Implement End-to-End Security with the Arrow Security Starter Kits

Connected devices are employed in a range of applications — from point-of-sale (POS) terminals and medical equipment to critical infrastructure and process control systems. Always-on connectivity leaves systems and devices vulnerable to security breaches and malware attacks, endangering sensitive business information, intellectual property, and business continuity. The security of connected devices is a growing concern and is now a top priority at every stage of the product design. Security has many aspects and breaches can occur along any single point of weakness. A comprehensive approach to device and system security is paramount and requires a thorough understanding of the relevant IoT security standards, security features required to mitigate risks, and implementation details.

Arrow has worked closely with several technology suppliers to create a set of solutions that employ ten major security features and take the guesswork out of implementation and reduce your overall time to market. Using an open-source software framework, the Arrow Security Starter Kits integrate readily available wireless evaluation kits and Arrow's 96Boards compliant single-board computers (SBCs) with Infineon's OPTIGA™ TPM 2.0 & OPTIGA™ Trust M security solutions and AWS cloud services. Using these kits, device makers can easily add security to their end products while adhering to the latest security standards, including ETSI TS 103 645, NISTIR 8259A, and ISO 27001.

Arrow Security Starter Kit Platforms Include Four Kits

- Two gateway/edge compute kits with the Infineon OPTIGA™ TPM 2.0 and
  - Arrow 96Boards SBC with the STM32MP157 MPU
  - Arrow 96Boards SBC with the i.MX 8X application processor
- Two wireless end node kits with the Infineon OPTIGA™ Trust M and
  - Silicon Labs Giant Gecko 11 and XBee3 module for LTE-M solution
  - ST Micro STM32WB55 for BLE and Bluetooth® 5 solutions

Security Features Supported by the Arrow Security Starter Kits

Unique Device Identity

Secure Boot

Secure OTA Updates

Secure Data (Encryption)

Device Authentication

Device Management (Allow/Deny)

X.509 Certificate Support

Isolation of Secure Firmware from Non-Secure Applications

Isolation of Credentials in a Tamper-resistant Element

Secure Supply Chain Support

The Arrow Security Starter Kit Portfolio

The Arrow Security Starter Kit portfolio has variants that support two wireless end node configurations and two gateway/edge compute solutions. These kits incorporate the Infineon OPTIGA™ TPM 2.0 and OPTIGA™ Trust M technologies and function independently or in combination to provide a secure end-to-end solution. Created with FreeRTOS or Linux, the portfolio supports AWS IoT Greengrass, and/or AWS IoT Core right out-of-the-box.

Gateways/Edge Compute Solution with Infineon OPTIGA™ Trusted Platform Module (TPM) 2.0

These kits use OPTIGA™ TPM 2.0 with AWS services to develop a gateway or edge compute solution enabled with a hardware layer security. They include a Tresor Mezzanine board with the OPTIGA™ TPM 2.0, and the Arrow 96Boards SBCs based on ST Micro STM32MP1 or NXP i.MX 8X processors.

