créez, déployez et **maintenez** des applications **évolutives et sécurisées**

avec Arduino Portenta X8 équipé du mini processeur d'applications i.MX 8M de NXP et de l'élément de sécurité EdgeLock® SE050

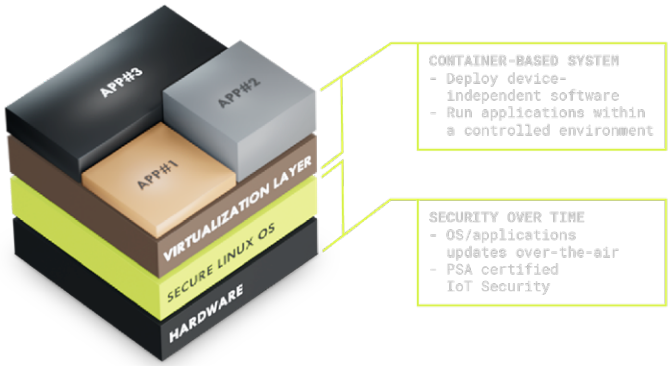
Contribué par NXP Semiconductors

La mise sur le marché d'un dispositif IdO implique des efforts de conception et de développement considérables avec des problèmes d'évolutivité, des défis de sécurité et des limitations de dispositifs à chaque coin de rue. L'ajout d'intelligence complexifie encore plus. C'est pourquoi la sélection du bon matériel et du bon logiciel de développement est essentielle pour mettre plus rapidement sur le marché des produits périphériques sécurisés. Cet article présente la plateforme Arduino Portenta X8, un *SoM* sécurisé de qualité industrielle basé sur le miniprocesseur d'applications i.MX 8M de NXP et un élément matériel de sécurité EdgeLock® SE050 intégré. Cette plateforme certifiée PSA est également Arm® SystemReady IR pour une sécurité assu.

Arduino Portenta X8 est un système puissant de qualité industrielle sur un module avec Linux® préchargé à bord, capable d'exécuter des logiciels indépendants du dispositif grâce à son architecture modulaire en conteneur. Il offre deux approches : la flexibilité d'utilisation de Linux combinée à des applications en temps réel via l'environnement Arduino. La connectivité wifi/BLE embarquée permet de mettre à jour le système d'exploitation et les applications à distance, tout en maintenant l'environnement du noyau Linux à un niveau de performance optimal.

Sécurité de pointe

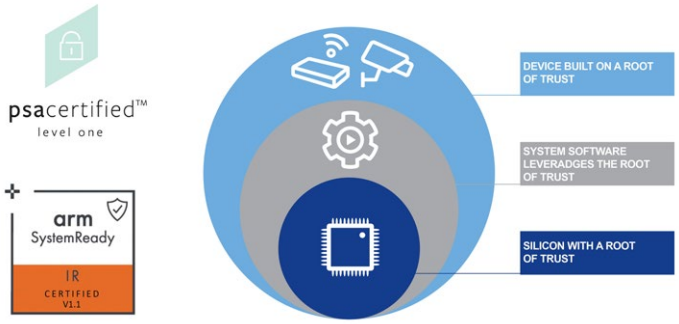
Le système basé sur des conteneurs intègre différentes couches de sécurité, à commencer par la matérielle qui comprend le *Secure Element* de NXP. Il utilise la plateforme DevOps basée sur le cloud de Foundries.io [1] pour réinventer la manière dont les solutions Linux embarquées sont construites, testées, déployées et maintenues. Le Portenta X8 comprend le système d'exploitation de microplateforme Linux open-source personnalisable, conçu selon les meilleures pratiques de l'industrie en matière de sécurité de bout en bout, de mises à jour *OTA* incrémentielles et de gestion de flotte.



Portenta X8 Container and Security.

