

# IOT CYBERSECURITY FROM EDGE-TO-CLOUD: BUILD HIGHLY SECURED CONNECTED DEVICES WITH NXP AND MICROSOFT AZURE SPHERE

Sudhanva Huruli, Program Manager, Microsoft  
Naama Bak, Global Business Development, NXP  
**MARCH 2021**



SECURE CONNECTIONS  
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.  
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.





## AGENDA

- Summary of the recent announcement
- Cybersecurity for IoT
- Properties of highly secured devices
- How does i.MX 8ULP-CS processor work with Azure Sphere
- Use cases for the i.MX 8ULP-CS & i.MX 9 processors



# NXP INTRODUCES ITS FIRST CLOUD-SECURED, MICROSOFT AZURE SPHERE-CERTIFIED PROCESSOR FAMILY

The infographic for the i.MX 8ULP processor features a central chip image surrounded by ten feature boxes:

- EDGELOCK™ SECURE ENCLAVE**: Cloud security.
- ADVANCED DSP AUDIO & ML**: Cadence® Tensilica® HiFi4® DSP.
- <800µW ALWAYS LISTENING**: Cadence® Tensilica® Fusion DSP.
- RICH 3D & 2D GRAPHICS**: 3D cube icon.
- ENERGY FLEX ARCHITECTURE WITH HETEROGENEOUS DOMAIN COMPUTING**: Chip icon.
- i.MX 8ULP**: Central chip image.
- µPower**: Power Management with ADAPTIVE DVFS.
- CUSTOM POWER MODES**: Bar chart icon.
- 2.5x DMIPS\***: Speed icon.
- VIVID DISPLAY ADVANCED COLOR E-PAPER**: Watch and phone icons.
- 75% MORE POWER EFFICIENT\***: Leaf icon.

\*Compared to predecessor

**NXP**

**First cloud-secured crossover applications processor, the i.MX 8ULP-CS with Azure Sphere**

## Plans to build additional Azure Sphere-certified processors as part of the NXP i.MX 9 series

The infographic for the i.MX 9 Applications Processor Series features a central chip image surrounded by eight feature boxes:

- EDGELOCK™ SECURE ENCLAVE**: Cloud security.
- MULTI-SENSORY EXPERIENCES**: Streaming Media, Rich 2D & 3D Graphics, Advanced Audio, Voice Processing, Touch Sensing, Vision.
- ENERGY FLEX ARCHITECTURE WITH HETEROGENEOUS DOMAIN COMPUTING**: Chip icon.
- i.MX 9 APPLICATIONS PROCESSOR SERIES**: Central chip image.
- INHERENTLY INTELLIGENT INTEGRATED ML ACCELERATORS**: Neural network icon.
- BUILT-IN MCU! REAL TIME RESPONSE FOR THE REAL WORLD ALWAYS-ON, LOW POWER SENSING**: Lightning bolt and chip icons.
- SCALABLE COMPUTE**: High performance - from single to many core configurations. Bar chart icon.
- ESSENTIAL CONNECTIVITY**: Globe icon.

\*Compared to predecessor

**NXP**

# Importance of Cybersecurity in IoT

---



SECURE CONNECTIONS  
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.  
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.





# **What happens when you connect a device to the internet?**

**“The internet is this cauldron of evil.”**

Dr. James Mickens, Harvard University

# CYBERATTACKS PUT BUSINESSES AT RISK



Devices bricked or held for ransom



Devices are used for malicious purposes



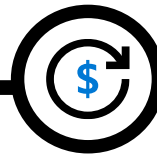
Data & IP theft



Data polluted & compromised



Devices used to attack networks



## The cost of IoT attacks

Stolen IP & other highly valuable data

Compromised regulatory status or certifications

Brand impact (loss of trust)

Recovery costs

Financial and legal responsibility

Downtime

Security forensics



## MIRAI BOTNET ATTACK

- Everyday devices are used to launch an attack that takes down the internet for a day
- 100k devices
- Exploited a well-known weakness
- No early detection, no remote update



# EXPECTATIONS ARE INCREASING WITH AWARENESS

## Consumers

65% of consumers wouldn't purchase a smart device from a brand that has experienced a security breach.

74% of consumers would pay more for a smart device that had additional security.

93% of consumers believe that manufacturers need to do more to secure smart devices.

