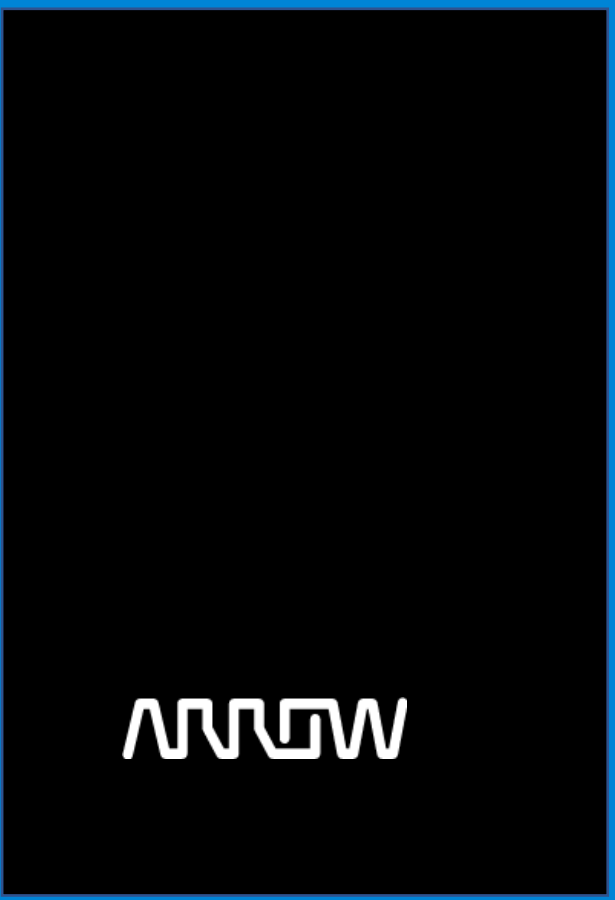
Sichere Cloud-Anbindung mit der Infineon PSoC64® Secure MCU Familie

Whitepaper
Sichere Cloudanbindung mit der Infineon PSoC64®
Secure MCU Familie

Dieter Kiermaier dieter.kiermaier@arrow.com
Technology Field Application Engineer
Arrow Central Europe GmbH



Warum sichere Cloud-Anbindung?

In Anwendungen wird es zunehmend wichtiger beziehungsweise zwingend erforderlich, dass die Root-of-Trust sichergestellt wird. Vom einfachsten Sensor-Node bis hoch zum Cloud Backend müssen alle Systembestandteile ihren Beitrag dazu leisten.

Die Frage nach dem "Warum?" lässt sich zum einen dadurch beantworten, dass das Thema Security zunehmend reguliert wird (siehe bspw. ETSI EN 303 645), andererseits sollte es aber auch im Interesse des Herstellers / Betreibers liegen, dass sensible Daten geschützt sind und vor allem auch Einfallstore in die IT-Systeme überhaupt nicht erst geöffnet werden.

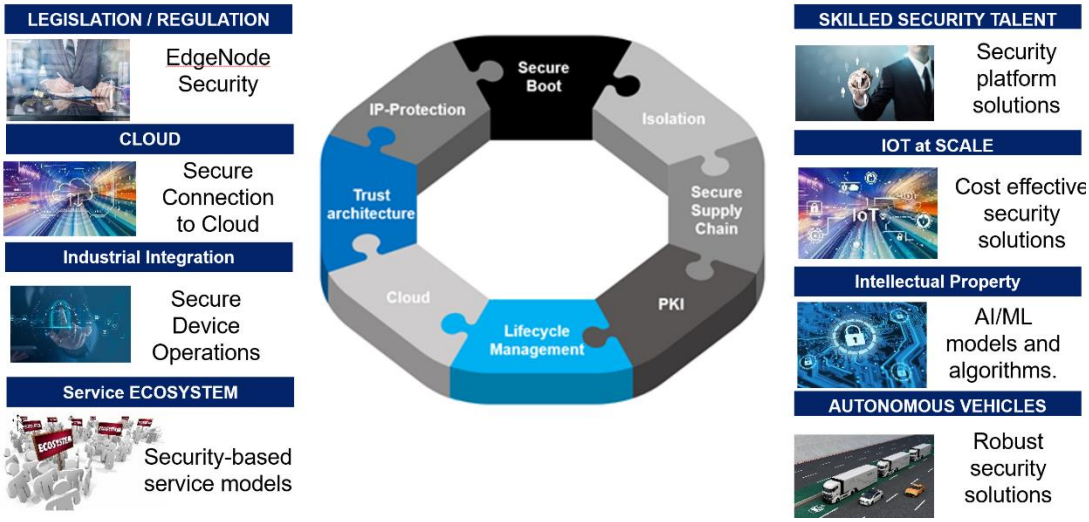
Der europäische Standard ETSI EN 303 645 regelt die grundlegenden Anforderungen an ein Consumer Device für das Internet der Dinge. In diese Geräteklasse fallen zum Beispiel alle Arten von Gateways, aber auch Alarmanlagen, vernetzte Temperaturfühler, Rauchmelder und dergleichen mehr.