La couche de virtualisation permet aux utilisateurs de déployer des logiciels indépendants des appareils et fonctionnant dans un environnement contrôlé. Ils peuvent créer leurs propres conteneurs à l'aide de Docker et télécharger des images préfaites à partir de Docker Hub ou d'autres registres publics disponibles pour conçevoir une application sur mesure. Si le développeur souhaite intégrer de l'embarqué, il peut le faire facilement en l'exécutant sur un conteneur, en la plaçant sur la carte et en la testant dès sa sortie de la boîte. Cela offre un large éventail de possibilités en mélangeant les capacités de Linux et d'Arduino.
Portenta X8 a obtenu la certification PSA et l'élément matériel de sécurité NXP EdgeLock SE050 assure la génération de clés, l'accélération des opérations cryptographiques et le stockage sécurisé. Il a également obtenu la certification Arm® SystemReady [2] et a intégré les services Parsec, ce qui en fait l'un des premiers produits Cassini ou dispositifs Edge natifs du cloud disponibles pour les développeurs sur le marché. Il fonctionne de manière transparente avec Fedora IoT, Fedora Server, Debian et la microplateforme Linux. En permettant la migration des charges de travail du cloud vers la périphérie, le

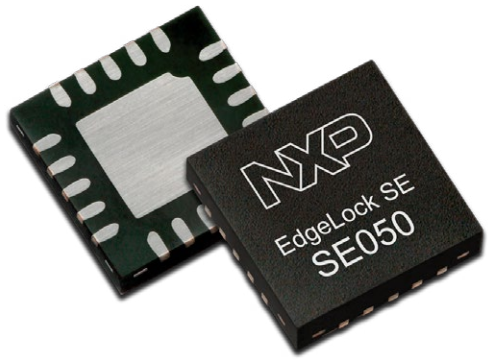
Portenta X8 contribue à une expérience de développeur cloud-native à travers l'écosystème IdO diversifié et sécurisé d'Arm.



Platform Security Architecture.

EdgeLock SE050 - Un ancrage de confiance pour l'IdO

L'EdgeLock SE050 [3] de NXP est un matériel de sécurité discret et inviolable destiné à protéger l'identité d'un dispositif, y compris les clés cryptographiques et les certificats. C'est un élément intégré relié au processeur principal via l'interface I²C. L'EdgeLock SE050 est certifié Critères Communs EAL 6+ pour le matériel et le système d'exploitation. Prêt à l'emploi pour les appareils IdO, il fournit une base de confiance au niveau du circuit intégré et offre une véritable sécurité de bout en bout, de la périphérie au cloud, sans qu'il soit nécessaire d'implémenter un code de sécurité ni de manipuler des clés et des informations d'identification critiques.

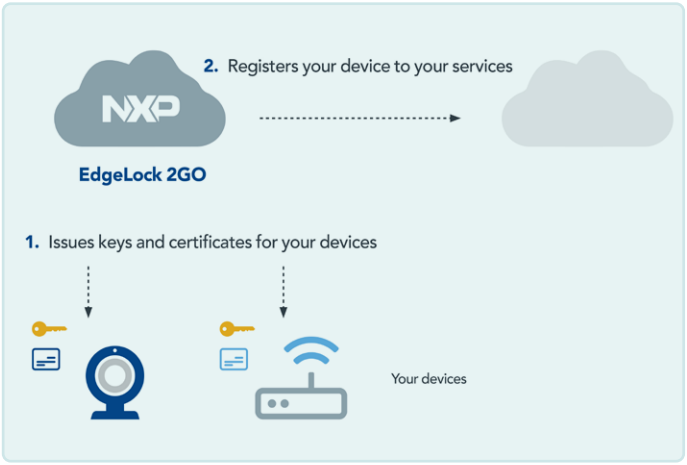


Une base de confiance fondée sur le silicium : élément de sécurité EdgeLock® SE050.

Livré sous la forme d'une solution prête à l'emploi, EdgeLock SE050 offre plusieurs algorithmes et protocoles cryptographiques pré-implémentés et est accompagné d'un paquet de support qui simplifie la conception et réduit le temps de mise sur le marché. En plus des bibliothèques pour différents microcontrôleurs (MCU) et MPU, le paquet de support offre également l'intégration avec les nombreux OS courants, y compris Linux, RTOS et Android.

Les concepteurs de dispositifs IdO sont confrontés à deux défis majeurs lors de la mise en œuvre de l'embarquement des dispositifs sur le cloud. D'abord, le provisionnement de l'identité du dispositif faisant référence à l'installation des clés et des certificats. Le second défi est la gestion des identités des dispositifs une fois libérés sur le terrain, faisant référence à la mise à jour, l'ajout ou la révocation des clés et des certificats tout au long du cycle de vie du dispositif.

