Skalierbare, sichere Anwendungen **erstellen, in Betrieb nehmen** und **pflegen**

Arduino Portenta X8 mit dem i.MX 8M Mini-Anwendungsprozessor von NXP und dem EdgeLock® Secure Element SE050

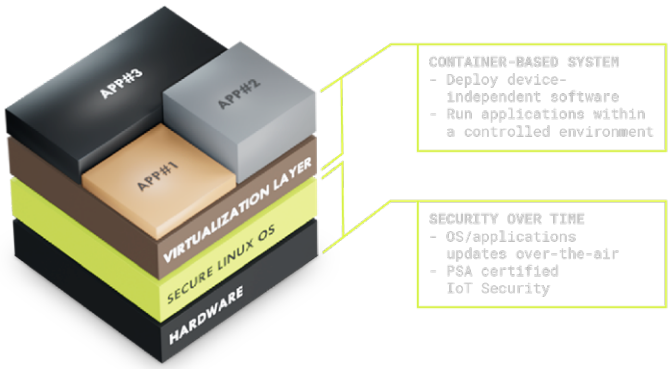
Ein Beitrag von NXP Semiconductors

Ein IoT-Gerät auf den Markt zu bringen ist mit erheblichem Design- und Entwicklungsaufwand verbunden - mit Skalierbarkeitsproblemen, Sicherheitsanforderungen und Gerätebeschränkungen an allen Ecken und Enden. Das Hinzufügen von Intelligenz macht es noch komplizierter. Daher ist die Auswahl der richtigen Entwicklungshard- und -software entscheidend, um sichere Edge-Produkte schneller auf den Markt zu bringen. In diesem Artikel wird die Arduino-Plattform Portenta X8 vorgestellt, ein industrietaugliches, sicheres System on Module (SoM), das auf dem Applikationsprozessor i.MX 8M Mini von NXP und einem integrierten Hardware-Sicherheitselement EdgeLock®-SE050 basiert. Diese PSA-zertifizierte Plattform ist auch *Arm® SystemReady IR* für Linux für garantierte Sicherheit auf Embedded-Arm-SoCs zertifiziert.

Arduino Portenta X8 ist ein leistungsfähiges, industrietaugliches System auf einem Modul mit vorinstalliertem Linux®-Betriebssystem, das dank seiner modularen Container-Architektur in der Lage ist, geräteunabhängige Software auszuführen. Es bietet zwei Ansätze: Flexibilität bei der Nutzung von Linux kombiniert mit Echtzeitanwendungen durch die Arduino-Umgebung. Die integrierte WLAN/Bluetooth®-Low-Energy-Konnektivität ermöglicht die Fernaktualisierung von Betriebssystemen und Anwendungen, wobei die Linux-Kernel-Umgebung stets auf dem höchsten Leistungsniveau gehalten wird.

Sicherheit auf dem neuesten Stand der Technik

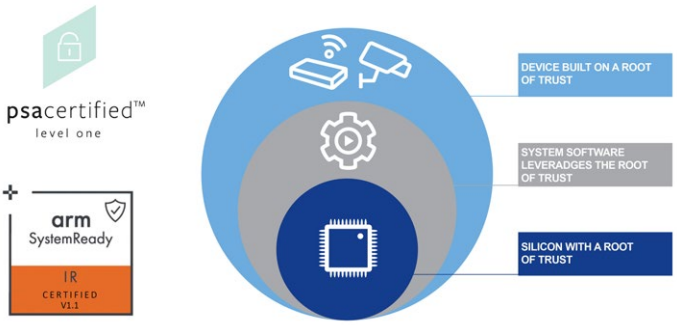
Das containerbasierte System vereint verschiedene Sicherheitsebenen, angefangen bei der Hardware-Ebene, die das Secure Element von NXP enthält. Es nutzt die Cloud-basierte DevOps-Plattform von Foundries.io [1], um die Art und Weise, wie Embedded-Linux-Lösungen entwickelt, getestet, bereitgestellt und gewartet werden, neu zu definieren. Der Portenta X8 enthält das anpassbare Open-Source-Betriebssystem Linux-MicroPlatform, das mit den besten Industriepraktiken für End-to-End-Sicherheit, inkrementellen OTA-Updates und Flottenmanagement entwickelt wurde.



Portenta X8 Container und Sicherheit.

