Bouw, uitrol en onderhoud van schaalbare, veilige applicaties

op basis van Arduino Portenta X8 – met de i.MX 8M Mini Applications Processor en EdgeLock® SE050 Secure Element van NXP

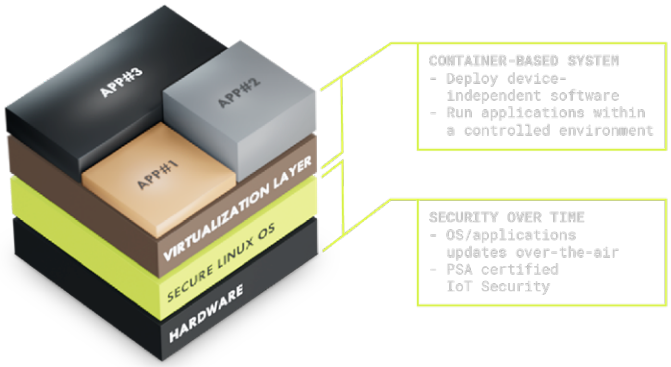
Een bijdrage van NXP Semiconductors

Een IoT-apparaat op de markt brengen vergt aanzienlijke ontwerp- en ontwikkelingsinspanningen – met in elk stadium schaalbaarheids- en beveiligingsproblemen en apparaatbeperkingen. Met de toevoeging van intelligentie wordt het nog ingewikkelder. Dat maakt de selectie van de juiste ontwikkelhardware en -software van cruciaal belang om veilige edge-producten sneller op de markt te brengen. Dit artikel introduceert het Arduino Portenta X8-platform, een industrieel en veilig SOM gebaseerd op de i.MX 8M Mini-applicatieprocessor en een EdgeLock® SE050 hardware secure element van NXP. Dit PSA-gecertificeerde platform is ook Arm® SystemReady IR voor gegarandeerde veiligheid.

Arduino Portenta X8 is een krachtig, industrieel system-on-module met voorgeïnstalleerd Linux OS aan boord en is geschikt om apparaat-onafhankelijke software te draaien dankzij de modulaire containerarchitectuur. Het biedt twee benaderingen: flexibel gebruik van Linux gecombineerd met realtime-toepassingen via de Arduino-omgeving. De ingebouwde WiFi/Bluetooth Low Energy-connectiviteit maakt updates van besturingssystemen/applicaties op afstand mogelijk, waarbij de Linux-kernelomgeving altijd op het hoogste prestatieniveau blijft.

State-of-the-art beveiliging

Het op containers gebaseerde systeem integreert verschillende beveiligingslagen, te beginnen met de hardwarelaag die het Secure Element van NXP huisvest. Het maakt gebruik van het cloudgebaseerde DevOps-platform van Foundries.io [1] waarmee de bouw, test, uitrol en het onderhoud van embedded Linux-oplossingen haast opnieuw is uitgevonden. De Portenta X8 bevat het aanpasbare open-source Linux microPlatform-OS, gebouwd volgens de beste industriële praktijken voor end-to-end beveiliging, incrementele OTA-updates en vlootbeheer.

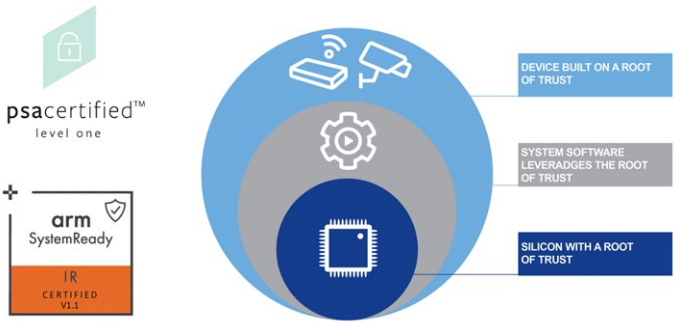


Portenta X8-container en beveiliging.

