Build, Deploy, and Maintain Scalable, Secure Applications

With Arduino Portenta X8 Featuring NXP's i.MX 8M Mini Applications Processor and EdgeLock® SE050 Secure Element

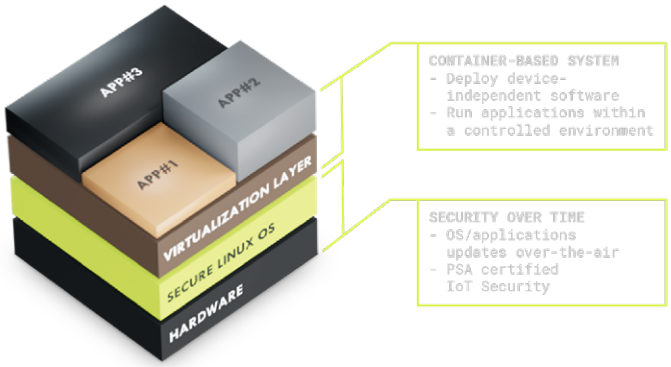
Contributed by NXP Semiconductors

Bringing an IoT device to the market involves significant design and development effort – with scalability issues, security challenges, and device limitations around every corner. Adding intelligence makes it even more complicated. This makes the selection of the right development hardware and software critical to getting secure edge products to market faster. This article introduces the Arduino Portenta X8 platform, an industrial-grade, secure SOM based on NXP's i.MX 8M Mini applications processor and an onboard EdgeLock® SE050 hardware secure element. This PSA-certified platform is also Arm® SystemReady IR for assured security.

Arduino Portenta X8 is a powerful, industrial-grade system on a module with Linux® OS preloaded onboard, capable of running device-independent software because of its modular container architecture. It offers two approaches: flexibility of usage of Linux combined with real-time applications through the Arduino environment. Onboard Wi-Fi/Bluetooth® Low Energy connectivity allows remote OS/application updates, always keeping the Linux kernel environment at top performance levels.

State-of-the-Art Security

The container-based system integrates different layers of security starting from the hardware layer which includes NXP's Secure Element. It utilizes the cloud-based DevOps platform from Foundries.io [1] to reinvent the way embedded Linux solutions are built, tested, deployed and maintained. The Portenta X8 includes the customizable open-source Linux microPlatform OS, built using best industry practices for end-to-end security, incremental OTA updates and fleet management.

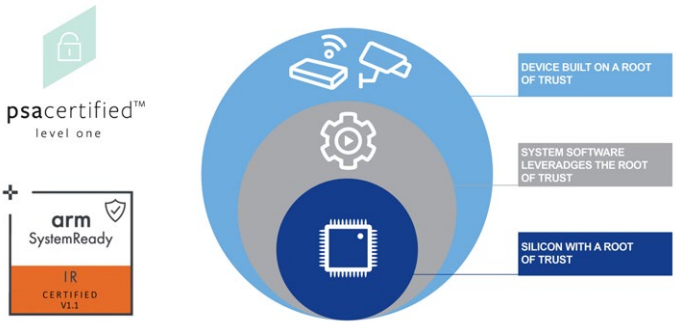


Portenta X8 Container and Security.

The virtualization layer allows users to deploy device-independent software running within a controlled environment. They can create their own containers using Docker and download premade images from Docker Hub or other public registries available to build a tailored application. If the developer wants to enter the embedded world, they can do so easily by building their application, running it on a container, putting it on the board and testing it out of the box. This provides a wide range of opportunities by mixing the Linux capabilities and the Arduino standard experience.

Portenta X8 achieved PSA Certification and the NXP EdgeLock SE050 hardware secure element provides key generation, accelerated crypto operations and secure storage. X8 also achieved Arm® SystemReady [2] certification and integrated Parsec services, making it one of the first Cassini Products or Cloud Native Edge devices available to developers in the market. It seamlessly runs Fedora IoT, Fedora Server, Debian and Linux microPlatform. Enabling the migration of cloud-na-

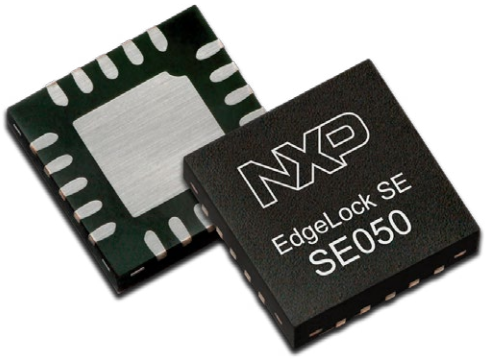
tive workloads from the Cloud to the edge, the Portenta X8 contributes to a cloud-native developer experience across Arm's diverse and secure IoT ecosystem.