Die Virtualisierungsschicht ermöglicht es Anwendern, geräteunabhängige Software in einer kontrollierten Umgebung auszuführen. Sie können ihre eigenen Container mit Docker erstellen und vorgefertigte Images vom Docker Hub oder anderen öffentlichen Registries herunterladen, um eine maßgeschneiderte Anwendung zu erstellen. Wenn ein Entwickler in die Welt der eingebetteten Systeme einsteigen möchte, kann er dies ganz einfach tun, indem er seine Anwendung erstellt, sie in einem Container überführt, sie auf dem Board installiert und sie sofort testet. Durch die Kombination von Linux-Fähigkeiten und Arduino-Erfahrung ergeben sich zahlreiche Möglichkeiten.
Portenta X8 hat die PSA-Zertifizierung erhalten. Das NXP EdgeLock SE050 Hardware-Sicherheitselement bietet Schlüsselgenerierung, beschleunigte Kryptooperationen und sichere Speicherung. X8 erhielt außerdem die Arm® SystemReady-Zertifizierung [2] und integrierte Parsec-Services, was es zu einem der ersten Cassini-Produkte oder Cloud-Native-Edge-Geräte macht, die für Entwickler auf dem Markt verfügbar sind. Es läuft nahtlos auf Fedora IoT, Fedora Server, Debian und Linux-microPlatform. Der Portenta X8 ermöglicht die Migration von Cloud-nativen Workloads von der Cloud zur Edge und trägt zu

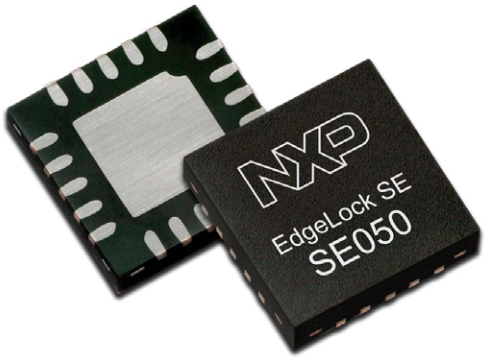
einer Cloud-nativen Entwicklererfahrung im vielfältigen und sicheren IoT-Ökosystem von Arm bei.



Architektur der Plattform-Sicherheit.

EdgeLock SE050 - Ein Anker des Vertrauens für das IoT

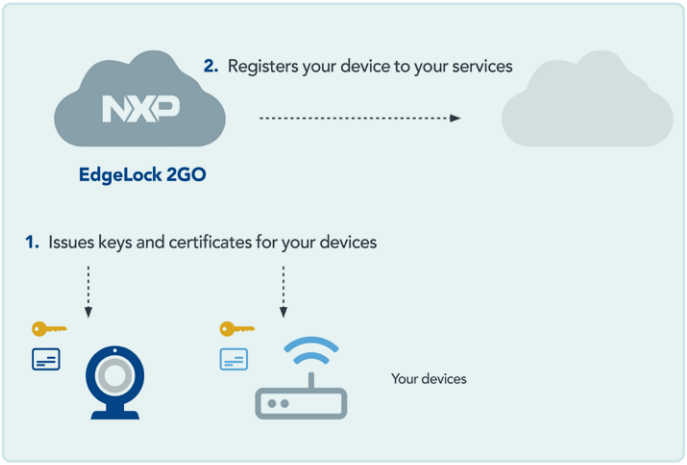
Der EdgeLock SE050 [3] von NXP ist eine diskrete und fälschungssichere Sicherheitshardware zum Schutz der Identität eines Geräts, einschließlich kryptografischer Schlüssel und Zertifikate. Es handelt sich um ein eigenständiges, eingebettetes Sicherheitselement, das über die I²C-Schnittstelle mit dem Hauptprozessor verbunden ist. Der EdgeLock SE050 ist nach *Common Criteria EAL 6+* für die Hardware und das Betriebssystem zertifiziert. Dieses sofort gebrauchsfertige Sicherheitselement für IoT-Geräte bietet eine Vertrauensbasis auf IC-Ebene und liefert echte End-to-End-Sicherheit – von der Edge bis zur Cloud - ohne die Notwendigkeit, Sicherheitscode zu implementieren oder kritische Schlüssel und Berechtigungsnachweise zu verwalten.



Quelle des Vertrauens auf Silizium: Das EdgeLock® SE050 Secure Element.

EdgeLock SE050 als gebrauchsfertige Lösung mit mehreren vorimplementierten kryptografischen Algorithmen und Protokollen sowie einem kompletten Produktunterstützungspaket vereinfacht die Entwicklung und die Markteinführungszeit. Zusätzlich zu den Bibliotheken für verschiedene MCUs und MPUs bietet das Support-Paket auch die Integration mit vielen gängigen Betriebssystemen wie Linux, RTOS und Android.