Met de virtualisatielaag kunnen gebruikers apparaatonafhankelijke software implementeren die binnen een gecontroleerde omgeving draait. Ze kunnen hun eigen containers maken met behulp van Docker en vooraf gemaakte images downloaden van Docker Hub of andere beschikbare openbare locaties om een op maat gemaakte toepassing te bouwen. Als de ontwikkelaar de embedded wereld wil betreden, kan hij dat gemakkelijk doen door zijn toepassing te bouwen, binnen een container te draaien, naar het board te laden en uit te proberen. Dit biedt een breed scala aan mogelijkheden door de capaciteiten van Linux te mixen met de Arduino-standaardervaring.

Portenta X8 behaalde PSA-certificering; het NXP EdgeLock SE050 hardware secure element zorgt voor het genereren van sleutels, versnelde cryptobewerkingen en veilige opslag. X8 behaalde ook Arm SystemReady [2] certificering en geïntegreerde Parsec-services, waardoor het een van de eerste Cassini-producten of Cloud Native Edge-apparaten is die voor ontwikkelaars op de markt zijn. Het draait naadloos Fedora IoT, Fedora Server, Debian en Linux microPlatform. De Portenta X8, die de migratie van cloud-native workloads van de

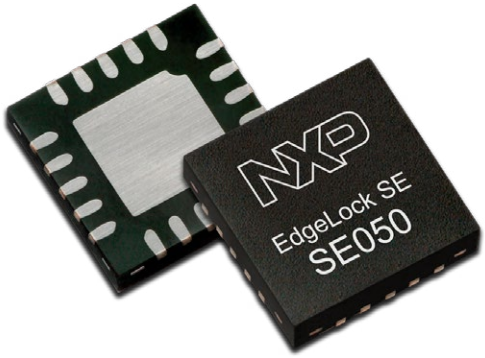
cloud naar de edge mogelijk maakt, draagt bij aan een cloud-native ontwikkelervaring in het diverse en veilige IoT-ecosysteem van Arm.



Platform-beveiligingsarchitectuur.

EdgeLock SE050 – een veilig anker voor IoT

De EdgeLock SE050 [3] van NXP is discrete en manipulatiebestendige beveiligingshardware voor de bescherming van de identiteit van een apparaat, inclusief cryptografische sleutels en certificaten. Het is een standalone embedded secure element dat via de I²C-interface aan de hoofdprocessor wordt gekoppeld. De EdgeLock SE050 is Common Criteria EAL 6+ gecertificeerd voor de hardware en het besturingssysteem. Dit kant-en-klare beveiligde element voor IoT-apparaten biedt een vertrouwensbasis op IC-niveau en levert echte end-to-end beveiliging – van edge tot cloud – zonder de noodzaak om beveiligingscode te implementeren of kritieke sleutels en referenties te verwerken.

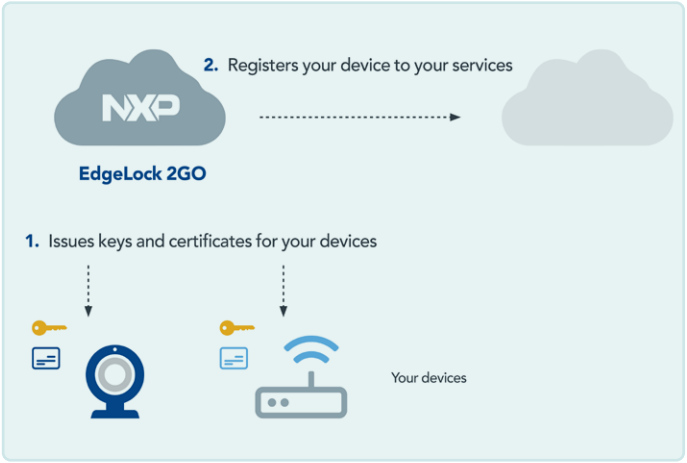


Root of Trust op silicium: het EdgeLock SE050 Secure Element.

EdgeLock SE050 wordt geleverd als een kant-en-klare oplossing met meerdere vooraf geïmplementeerde cryptografische algoritmen en protocollen en een compleet product-ondersteuningspakket dat het ontwerp vereenvoudigt en de time-to-market verkort. Naast bibliotheken voor verschillende MCU's en MPU's biedt het ondersteuningspakket ook integratie met de vele gangbare besturingssystemen, waaronder Linux, RTOS en Android.

