Registration (SDR) relies on strong mutual authentication between a gateway device and the cloud registration servers. Furthermore, the device registration involves a binding of user and device authentications, while allowing the ease of use experience by use of convenient mobile applications assisting the process. The device authentication is based on use of SHA256_ECDSA X.509 certificates for both devices and servers as part of a mutual TLS handshake.

To ensure the integrity of the certificate based TLS authentication, ARTIK devices and servers are provisioned with certificates from a Public Key Infrastructure (PKI) as a root of trust for the ARTIK ecosystem. Furthermore, ARTIK devices are equipped with secure storage for the purpose of storing factory-provisioned keys and assisting the TLS authentication as a session key generation, using secure APIs.

BLE Onboarding Service

ARTIK BLE Onboarding service is reliant on the ARTIK Cloud Secure Device Registration (SDR) for communication from ARTIK Cloud to the device.

EDGE NODE MANAGER

The economics, security, reliability and environmental requirements for many IoT edge node devices dictate their connectivity to be restricted to a local network. A small, inexpensive, battery driven device may not have the memory, processing and hardware/ software capabilities for connecting to public Internet using a TCP/ IP stack. The ARTIK Platform Software solution provides the End Node Manager (ENM) to securely connect the resource constraint edge node devices to ARTIK Cloud. The ENM was designed using technologies to improve future compatibility with other systems. The ENM offers the ability to perform discovery of all edge node devices within its local network, and is capable of using wireless stacks supported by a variety of technologies.

The registration of the edge node devices is performed by the ENM after the edge node discovery process. Then ENM is able to receive firmware updates for the known edge nodes and perform integrity validation before forwarding to the edge node device.

OTA

Over their lifetime, IoT devices may require software updates to support new functionality, standards, security, or environments. At the same time, given the number of players in IoT ecosystem, it is important to ensure that the software update has originated from a legitimate source. And an update must be delivered and installed to the intended device in a tamper-free manner.

Samsung ARTIK Cloud offers a secure Over The Air (OTA) infrastructure for delivery of the software updates to all registered ARTIK devices. The ARTIK OTA solution follows the Light Weight Mobile To Mobile (LWM2M) payload format as its delivery mechanism. In addition to TLS link protection, the ARTIK OTA solution is designed specifically to be resistant against redirect attacks. This may be where an attacker might send an unsuspecting device to a malicious software store that in turn could direct the device to download a malicious or unauthorized update or cause the device to cease functioning.

In addition, the OTA infrastructure is designed to protect against DDOS attacks against the image store by ensuring that only registered and authorized devices will be able to download a new image. Finally, ARTIK Cloud generates and provides a unique onetime usable URL for each device to download the update. This unique URL is provided for every OTA update. With these capabilities, ARTIK Cloud provides the maximum flexibility in an update mechanism while providing the ability to customize the update process to include additional security measures for different types of application requirements.

ARTIK SDK

Security Library Integration

The Samsung ARTIK SDK is a set of development libraries for use on the ARTIK platform. The ARTIK SDK provides a simple, easy to use, and portable software framework for use across the ARTIK device portfolio. Included in the ARTIK SDK is a simple and easy to use integration with the Samsung ARTIK SEE security libraries.

SSL Parameters for Connectivity

The ARTIK SDK provides many ease of use solutions for communications between clients and server applications. In the ARTIK SDK connectivity, HTTP requests, MQTT messaging, and WebSockets are available to create secure connections. Included is a SSL configuration structure to easily customize TLS handshake parameters for secure connections. This gives flexibility for easily generating a secure communication channel for an application.

OpenSSL Library

For applications that are already using or planned to use the OpenSSL software library, one can still take advantage of the ARTIK Security features. The ARTIK security library is integrated with the OpenSSL engine.

The OpenSSL engine takes advantage of the hardware accelerated ARTIK security library to get keys from the secure element, encrypt and decrypt, encode and decode, sign and verify, get a hash digest. The ARTIK security library supports the following OpenSSL ciphers:

Table 3. ARTIK OpenSSL Cipher Support

Supported ARTIK Security OpenSSL Ciphers		
aes-128-cbc	aes-128-ecb	aes-128-ctr
aes-192-cbc	aes-192-ecb	aes-192-ctr
aes-256-cbc	aes-256-ecb	aes-256-ctr

LEGAL INFORMATION

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH THE SAMSUNG ARTIK™ DEVELOPMENT ENVIRONMENT AND ALL RELATED PRODUCTS, UPDATES, AND DOCUMENTATION (HEREINAFTER "SAMSUNG PRODUCTS"). NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. THE LICENSE AND OTHER TERMS AND CONDITIONS RELATED TO YOUR USE OF THE SAMSUNG PRODUCTS ARE GOVERNED EXCLUSIVELY BY THE SAMSUNG ARTIK™ DEVELOPER LICENSE AGREEMENT THAT YOU AGREED TO WHEN YOU REGISTERED AS A DEVELOPER TO RECEIVE THE SAMSUNG PRODUCTS. EXCEPT AS PROVIDED IN THE SAMSUNG ARTIK™ DEVELOPER LICENSE AGREEMENT, SAMSUNG ELECTRONICS CO., LTD. AND ITS AFFILIATES (COLLECTIVELY, "SAMSUNG") ASSUMES NO LIABILITY WHATSOEVER, INCLUDING WITHOUT LIMITATION CONSEQUENTIAL OR INCIDENTAL DAMAGES, AND SAMSUNG DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, ARISING OUT OF OR RELATED TO YOUR SALE, APPLICATION AND/OR USE OF SAMSUNG PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATED TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT.

SAMSUNG RESERVES THE RIGHT TO CHANGE PRODUCTS, INFORMATION, DOCUMENTATION AND SPECIFICATIONS WITHOUT NOTICE. THIS INCLUDES MAKING CHANGES TO THIS DOCUMENTATION AT ANY TIME WITHOUT PRIOR NOTICE. THIS DOCUMENTATION IS PROVIDED FOR REFERENCE PURPOSES ONLY, AND ALL INFORMATION DISCUSSED HEREIN IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND. SAMSUNG ASSUMES NO RESPONSIBILITY FOR POSSIBLE ERRORS OR OMISSIONS, OR FOR ANY CONSEQUENCES FROM THE USE OF THE DOCUMENTATION CONTAINED HEREIN.

Samsung Products are not intended for use in medical, life support, critical care, safety equipment, or similar applications where product failure could result in loss of life or personal or physical harm, or any military or defense application, or any governmental procurement to which special terms or provisions may apply.

This document and all information discussed herein remain the sole and exclusive property of Samsung. All brand names, trademarks and registered trademarks belong to their respective owners. For updates or additional information about Samsung ARTIK™, contact the Samsung ARTIK™ team via the Samsung ARTIK™ website at www.artik.io.