Entwickler von IoT-Geräten stehen vor zwei großen Herausforderungen, wenn sie Geräte mit der Cloud verbinden wollen: die Bereitstellung der Geräteidentität und die Verwaltung der Geräteidentitäten nach der Freigabe für das Feld. Ersteres bezieht sich auf die Installation von Schlüsseln und Zertifikaten, der zweite Punkt auf die Aktualisierung, das Hinzufügen oder den Entzug von Schlüsseln und Zertifikaten während des gesamten Lebenszyklus des Geräts.
Um Entwickler bei der Bewältigung dieser Herausforderungen zu unterstützen, bietet NXP den *EdgeLock 2GO Managed Service* [4] an. Bei der Plattform handelt es sich um eine speziell entwickelte Hardware- und Servicekombination, die eine siliziumbasierte Vertrauenswürdigkeit (Root of Trust) einrichtet. EdgeLock 2GO stellt die für IoT-Geräte erforderlichen Identitäten aus und installiert die Anmeldedaten sicher in der EdgeLock-SE050-Hardware. Außerdem registriert der Service das IoT-Gerät direkt automatisch beim Cloud-Dienst.



NXP regelt die Geräteberechtigungen.

Dieser flexible Dienst unterstützt mehrere Arten von Berechtigungsnachweisen und wendet je nach Projekt unterschiedliche Konfigurationen an. Berechtigungsnachweise (Device Credentials) können erneuert oder zu im Feld freigegebenen Geräten hinzugefügt werden. Mit der Inbetriebnahme von EdgeLock SE050 und EdgeLock 2GO erhalten Anwender eine End-to-End-Lösung, die einfach, sicher und flexibel ist. Mit der zunehmenden Verbreitung des IoT steigen auch die Risiken. Die EdgeLock-Kombination von NXP mit ihrer hardwarebasierten Sicherheit und dem Service für die Verwaltung von Berechtigungsnachweisen bietet Geräteherstellern Sicherheit in ihrem Geschäft. Wenn NXP EdgeLock die Bereitstellung eines Geräts unterstützt, verkürzt sich nicht nur die Zeit bis zur Markteinführung, es werden auch die täglichen Kosten für den Betrieb einer IoT-Bereitstellung gesenkt, während gleichzeitig die Gewissheit besteht, dass die Geräte durch ein hohes Maß an Sicherheit geschützt sind.

Entfesseln Sie die Kraft: Mehr Geschwindigkeit und verbesserte Effizienz

Das System-on-Chip i.MX 8M Mini [5] ist der erste eingebettete Multicore-Anwendungsprozessor von NXP, der in der fortschrittli-

chen 14LPC FinFET-Prozesstechnologie gefertigt wird und höhere Geschwindigkeit und eine verbesserte Energieeffizienz bietet. Die i.MX 8M Mini-Familie von Anwendungsprozessoren vereint High-Performance-Computing, Energieeffizienz und eingebettete Sicherheit für die schnell wachsende Zahl an Edge-Node-Computing-, Streaming-Multimedia- und Machine-Learning-Anwendungen.