Pour aider les concepteurs à relever ces défis, NXP propose le service géré EdgeLock 2GO [4]. La plateforme est une combinaison de matériel et de services spécialement conçue qui établit une base de confiance fondée sur le silicium. EdgeLock 2GO émet les identités requises pour les dispositifs IdO et installe les références en toute sécurité dans le matériel EdgeLock SE050. Il enregistre également automatiquement le dispositif IdO directement auprès du cloud.



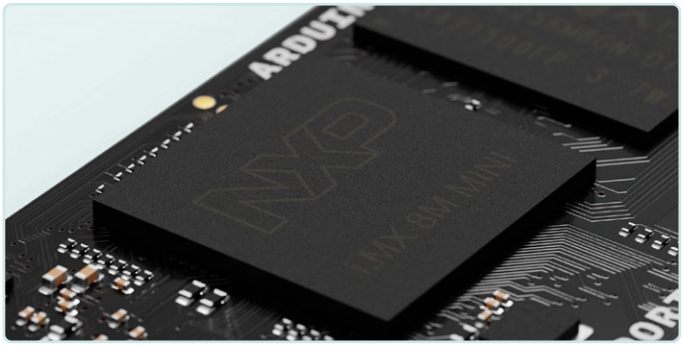
NXP gère les informations d'identification des dispositifs.

TCe service flexible prend en charge plusieurs types de justificatifs d'identité et applique différentes configurations en fonction du projet. Les accréditations peuvent être renouvelées ou ajoutées aux dispositifs mis en service sur le terrain. Avec la mise en place d'EdgeLock SE050 et de l'EdgeLock 2GO, les utilisateurs bénéficient d'une solution de bout en bout qui est simple, sûre et flexible.

L'IdO continue de se développer, mais les risques aussi. La combinaison EdgeLock de NXP, avec sa sécurité matérielle et son service de gestion des informations d'identification, offre aux fabricants de dispositifs un moyen plus sûr de faire des affaires. En prenant en charge le déploiement d'un appareil, NXP EdgeLock réduit les délais de mise sur le marché et les coûts quotidiens d'exploitation d'un déploiement IdO tout en ayant la certitude que les appareils sont protégés par une sécurité de haut niveau.

Libérez la puissance : plus de vitesse et une meilleure efficacité

Le SoC i.MX 8M Mini [5] est le premier processeur d'applications multi-cœur embarqué de NXP construit à l'aide de la technologie de processus 14LPC FinFET avancée, offrant plus de vitesse et une meilleure efficacité énergétique. La famille de processeurs d'applications i.MX 8M Mini associe la haute performance informatique, l'efficacité énergétique et la sécurité embarquée nécessaires à la croissance rapide de l'informatique des nœuds de périphérie, du streaming multimédia et des applications de *machine learning*.



Le SoC i.MX 8M Mini est proposé dans des variantes à un, deux et quatre cœurs utilisant le processeur Arm® Cortex®-A53 et fonctionnant jusqu'à 1,8 GHz par cœur. Livré dans un processus avancé à faible consommation, le complexe de cœurs est optimisé pour un fonctionnement sans ventilateur, un faible coût thermique du système et une longue durée de vie de la batterie. Les cœurs Cortex-A peuvent être mis hors tension tandis que le sous-système Cortex-M4 assure la surveillance du système en temps réel et à faible consommation. Le contrôleur DRAM prend en charge les mémoires 32 bits/16 bits LPDDR4, DDR4 et DDR3L, offrant ainsi une grande souplesse de conception du système.

Les options de cœur du i.MX 8M Mini sont optimisées pour une consommation ultra-faible, voire inférieure à un watt dans certaines applications spécifiques, mais offrent la puissance de traitement nécessaire pour les applications grand public, audio, industrielles, de machine learning et d'inférence sur une gamme de fournisseurs de cloud. Le SoC i.MX 8M Mini intègre également l'accélération matérielle de la vidéo 1080p pour permettre des applications vidéo bidirectionnelles, des graphiques 2D et 3D pour offrir une expérience visuelle IHM riche, et des capacités audio avancées pour permettre des applications riches en sons. Une sélection étendue d'interfaces à haut débit permet une connectivité plus large du système et vise une qualification de niveau industriel.