Um Entwickler bestmöglich zu unterstützen und eine möglichst kurze Time-to-market zu ermöglichen, stellen Cypress, Arm® und Arrow Electronics mit vereintem Know-How mehrere Entwicklungskits inklusive der passenden Firmware zur Verfügung.

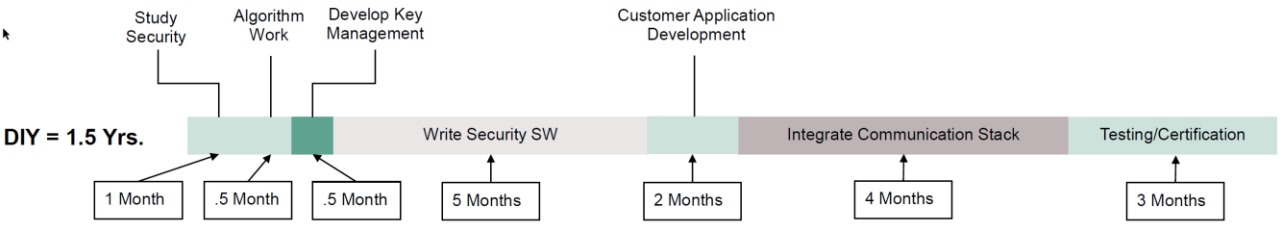
Arm® hat vor kurzem eine Platform Security Architecture, unterstützt durch die Trusted Firmware (TF-M), welche auf dem Cypress PSoC® 64 erstmals vollständig implementiert wurde und den Kunden zur Verfügung steht. Die PSA unterstützt alle Anforderungen der ETSI und adressiert darüber hinaus noch die Konfiguration der Geräte:

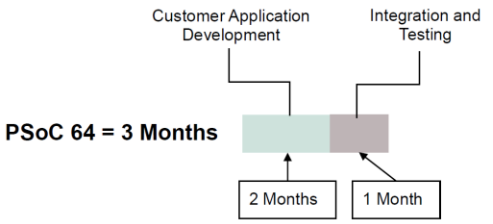
Requirement	SB-327	NIST 8259A	ETSI 303 645	PSA Certified with PSoC 64
Authentication / Password	✓	✓	✓	✓
Configuration		✓		✓
Crypto		✓	✓	✓
Hardening		✓	✓	✓
Logging		✓		✓
Privacy		✓	✓	✓
Secure Storage		✓	✓	✓
Update		✓	✓	✓

Die folgenden Trends im Bereich Security sehen wir im täglichen Gespräch mit unseren Kunden:



Wie sich unschwer erahnen lässt, bringen diese Themen eine Menge neuer Herausforderungen mit sich. Das Ziel von Arrow als Distributor ist, Sie beim Design bestmöglich zu unterstützen und zu beraten, damit möglichst viele Anforderungen bereits durch die Auswahl einer idealen Plattform abgedeckt werden. Speziell im Bereich Embedded Security sticht die neue PSoC64® Microcontroller-Familie von Infineon hervor. Die folgende Grafik zeigt eine Abschätzung der möglichen Entwicklungsaufwände für die benötigen Module und gibt einen Anhalt, wie viel Entwicklungsaufwand durch Einsatz des PSoC®64 eingespart werden kann:

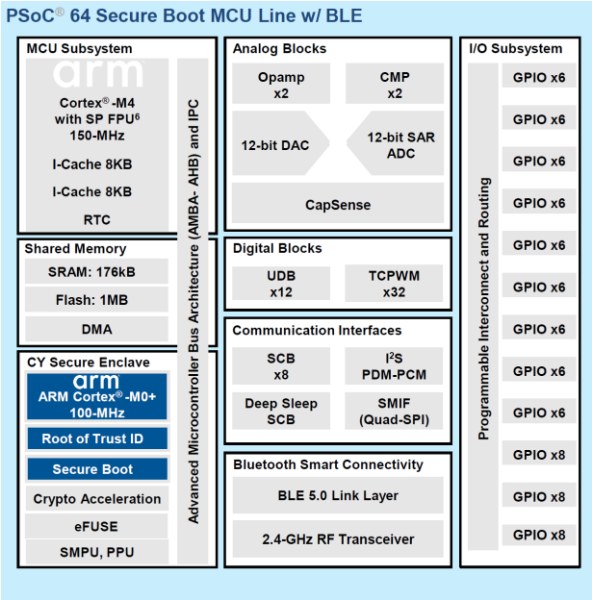




Design Your Secure IoT Device in 1/5 the time using certified FW that comes with PSoC 64!

PSoC®64 Architektur

Das folgende Blockschaltbild gibt einen Überblick über die Hardware-Architektur und die wichtigsten Features:



MCU Subsystem
- 150-MHz Arm® Cortex®-M4F with ultra-low-power and low-power operation modes
- Up to 1MB Flash, 288KB SRAM with DMA

CY Secure Enclave
- Hardware isolated, 100-MHz Arm Cortex®-M0+ with privileged access to memory and IO
- Hardware isolated keys, cryptographic functions and trusted applications
- Hardware root-of-trust providing secure device identity
- Secure boot with attestation and anti-rollback
- Advanced hardware cryptographic acceleration and TRNG
- CY Secure Bootloader for secure firmware updates

Digital Blocks and Communication Interfaces
- 12 x universal digital blocks (UDBs): custom digital peripherals
- 24 x 16-bit and 8 x 32-bit timer/counter/pulse-width modulation blocks (TCPWM)1
- 8 x serial communication blocks (SCBs)2, deep-sleep SCB

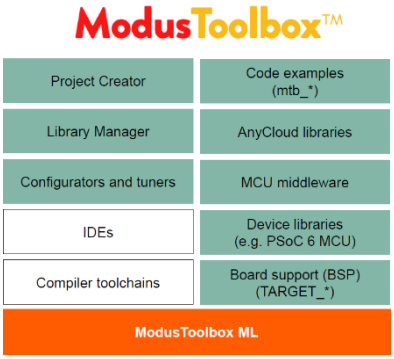
Bluetooth Smart Connectivity
- Bluetooth Low Energy (BLE) 5.0 radio with 2-Mbps data throughput

Die Secure Enclave ist über IPC (Inter Process Communication) an dem Applikationsprozessor angebunden. Erwähnenswert sind die programmierbaren Digital- und Analogblöcke, die in dieser Form einmalig sind. Ein BLE 5.0 Radio ist ebenfalls bereits integriert, so dass hoch integrierte Lösungen möglich werden.

Andere PSoC® 64 Derivate ohne BLE haben bis zu 2MByte Flash und 1MByte SRAM.

Wichtig zu erwähnen istaußerdem , dass es zwei PSoC® 64 Linien gibt:
* PSoC® 64 Standard Secure MCU Line für IoT Gateways vorbereitet für AWS und FreeRTOS
* PSoC® 64 Secure Boot MCU Line (mit oder ohne BLE) wird durch die ModusToolbox konfiguriert

Für die **Entwicklung** kann die kostenlose Infineon ModusToolbox verwendet werden:



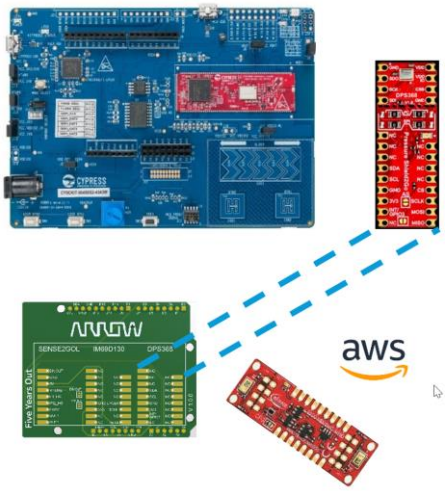
Es handelt sich hier um eine Eclipse IDE mit vielen Tools zum Anlegen, Konfigurieren, Kompilieren und Debuggen von Projekten. Die Toolbox wird durch Beispiele, Libraries, Device Drivers und Board Support Packages vervollständigt.

Unter den Tools ist z.B. ein Bluetooth Konfigurator oder ein Library Manager. Neu ist das Machine Learning (ML) Paket, welches zur Evaluierung und Benchmarking auf Infineon MCUs genutzt werden kann.

Wie adressiert die PSoC®64 Familie die speziellen Security Anforderungen?

Durch reine Hardware kann der geforderte Umfang selbstverständlich nicht realisiert werden. Aus diesem Grund existiert ein umfangreiches Portfolio aus Software-Lösungen, Entwicklungs-Tools und Referenz-Implementierungen, aus denen sich Entwickler je nach Bedarf bedienen können.

Das Entwicklungskit umfasst alle nötigen Bestandteile inklusive eines AWS Vouchers, um sofort zu starten:



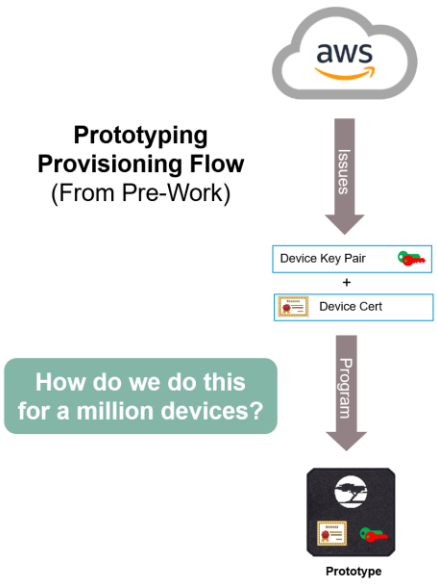
Was ist enthalten:

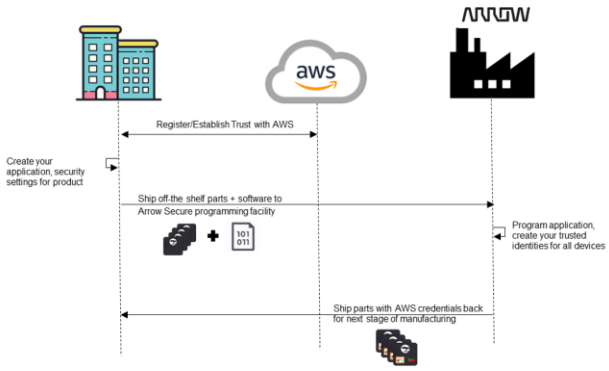
- PSoC® 64 Standard Secure AWS Wi-Fi / BLE Pioneer Kit
- $10 AWS Cloud Credits

Zusätzlich erhältlich:

- Arrow PSoC6_IoT_Sensor_Shield Custom Interface Board
- Shield2Go DPS368 Barometric Pressure Sensor Board
- Shield2Go IM69D MEMS Microphone Board

Darüber hinaus bietet Arrow über das Programmiercenter auch einen **Secure Provisioning** Service, der die Lücke zwischen Entwicklung und dem Serieneinsatz schließt.





Arrow Electronics guides innovation forward for over 180,000 leading technology manufacturers and service providers. With 2020 sales of $29 billion, Arrow develops technology solutions that improve business and daily life. Learn more at **arrow.com/fiveyearsout.com**

Arrow Electronics, Inc.
9201 East Dry Creek Road
Centennial, CO 80112 USA
arrow.com

Five Years Out