Platform Security Architecture.

EdgeLock SE050 – A Trust Anchor for IoT

NXP's EdgeLock SE050 [3] is a discrete and tamper-resistant security hardware for protecting the identity of a device, including cryptographic keys and certificates. It's a standalone embedded secure element that is attached to the main processor over the I2C interface. The EdgeLock SE050 is certified Common Criteria EAL 6+ for the hardware and operating system. This ready-to-use secure element for IoT devices provides a root of trust at the IC level and delivers real end-to-end security – from edge to cloud – without the need to implement security code nor handle critical keys and credentials.

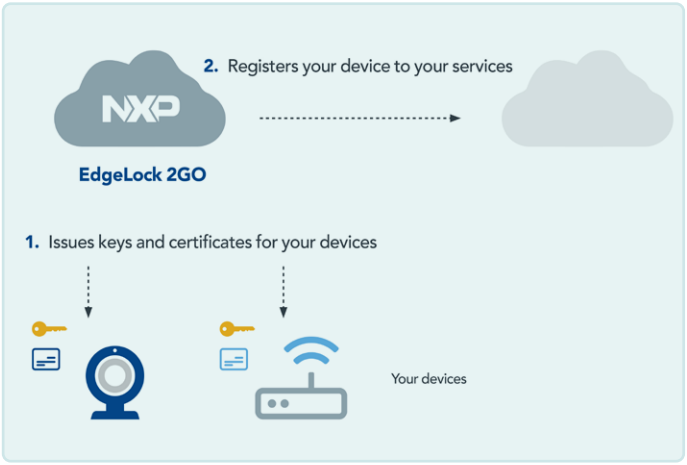


Silicon-based Root of Trust: EdgeLock® SE050 Secure Element.

Delivered as a ready-to-use solution, EdgeLock SE050 comes with multiple pre-implemented cryptographic algorithms and protocols and a complete product support package that simplifies design-in and reduces time to market. In addition to libraries for different MCUs and MPUs, the support package also offers integration with the many common OSs including Linux, RTOS and Android.

IoT device designers are facing two major challenges when implementing device onboarding to the cloud: provisioning of the device identity and managing device identities once released to the field. The provisioning of the device refers to the installation of keys and certificates. Managing device identities refers to the update, addition or revocation of keys and certificates throughout the device lifecycle.

To help designers solve these challenges, NXP provides the EdgeLock 2GO [4] managed service. The platform is a purpose-built hardware and service combination that establishes a silicon-based root of trust. EdgeLock 2GO issues the identities required for IoT devices and installs the credentials securely into the EdgeLock SE050 hardware. It also automatically registers the IoT device directly to the cloud service.



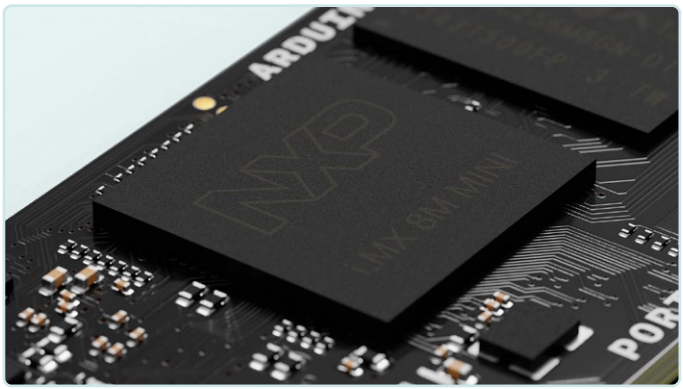
NXP Manages Device Credentials.

This flexible service supports multiple types of credentials and applies different configurations depending on the project. Credentials can be renewed or added to devices released in the field. With the commissioning of EdgeLock SE050 and EdgeLock 2GO, users get an end-to-end solution that is simple, secure and flexible.

As IoT continues to expand, so do the risks. NXP's EdgeLock combination, with its hardware-based security and service for credential management, gives device manufacturers a safer way to do business. With NXP EdgeLock supporting the deployment of a device, it reduces time-to-market and lowers the day-to-day costs of operating an IoT deployment while having the confidence of knowing devices are protected by high-level security.

Unleash the Power: Providing More Speed and Improved Efficiency

The i.MX 8M Mini [5] SoC is NXP's first embedded multicore applications processor built using advanced 14LPC FinFET process technology, providing more speed and improved power efficiency. The i.MX 8M Mini family of applications processors brings together high-performance computing, power efficiency, and embedded security needed to drive the fast-growing edge node computing, streaming multimedia, and machine learning applications.



