Product Brief

# Security Starter Kit with i.MX 8X and OPTIGA™ TPM2.0

Arrow has worked closely with several technology suppliers to create a solution that employ's ten major security features and take the guesswork out of implementation and reducing your overall time to market. The Arrow Security Starter Kit integrates Yocto Linux open-source software framework, with a readily available Arrow 96boards single-board computer (SBC) based on the NXP i.MX 8X MPU, Infineon's OPTIGA™ TPM2.0 secure solution and AWS IoT Greengrass. AWS IoT Greengrass is software that lets you run local compute, messaging & data caching for connected IoT devices in a secure way. Using this kit, 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.

## Security Starter Kit with i.MX 8X and OPTIGA™ TPM2.0

This combination includes the Arrow 96boards SBC, based on the NXP i.MX 8X MPU and supports WiFi IEEE 802.11 a/b/g/n/ac and Bluetooth 4.2 connectivity. The Tresor Mezzanine Board adds advanced security features to the 96Boards SBCs and includes the OPTIGA™ SLB9670x or SLM9670x 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)

**Part Number: i.MX_8X-SSK**

| Security Feature Implemented | Description |
|---|---|
| Unique Device Identifier | EUI64 is used and stored in the OPTIGA™ TPM 2.0 |
| Secure Boot | Software based secure boot feature performed with OPTIGA™ TPM 2.0 |
| Secure OTA Updates | Implemented software-based capability for OTA updates with OPTIGA™ TPM 2.0 |
| Secure Data (encryption) | Data encrypted and decrypted using keys stored in the OPTIGA™ TPM 2.0 |
| Device Authentication | Device authentication feature enabled in the OPTIGA™ TPM 2.0 |
| Device Management (Allow/Deny) | Performed in AWS Cloud Services |
| Isolation of secure firmware from non-secure application | Stored in the OPTIGA™ TPM 2.0 |
| Isolation of credentials (keys) in a Tamper-resistant element | Stored in the OPTIGA™ TPM 2.0 |
| X.509 certificate support | A digital certificate to verify that a public key belongs to the Hostname/domain or organization and stored in the OPTIGA™ TPM 2.0 |
| Secure Supply Chain | Register Root CA in AWS and using Root CA to create the device certificate. An Intermediate CA is not employed. Private key and device certificate are stored in the OPTIGA™ TPM 2.0 |

## Out-of-the-Box Demonstration with Infineon OPTIGA™ TPM2.0 for Gateway/Edge Compute solutions

The demo integrates the Arrow 96boards SBC, based on the i.MX 8X MPU with the OPTIGA™ TPM 2.0 and AWS IoT Greengrass to securely communicate with the Cloud.

## i.MX_8X-SSK Kit Contents:

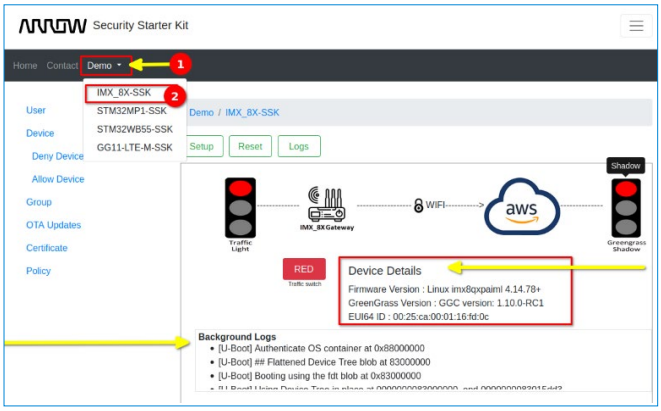
- Arrow 96boards I.IMX8X_AI_ML SBC
- Arrow 96boards Tresor Mezzanine card (with OPTIGA™ TPM 2.0 installed)
- SDcard – 16GB
- MicroUSB debug cable
- Power Supply
- User & Developer Guides and Cloud Connect Tool installation guide available on: https://www.arrow.com/en/products/imx-8x-ssk/arrow-development-tools
- Cloud Connect tool & FreeRTOS source code includes example code, application and demo provided on Github. https://github.com/ArrowElectronics/Security-Starter-Kits

### Gateway/Edge Compute Solutions


Tresor Mezzanine with OPTIGA™ TPM 2.0

Arrow 96Boards SBC based on the NXP i.MX 8X processor

### Cloud Connect Tool




## 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.


### Email

security@arrow.com

### Online

arrow.com/iot/iot-security


Five Years Out



11_10/20