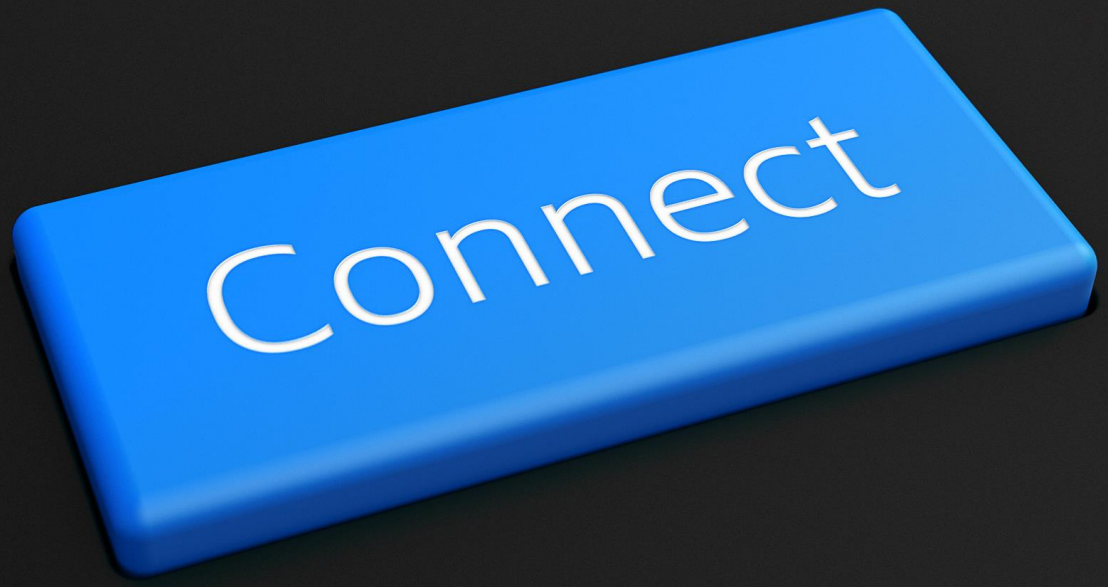
IoT Accelerator Cloud Connect

Introduction



Cloud Connect

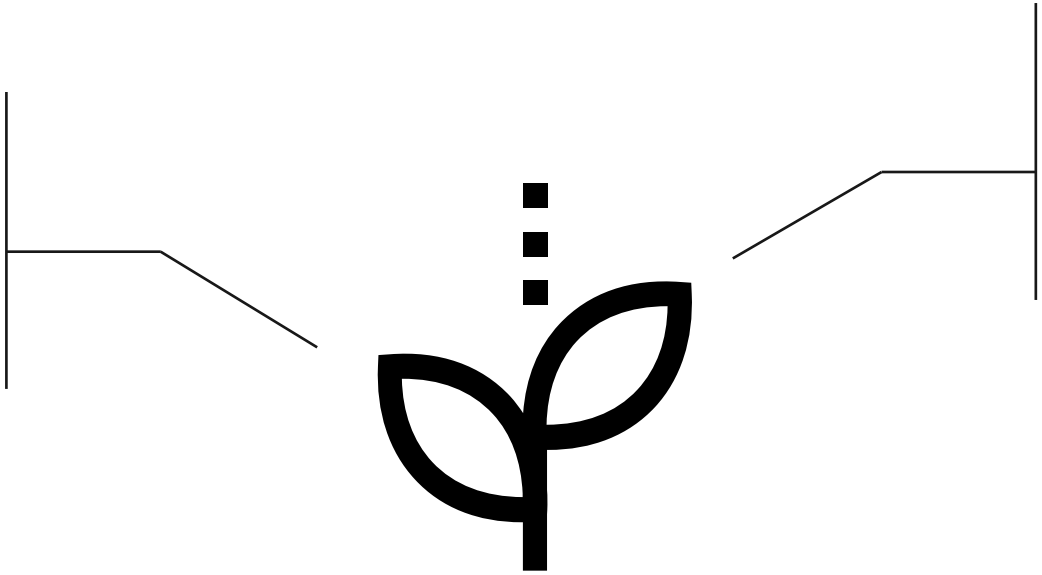
Solving a Hyperscale Cloud Provider business challenge

Connecting low powered cellular devices to their data platforms

What's special about low-powered IoT devices?