Tresor Mezzanine OPTIGA™ TPM 2.0

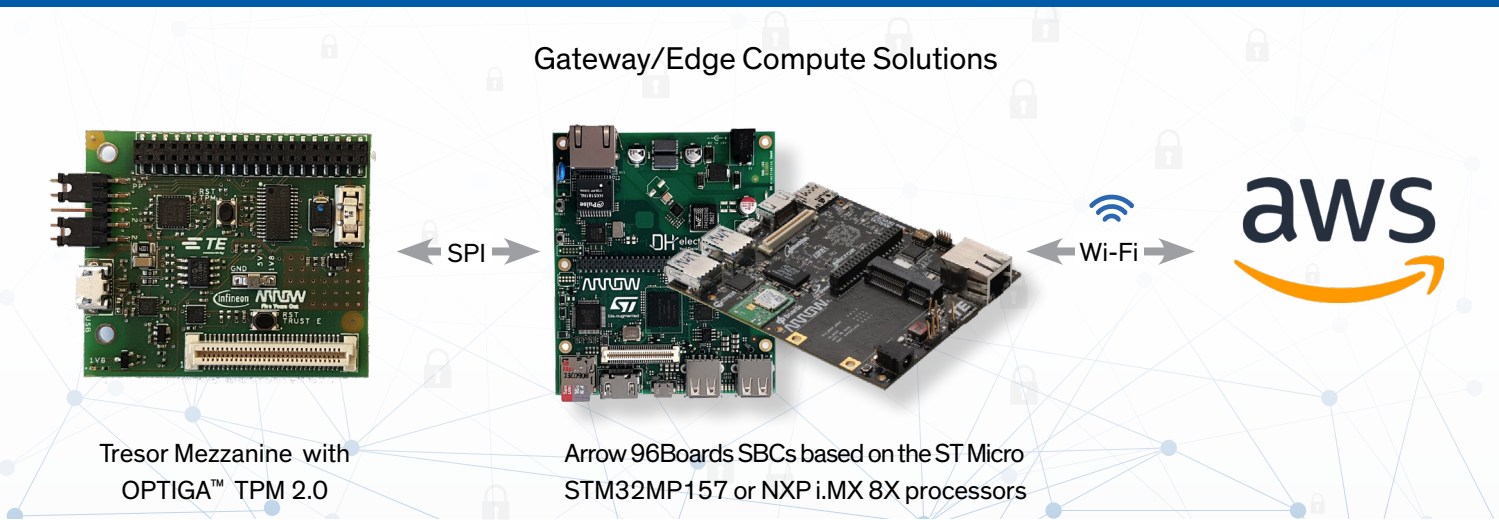
The Tresor Mezzanine Board adds advanced security features to the 96Boards SBCs. It includes the OPTIGA™ SLB9670× TPM 2.0 that supports the following features:

- Compliant to TPM Main Specification, Family "2.0"
- Hardware and firmware are validated according to FIPS 140-2 Level 2
- Random Number Generator (RNG) according to NIST SP800-90A
- Full personalization with Endorsement Key (EK) and EK certificate
- 24 PCRs (SHA-1 or SHA-256)
- SPI interface

Tresor Mezzanine with OPTIGA™ TPM 2.0

Out-of-the-Box Demonstration with Infineon OPTIGA™ TPM 2.0

The demo runs on the Linux Yocto platform with the OPTIGA™ TPM 2.0. It showcases the implementation of the ten security features and the functionality of AWS IoT Greengrass, AWS IoT Core, AWS Provisioning, AWS Authentication, and secure communication features.

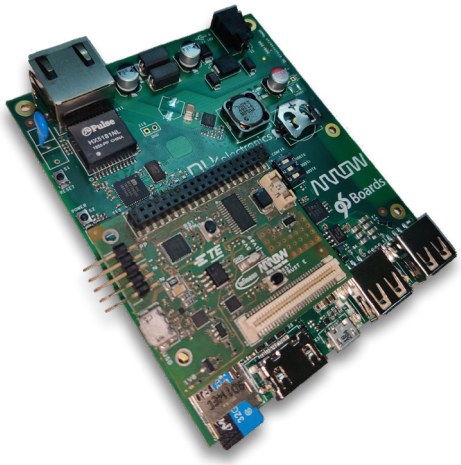


Tresor Mezzanine with OPTIGA™ TPM 2.0

Arrow 96Boards SBCs based on the ST Micro STM32MP157 or NXP i.MX 8X processors

Security Starter Kit with ST STM32MP1 and Infineon OPTIGA™ TPM 2.0

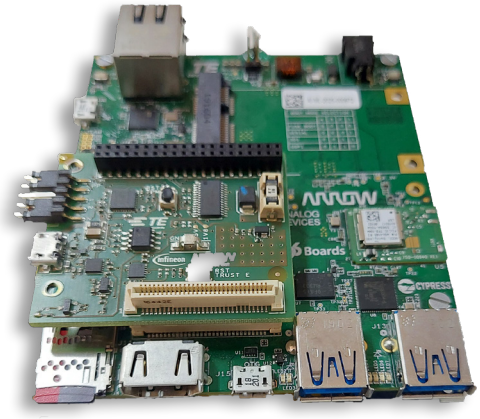
STM32MP1 microprocessor includes dual Arm® Cortex® A7 and Cortex® M4 cores and supports the Arm TrustZone® peripherals and active tamper security features.