*According to Greenberg research 2019*

## Enterprise Customers

97% of enterprises call out security as a concern when adopting IoT.<sup>1</sup>

Enterprise customers would purchase 70% more devices if security concerns were mitigated.<sup>2</sup>

Enterprise customers are willing to pay 22% more for IoT cybersecurity.<sup>2</sup>

<sup>1</sup> IoT Signals 2020

<sup>2</sup> Bain & Co. 2018

## Government Action

In the USA, several bills have been introduced in Congress, with two passed in California ([SB-327](#)) and Oregon ([HB2395](#)).

In Europe, upcoming EU Cybersecurity Act with three security assurance levels will become basis for regulation—*basic, substantial, high*.

ETSI EN 303 645, with 13 security requirements, with increasing adoption globally (e.g. Singapore, Finland, UK).



## WHAT WE HEAR FROM CUSTOMERS ABOUT THE CHALLENGES OF SECURING IOT



### Manufacturing

While in the factory or in the supply chain, ICs and devices are subject to malware injection, counterfeiting, key capture, overproduction, and the creation of security backdoors.



### Operations

Once in the field, ICs and devices are susceptible to a wide range of logical attacks and physical attacks, including malware injection, theft of unencrypted data, and malicious software updates, as well as reverse engineering.



### Maintenance

While this capability is key to maintaining device security, the upgrade process must be totally secure to prevent loading of malware/unauthorized SW.

# THE 7 PROPERTIES OF HIGHLY SECURED DEVICES



## Hardware Root of Trust

*Is your device's identity and software integrity secured by hardware?*



## Defense in Depth

*Does your device remain protected even if some security mechanism is defeated?*



## Small Trusted Computing Base

*Is your device's security-enforcement code protected from bugs in application code?*



## Dynamic Compartments

*Can your device's security improve after deployment?*



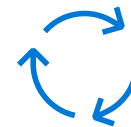
## Certificate-Based Authentication

*Does your device authenticate itself with certificates?*



## Error Reporting

*Does your device report back errors to give you in-field awareness?*



## Renewable Security

*Does your device software update automatically?*

# AZURE SPHERE

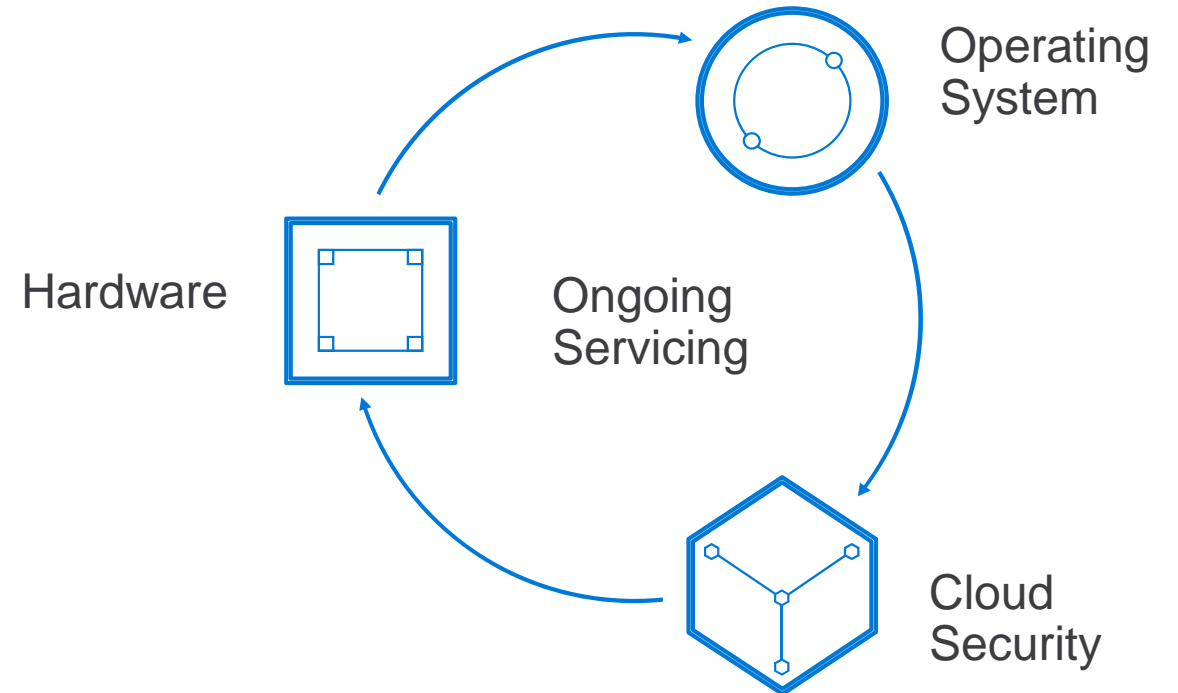
An end-to-end solution for securely connecting existing equipment and to create new IoT devices with built-in security.