The i.MX 8M Mini SoC is offered in single, dual and quadcore variants using Arm® Cortex®-A53 operating at up to 1.8 gigahertz per core. Delivered in advanced low-power process, the core complex is optimized for fanless operation, low thermal system cost and long battery life. The Cortex-A cores can be powered off while the Cortex-M4 subsystem performs low-power, real-time system monitoring. The DRAM controller supports 32-bit/16-bit LPDDR4, DDR4, and DDR3L memory, providing great system design flexibility.

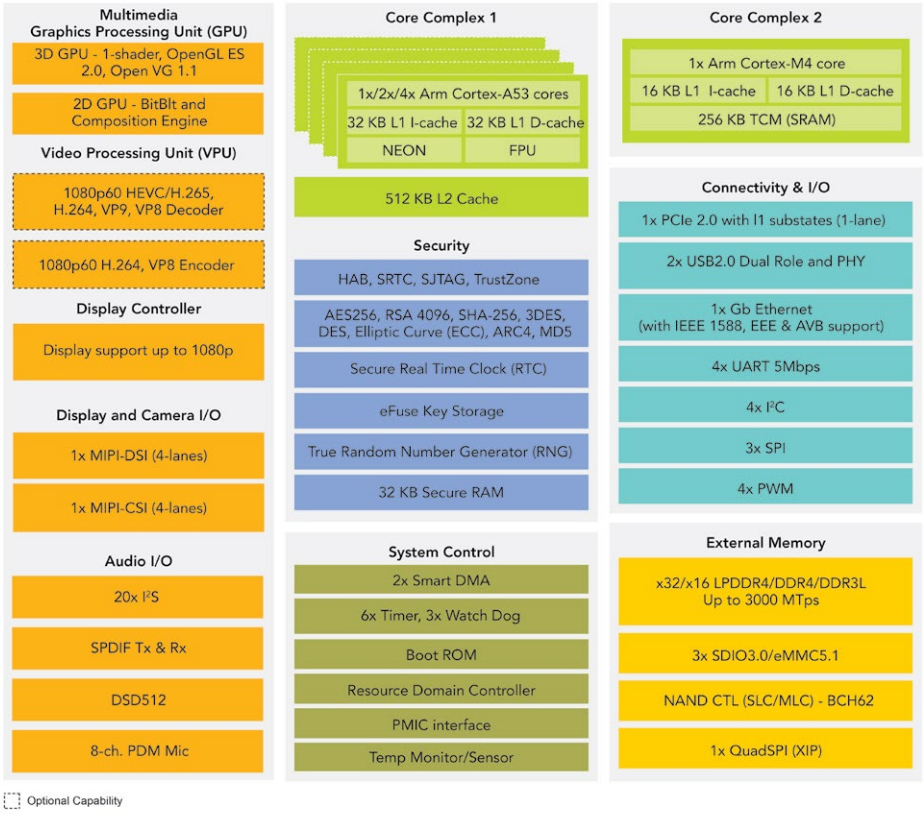
i.MX 8M Mini core options are optimized for ultra-low-power, even sub-Watt in specific applications, but offer the breadth of processing power necessary for consumer, audio, industrial, machine learning training and inferencing across a range of cloud providers. The i.MX 8M Mini SoC also packs-in hardware 1080p video acceleration to enable two-way video applications, 2D and 3D graphics to provide a rich visual HMI experience, and advanced audio capabilities to enable audio-rich applications. An extensive selection of high-speed interfaces enables broader system connectivity and targets industrial-level qualification.

Application Examples Include:

- **Industrial Automation**
  - The Portenta X8 can then act as a multi-protocol gateway, sending data to the Cloud or ERP system via Wi-Fi, LoRa, NB/IoT, LTE Cat.M1.
  - The availability of Linux containers like ROS within the Arduino environment makes the Portenta X8 a great fit for autonomous guided vehicles.
- **Building Automation**
  - Interacting with environmentally smart sensors, Portenta X8 allows the implementation of real-time ML and image processing on the edge.
  - Smart kiosks usually leverage several components (e.g. card readers, cameras, microphones), requiring a diverse selection of I/Os. When combined with a Max Carrier, the Portenta X8 ensures Wi-Fi connectivity and allows administrators to remotely monitor machine usage.
  - The Portenta X8 can simultaneously control HVAC systems, switch on/off smart appliances, autonomously adjust lighting and control accesses on the edge.

Start developing today with the industrial-grade, secure Portenta X8 SOM [6] with outstanding computational density.

220576-01



i.MX 8M Mini Applications Processor Block Diagram

WEB LINKS

[1] Foundries.io: https://foundries.io/
[2] Arm SystemReady: https://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] Portenta X8 SOM: https://www.arduino.cc/pro/hardware/product/portenta-x8