Limited battery

- Meant to last on the field for years
- CPU usage is critical
- Must talk as little as possible
- Must communicate very efficiently

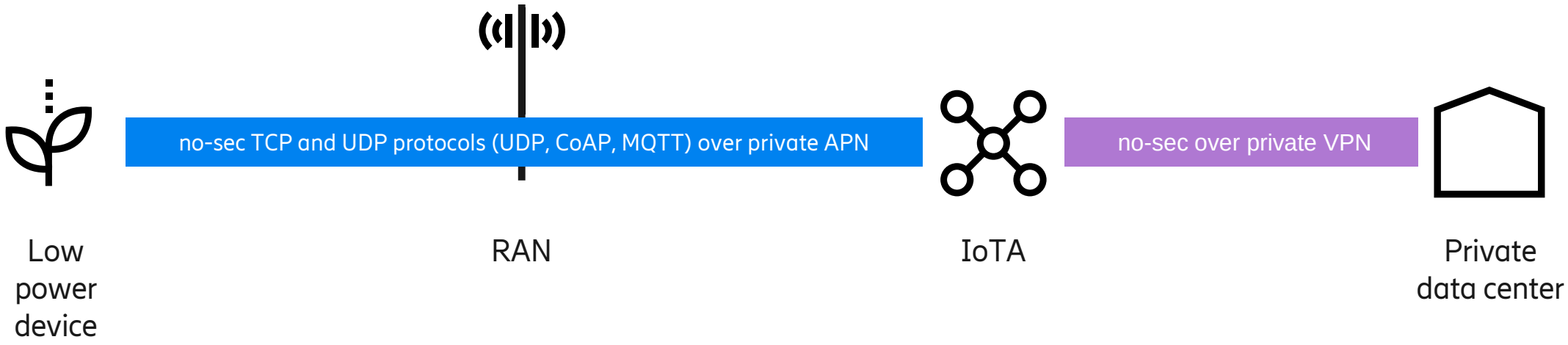


Limited capability

- Smaller processors and memory
- Designed for low powered UDP networks
- Optimized for small firmware protocol stacks

Traditional setup for low-powered devices

Unencrypted routing over private APNs and VPNs into private data centers. No extra security needed.



Hyperscale Cloud Providers (HCP)

- Microsoft and Amazon dominate the data analytics and management market

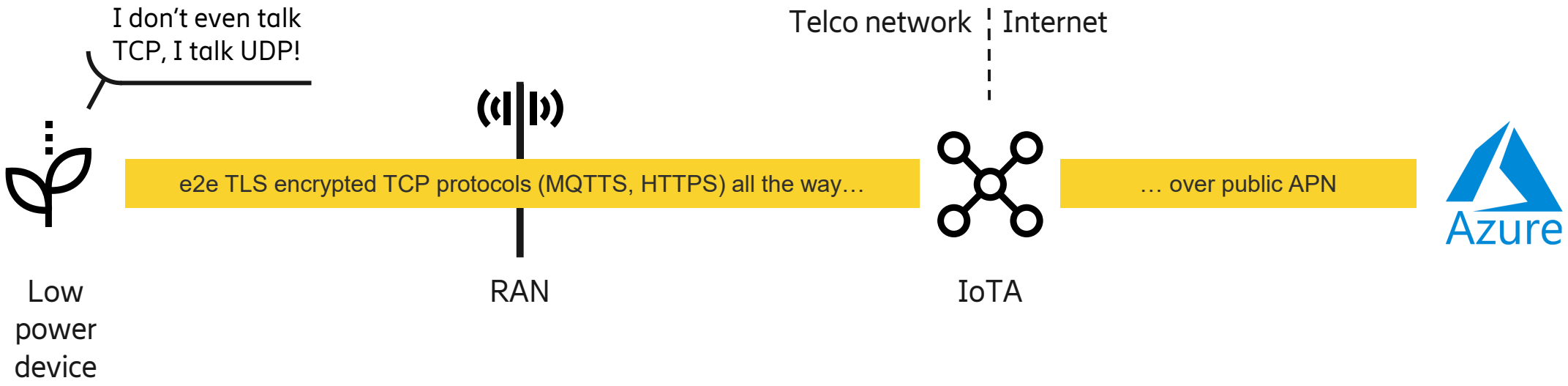
- The “go-to” endpoints for connecting devices are
  - Azure IoT Hub
  - Azure IoT Central

Hyperscale Cloud Providers (HCP)