**Integrated hardware, software, and cloud services** work seamlessly together and deliver active security by default.

**Ongoing security and OS updates** from Microsoft keep your devices secured over time.

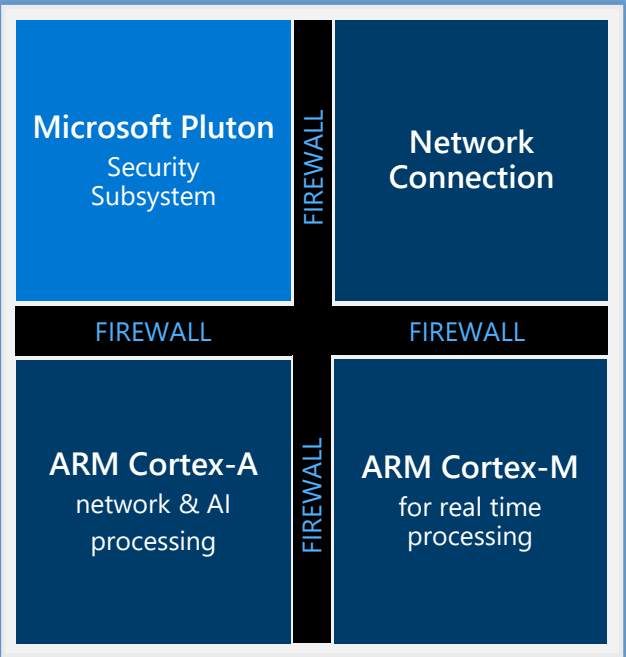
**Defense in depth** provides multiple layers of protection to help guard devices against and respond to threats.