Ontwerpers van IoT-apparaten worden geconfronteerd met twee grote uitdagingen bij de implementatie van onboarding naar de cloud: de provisionering van de apparaatidentiteit en het beheer daarvan zodra deze is vrijgegeven voor het veld. De provisionering van het apparaat verwijst naar de installatie van sleutels en certificaten. Het beheren van apparaatidentiteiten heeft betrekking op het bijwerken, toevoegen of intrekken van sleutels en certificaten gedurende de gehele levenscyclus van het apparaat.

Om ontwerpers te helpen deze uitdagingen op te lossen, biedt NXP de EdgeLock 2GO [4] managed service. Het platform is een speciaal gebouwde hardware- en servicecombinatie die een op silicium gebaseerde vertrouwensbasis creëert. EdgeLock 2GO verstrekt de voor IoT-apparaten de vereiste identiteiten en installeert de 'credentials' veilig in de EdgeLock SE050-hardware. Ook wordt het IoT-apparaat automatisch rechtstreeks bij de cloudservice geregistreerd.



NXP beheert de device credentials.

Deze flexibele service ondersteunt meerdere soorten referenties en past verschillende configuraties toe, afhankelijk van het project. Credentials kunnen worden vernieuwd of toegevoegd aan apparaten die in het veld worden vrijgegeven. Met de ingebruikname van EdgeLock SE050 en EdgeLock 2GO krijgen gebruikers een end-to-end oplossing die eenvoudig, veilig en flexibel is.

Naarmate IoT blijft groeien, nemen ook de risico's toe. De EdgeLock-combinatie van NXP, met zijn op hardware gebaseerde beveiliging en service voor credential management, geeft fabrikanten van apparaten een veiligere manier om zaken te doen. Als NXP EdgeLock de implementatie van een apparaat ondersteunt, verkort het de time-to-market en verlaagt het de dagelijkse kosten van een IoT-implementatie, terwijl men erop kan vertrouwen dat apparaten worden beschermd door high-level beveiliging.

Ontketend: meer snelheid en efficiëntie

De i.MX 8M Mini [5] SoC is NXP's eerste embedded multicore applicatieprocessor, gebouwd met behulp van geavanceerde 14LPC FinFET-procestechnologie, die meer snelheid en een verbeterde energie-efficiëntie biedt. De i.MX 8M Mini-familie van applicatieprocessoren combineert high-performance computing, efficiëntie en embedded beveiliging – nodig voor snelgroeiende edge node computing-applicaties, streaming multimedia en machine learning-toepassingen.

De i.MX 8M Mini SoC wordt aangeboden in varianten met één, twee en vier kernen met Arm Cortex-A53 op maximaal 1,8 GHz per kern. Dankzij een geavanceerd low-power proces is het core complex geoptimaliseerd voor gebruik zonder ventilator, geringe thermische systeemkosten en een lange batterij-levensduur. De Cortex-A kernen kunnen worden uitgeschakeld terwijl het Cortex-M4 subsysteem energiezuinige, realtime systeembewaking uitvoert. De DRAM-controller ondersteunt 32-bit/16-bit LPDDR4-, DDR4- en DDR3L-geheugen, wat een grote flexibiliteit in het systeemontwerp garandeert.
De i.MX 8M Mini core-opties zijn geoptimaliseerd voor ultra-low-power, zelfs sub-watt in specifieke toepassingen, maar bieden de ruime verwerkingskracht die nodig is voor consumenten-, audio-, industriële, machine learning training- en inferencing-toepassingen in een reeks van cloud providers. De i.MX 8M Mini SoC bevat ook hardwarematige 1080p video-versnelling om tweeweg videotoepassingen mogelijk te maken, 2D en 3D graphics om een rijke visuele HMI-ervaring te bieden, en geavanceerde audiomogelijkheden. Een uitgebreide selectie van high-speed interfaces maakt brede systeemconnectiviteit mogelijk en is gericht op kwalificatie op industrieel niveau.