Part Number: STM32MP157-SSK

Security Starter Kit with NXP i.MX 8X and Infineon OPTIGA™ TPM 2.0

The NXP i.MX 8X processor has a quad-core 64-bit Arm® Cortex® A35, dedicated GPU, and VPU. Advanced security features supported by the application processor include AHAB secure and encrypted boot, random number generator, and RSA up to 4096.



Part Number: i.MX_8X-SSK

Security Features Incorporated in the Gateway/Edge Compute Kits

Security Feature Implemented	Description
Unique device identity	EUI64 is used for unique device identifier. Stored in the OPTIGA™ TPM 2.0
Secure boot	Software based secure boot feature performed in OPTIGA™ TPM 2.0
Secure OTA updates	Implemented software-based capability for OTA updates implemented in OPTIGA™ TPM 2.0
Secure data (encryption)	Data encrypted and decrypted using the OPTIGA™ TPM 2.0
Device authentication	Device authentication feature enabled in the OPTIGA™ TPM2.0
Device management (allow/deny)	Performed in the AWS cloud
X.509 certificate support	A digital certificate to verify that a public key belongs to the hostname/domain, organization, or individual contained within the certificate.
Isolation of secure firmware from non-secure application	Stored in OPTIGA™ TPM 2.0
Isolation of credentials (keys) in a tamper-resistant element	Stored in OPTIGA™ TPM 2.0
Secure supply chain	Register RootCA in AWS and using RootCA creating the device certificate. Intermediate CA not used. Private key and device certificate are stored in the OPTIGA™ TPM 2.0

Wireless End Node Security Kits with OPTIGA™ Trust M

These boards support Bluetooth® LE and LTE-M connectivity. Trust M S2GO, which includes the OPTIGA™ Trust M, connects to the ST STM32WB55 EVK or the Silicon Labs Giant Gecko board. Arrow provides Android & iOS based mobile applications, which function as the BLE to WiFi conversion for AWS cloud services connectivity.

Trust M S2GO Board

Shield2Go (S2GO Board) for OPTIGA™ Trust M offers a unique evaluation experience for developers building security solutions — the board has one OPTIGA™ Trust M security chip on an easy to handle PCB. It provides a root of trust in the form of a unique X.509 certificate coupled with hardware support to establish a TLS (Transport Layer Security) connection between devices and cloud, forming a robust basis for secured communication. All these features enable the rapid evaluation and development of secure IoT systems.

Features

- CC EAL6+ (high) certified high-end security controller — ECC NIST P-256/P-384, RSA® 1024/2048, SHA-256, TRNG/DRNG
- I2C interface with shielded connection
- Hibernate mode for zero power consumption

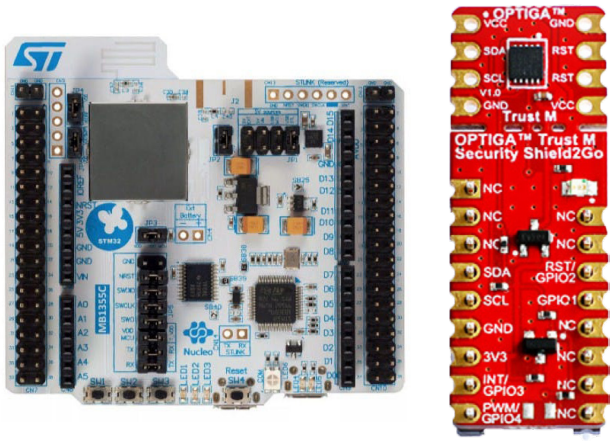
Trust M S2GO Board

Out-of-the-Box Demonstration with Infineon OPTIGA™ Trust M for Wireless End Nodes

The demo integrates FreeRTOS in a BLE or LTE-M configuration with the OPTIGA™ Trust M on the ST Micro STM32WB55 EVK or the Silicon Labs Giant Gecko 11 and XBee3 boards. AWS IoT Core also enabled and securely communicates with the Cloud.