**Implementation options** allow you to secure existing equipment and build security into new IoT devices.

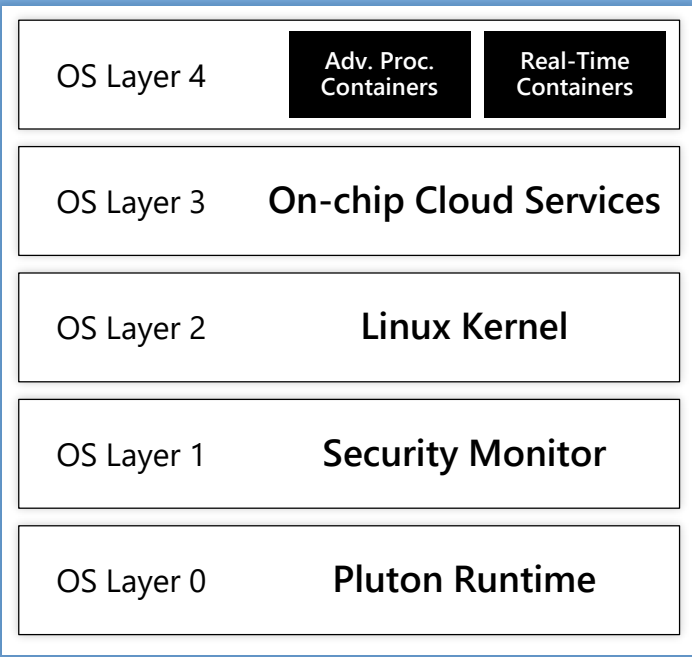




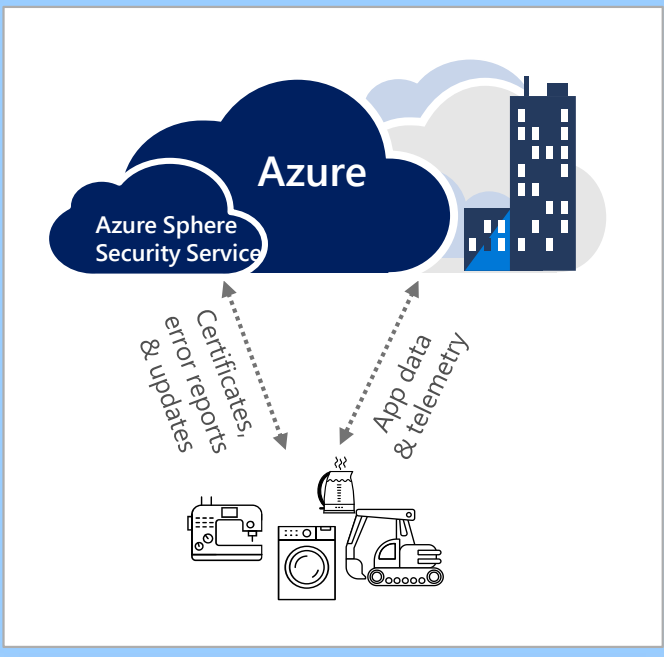
## Azure Sphere certified chips



## The Azure Sphere Operating System



## The Azure Sphere Security Service



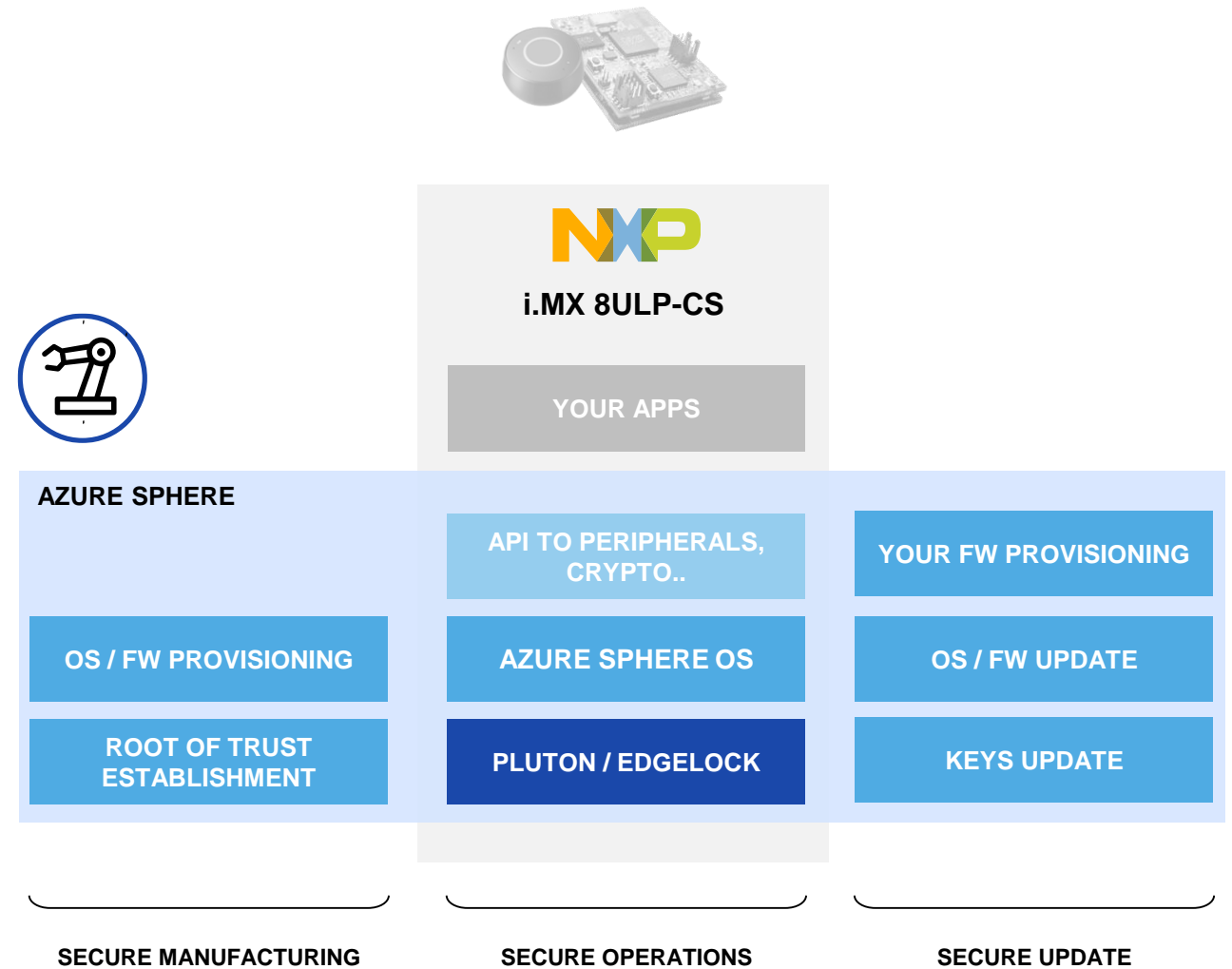
# AZURE SPHERE & NXP i.MX 8ULP-CS OVERVIEW