Les exemples d'application comprennent :

Automatisation industrielle

Le Portenta X8 peut alors faire office de passerelle multiprotocole, en envoyant des données au cloud ou au système ERP via wifi, LoRa, NB/IoT, LTE Cat.M1.

La disponibilité de conteneurs Linux comme ROS au sein de l'environnement Arduino fait du Portenta X8 une solution idéale pour les véhicules guidés autonomes.

Automatisation des bâtiments

Interagissant avec des capteurs intelligents sur le plan environnemental, Portenta X8 permet la mise en œuvre de ML et de traitement d'images en temps réel sur la périphérie.

Les kiosques intelligents s'appuient généralement sur plusieurs composants (par exemple, des lecteurs de cartes, des caméras, des microphones), ce qui nécessite une sélection diversifiée d'E/S. Associé à un Max Carrier, le Portenta X8 assure la connectivité wifi et permet aux administrateurs de surveiller à distance l'utilisation des machines.

Le Portenta X8 peut simultanément contrôler les systèmes CVC, allumer/éteindre les appareils intelligents, régler de manière autonome l'éclairage et contrôler les accès en périphérie.

Commencez à développer dès aujourd'hui avec le SOM Portenta X8 [6] de qualité industrielle, sécurisé et doté d'une densité de calcul exceptionnelle.

220576-04

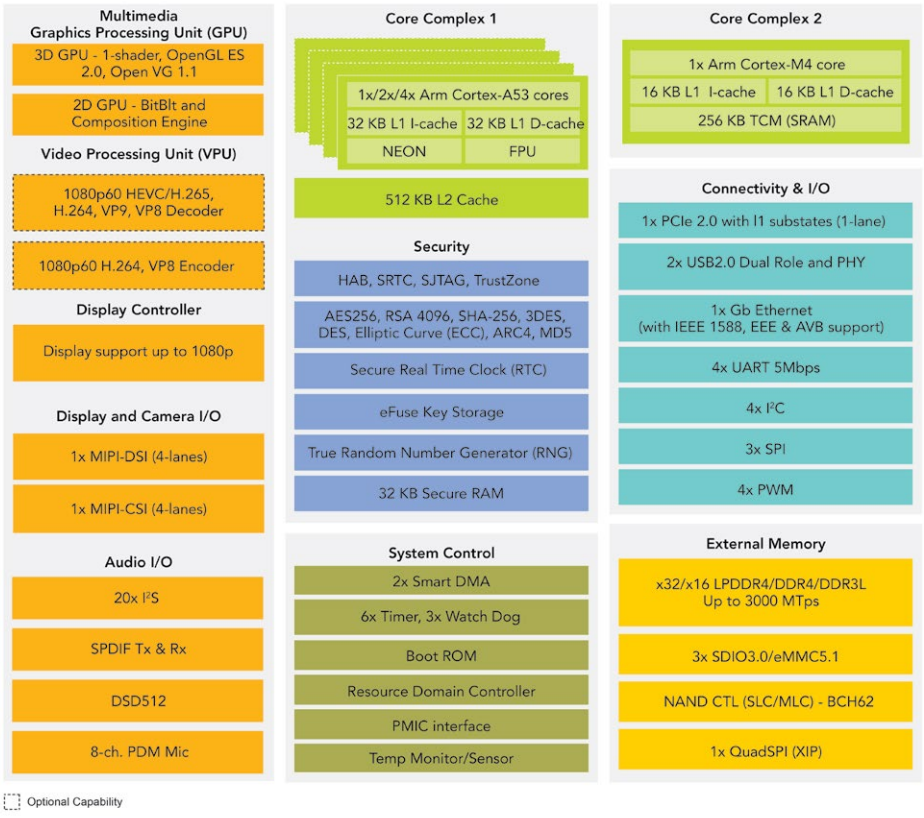


Schéma fonctionnel du processeur d'applications i.MX 8M Mini

LIENS

[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