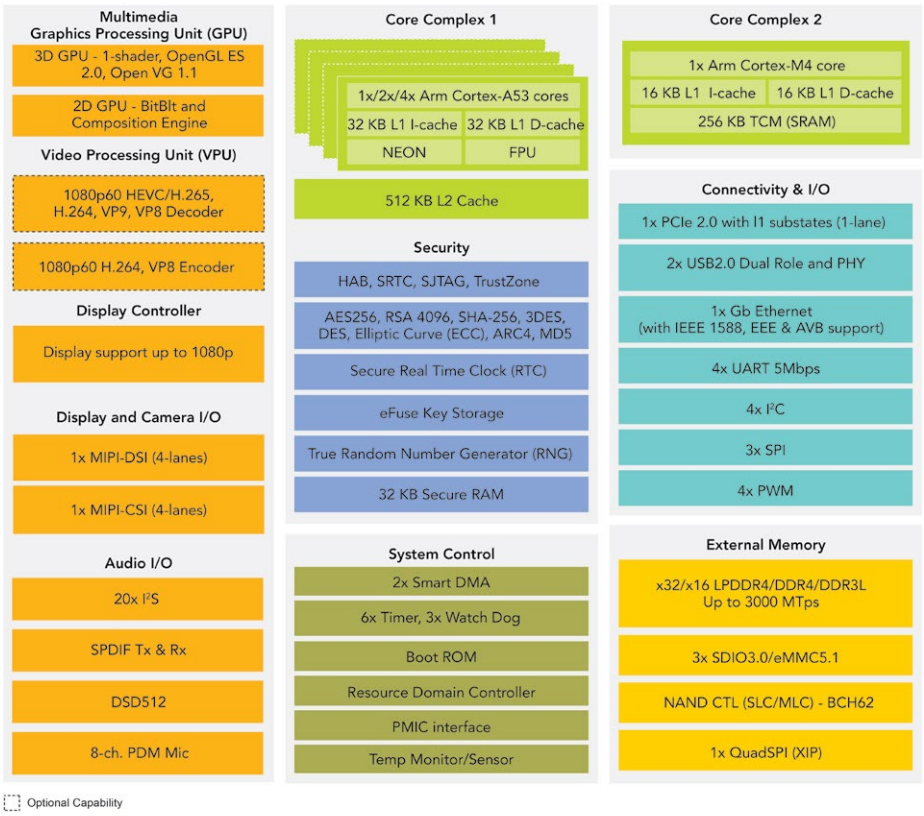
Das System-on-Chip i.MX 8M Mini wird in Single-, Dual- und Quadcore-Varianten mit Arm® Cortex®-A53 angeboten, die mit bis zu 1,8 GHz pro Kern arbeiten. Der in einem fortschrittlichen Low-Power-Prozess gefertigte Kernkomplex ist für lüfterlosen Betrieb, niedrige thermische Systemkosten und lange Batterielebensdauer optimiert. Die Cortex-A-Kerne können abgeschaltet werden, während das Cortex-M4-Subsystem eine stromsparende Systemüberwachung in Echtzeit durchführt. Der DRAM-Controller unterstützt 32-Bit/16-Bit-LPDDR4-, DDR4- und DDR3L-Speicher und bietet damit eine große Flexibilität beim Systemdesign.
Die Kern-Optionen sind beim i.MX 8M Mini für einen extrem niedrigen Stromverbrauch optimiert, der in bestimmten Anwendungen sogar unter einem Watt liegt, und bieten dennoch die nötige Rechenleistung für Consumer-, Audio- und Industrie-Anwendungen sowie beim Machine-Learning-Training und Inferencing bei einer Reihe von Cloud-Anbietern. Das SoC i.MX 8M Mini bietet außerdem Hardware-Beschleunigung für 1080p-Videos, um Zwei-Wege-Videoanwendungen zu ermöglichen, 2D- und 3D-Grafiken für ein reichhaltiges visuelles HMI-Erlebnis sowie fortschrittliche Audio-Funktionen. Eine umfangreiche Auswahl an Hochgeschwindigkeitsschnittstellen ermöglicht eine breitere Systemkonnektivität und zielt auf eine Qualifizierung auf industrieller Ebene ab.
Die Anwendungsbeispiele umfassen:

Industrielle Automatisierung
Der Portenta X8 kann dann als Multiprotokoll-Gateway fungieren und Daten über WLAN, LoRa, NB/IoT, LTE Cat.M1 an die Cloud oder das Enterprise-Resource-Planning-System senden. Durch die Verfügbarkeit von Linux-Containern wie ROS innerhalb der Arduino-Umgebung eignet sich der Portenta X8 hervorragend für autonome, fahrerlose Fahrzeuge.

Gebäude-Automatisierung
Im Zusammenspiel mit intelligenten Umgebungssensoren ermöglicht Portenta X8 die Implementierung von Echtzeit-ML und Bildverarbeitung „on the edge". Intelligente Kioske nutzen in der Regel mehrere Komponenten wie Kartenleser, Kameras oder Mikrofone, was eine vielfältige Auswahl an I/Os erfordert. In Kombination mit einem Max-Carrier gewährleistet der Portenta X8 WLAN-Konnektivität und ermöglicht es Administratoren, die Nutzung der Geräte aus der Ferne zu überwachen. Der Portenta X8 kann gleichzeitig Klimasysteme steuern, intelligente Geräte ein- und ausschalten, die Beleuchtung autonom regeln und die Zugänge kontrollieren.

Beginnen Sie noch heute Ihre Entwicklung mit dem industrietauglichen, sicheren Portenta-X8-SoM [6] mit herausragender Rechenleistung.

(20576-02)RG



Blockschaltung des Anwendungsprozessors i.MX 8M Mini.

WEBLINKS

[1] Foundries.io: https://foundries.io/
[2] Arm SystemReady: www.arm.com/architecture/system-architectures/systemready-certification-program
[3] EdgeLock SE050: https://bit.ly/EdgeLockSE050
[4] EdgeLock 2GO: https://bit.ly/EdgeLock2GO
[5] i.MX 8M Mini: https://bit.ly/iMX8MMini
[6] SoM Portenta X8: www.arduino.cc/pro/hardware/product/portenta