## Hardware

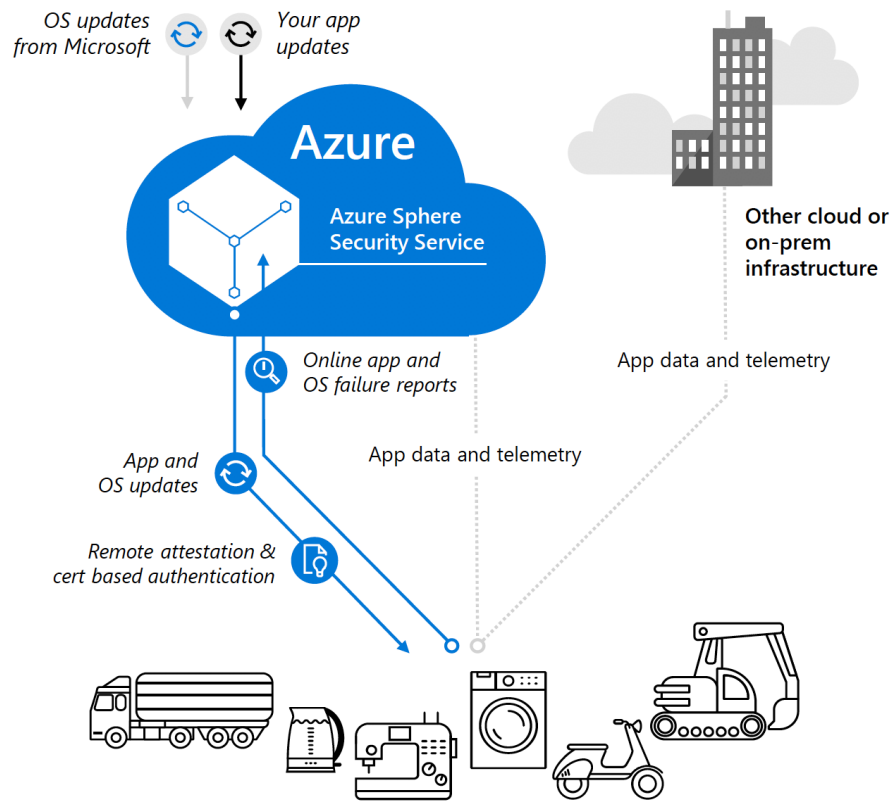
- i.MX 8ULP-CS processor
- Microsoft Pluton Enabled EdgeLock™ Secure Enclave
- Root of Trust established at NXP

## Operating System

- Managed OS for users
- Built off existing technology
- Secure boot ROM code based; Keys fused at NXP