Security Starter Kit with ST Micro STM32WB55 and OPTIGA™ Trust M

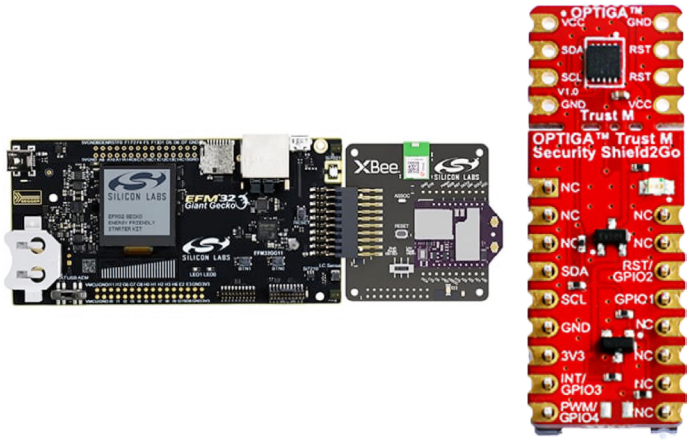
This combination includes a Trust M S2GO board and the ST Micro P-Nucleo-WB55 EVK. It supports BLE and Bluetooth® 5 connectivity. iOS and Android mobile apps are provided.



Part Number: STM32WB55-SSK

Security Starter Kit with Giant Gecko 11, XBee3 Module and OPTIGA™ Trust M

This combination includes a Trust M S2GO board, Silicon Labs Giant Gecko 11 board, and XBee3 module for LTE-M connectivity.



Part Number: GG11-LTE-M-SSK

Security Features Incorporated in the Wireless End Node Kits

Security Feature Implemented	Description
Unique device identity	EUI64 is used for unique device identifier. Stored in the OPTIGA™ Trust M
Secure boot	Secure boot is performed in the bootloader
Secure OTA updates	Verified the signed firmware using OPTIGA™ Trust M feature
Secure data (encryption)	Data encrypted and decrypted using the OPTIGA™ Trust M
Device authentication	Device authentication feature enabled in the OPTIGA™ Trust M
Device management (allow/deny)	Performed in AWS cloud
X.509 certificate support	A digital certificate to verify that a public key belongs to the hostname/domain, organization, or individual contained within the certificate.
Isolation of secure firmware from non-secure application	Stored in OPTIGA™ Trust M
Isolation of credentials (keys) in a tamper-resistant element	Stored in OPTIGA™ Trust M
Secure supply chain	Register RootCA in AWS and using RootCA creating the device certificate. Intermediate CA not used. Private key and device certificate are stored in the OPTIGA™ Trust M

About Arrow Engineering Services with eInfochips

eInfochips, an Arrow company, is a leading global provider of product engineering and semiconductor design services. With over 500+ products developed and 40M deployments in 140 countries, eInfochips continues to fuel technological innovations in multiple verticals. The company offers complete product lifecycle solutions including hardware design, firmware, application software, testing, re-engineering, and manufacturing support. With an innovation-centric fabric, eInfochips has enabled companies to develop customized evaluation kits, reference designs and next-generation, fully featured products on leading platforms.

Security Starter Kit Ordering Information

Part Number	Description
i.MX 8X-SSK	NXP i.MX 8X and Infineon OPTIGA™ TPM 2.0
STM32MP157-SSK	ST Micro STM32MP1 and Infineon OPTIGA™ TPM 2.0
STM32WB55-SSK	ST Micro STM32WB55 and Infineon OPTIGA™ Trust M
GG11-LTE-M-SSK	Silicon Labs Giant Gecko 11, XBee3 and Infineon OPTIGA™ Trust M

Resources

Arrow Embedded Security Resources Page: https:// www.arrow.com/embedded-security

Featured products, reference designs, and security services provided by Arrow and our supplier ecosystem

In Person

North America
+1 855 326 4757

Europe, Middle East, and Africa
+44 20 3936 5486

Asia-Pacific
+86 400 920 0628

Online

arrow.com

Five Years Out