Toepassingsvoorbeelden omvatten:

Industriële automatisering

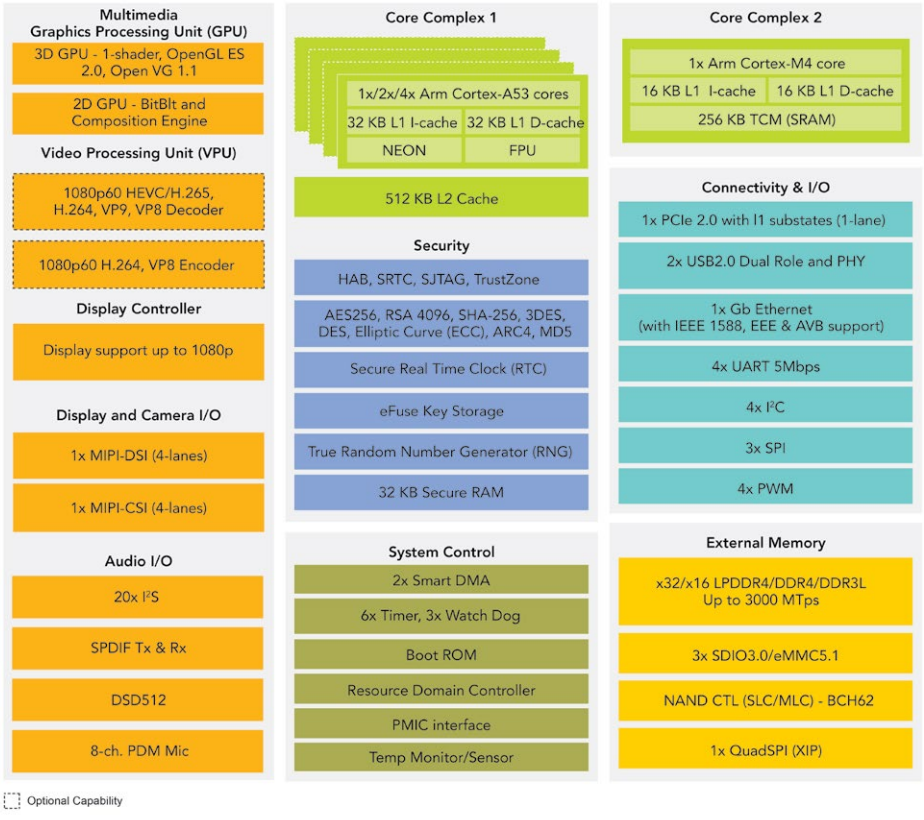
- De Portenta X8 kan hier fungeren als een multi-protocol gateway, waarbij gegevens via WiFi, LoRa, NB/IoT, LTE Cat.M1 naar de Cloud of het ERP-systeem worden gestuurd.
- De beschikbaarheid van Linux-containers zoals ROS binnen de Arduino-omgeving maakt de Portenta X8 zeer geschikt voor autonoom geleide voertuigen.

Gebouwautomatisering

- De Portenta X8 werkt samen met slimme omgevingssensoren en maakt de implementatie van real-time ML en edge-beeldverwerking mogelijk.
- Slimme kiosken maken meestal gebruik van verschillende componenten (zoals kaartlezers, camera's, microfoons), wat diverse soorten I/O's vereist. In combinatie met een Max Carrier zorgt de Portenta X8 voor WiFi-connectiviteit en kunnen beheerders het machinegebruik op afstand controleren.
- De Portenta X8 kan tegelijkertijd HVAC-systemen bedienen, slimme apparaten in- en uitschakelen, verlichting autonoom aanpassen en edge-toegang regelen.

Ga vandaag nog aan de slag met de industriële, veilige Portenta X8 SOM [6] voor uitgelezen rekenkracht op een klein oppervlak.

220576-03



i.MX 8M Mini Applications Processor: blokschema

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] Portenta X8 SOM: www.arduino.cc/pro/hardware/product/portenta