## MANAGED SECURITY SERVICE TO PROVIDE UPDATES

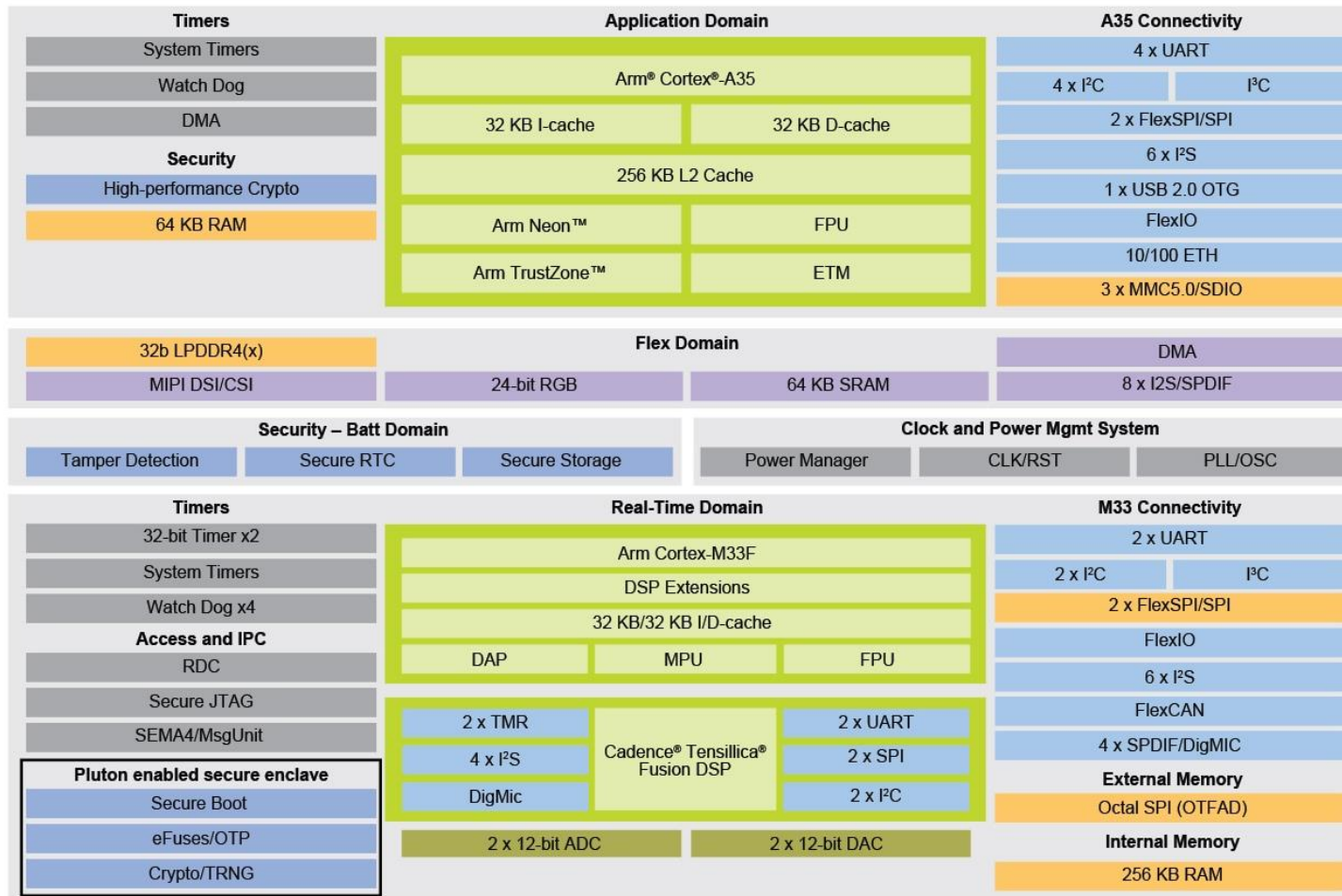


- Fully managed OTA service by Microsoft for OS components updates and on demand user application update
- Users use Microsoft frontend to interact with device
- Azure Sphere Service is agnostic to your cloud provider
- Microsoft provides constant updates for the lifetime of the chip



# OVERVIEW ON i.MX 8ULP APPLICATION PROCESSOR

i.MX 8ULP-CS Cloud Secured



## SPECIFICATIONS:

### CPU

Arm Cortex-A35 @ 1.0 GHz  
Arm Cortex-M33 @ 240Mhz  
Fusion DSP @200MHz

### Connectivity

10/100 ETH  
CAN Bus

### Packaging

9.4x9.4mm<sup>2</sup>, 15x15mm<sup>2</sup>

### External Memory

SPI-NAND  
LPDDR4  
SPI NOR

### Temp Range

-40°C to 105°C

# Use Cases for i.MX 8ULP-CS

---



SECURE CONNECTIONS  
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.  
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



# i.MX 8ULP-CS & i.MX 9 USE CASES



## Cloud connected Gateways

Wireless Base Stations  
Switches  
Home Hub



## Home Control & Security

Smart Appliances  
Thermostats



## Manufacturing Automation

Temperature Monitoring  
Machine Diagnosis & Control  
Remote Asset Control  
Fleet Tracking



## Energy Consumption & Monitoring

PV Inverters  
EV Charging Station



## Connected Printers

Barcode Scanner



## Wearables

Smart Watch  
Activity Tracking  
Smart Glass



## Building Control System

Smart Parking  
Smart Lighting



## eReaders



## EBS SOM Modules



# Contact Us!

If you are interested to share insights and discuss how Azure Sphere and i.MX 8ULP-CS could shape your next generation IoT products.

[naama.bak@nxp.com](mailto:naama.bak@nxp.com)

[suhuruli@microsoft.com](mailto:suhuruli@microsoft.com)



SECURE CONNECTIONS  
FOR A SMARTER WORLD