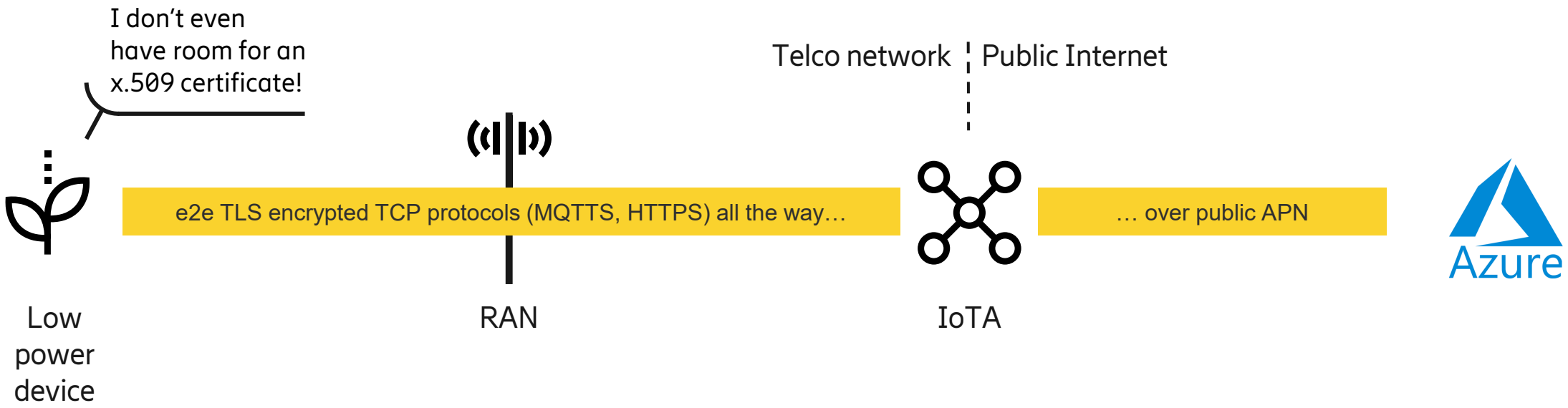
- HCPs need to trust IoT devices
- HCPs require end-to-end encryption with a limited range of TCP protocols
- While this is OK for sophisticated IoT devices (e.g., vehicles and gateways) it is not workable for low powered devices
- Especially, this is problematic for devices who only use UDP based protocols

Connecting to HCP → The challenge

HCP requires e2e encryption and the use of TCP protocols



Connecting to HCP → The challenge

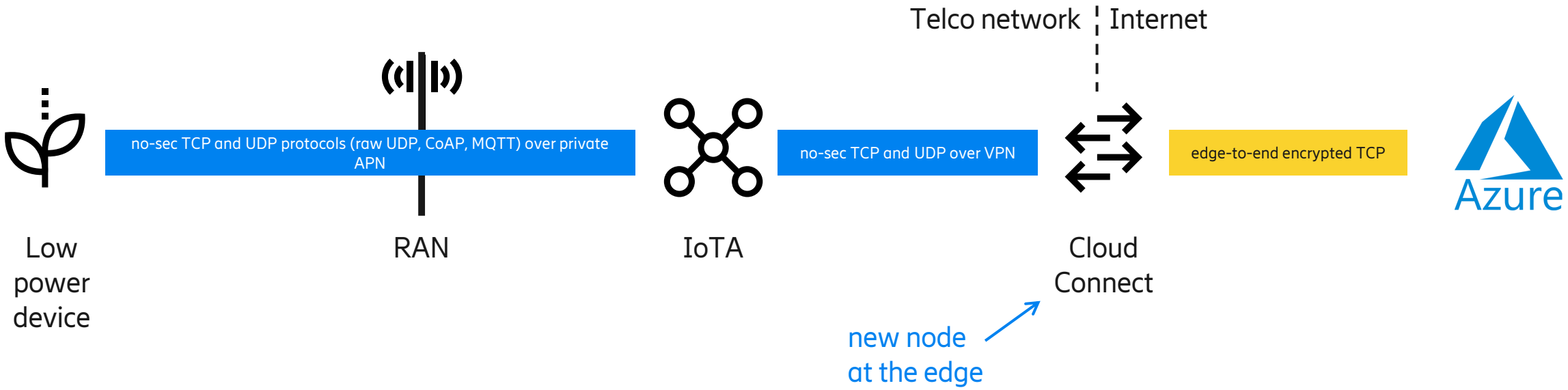


Problems

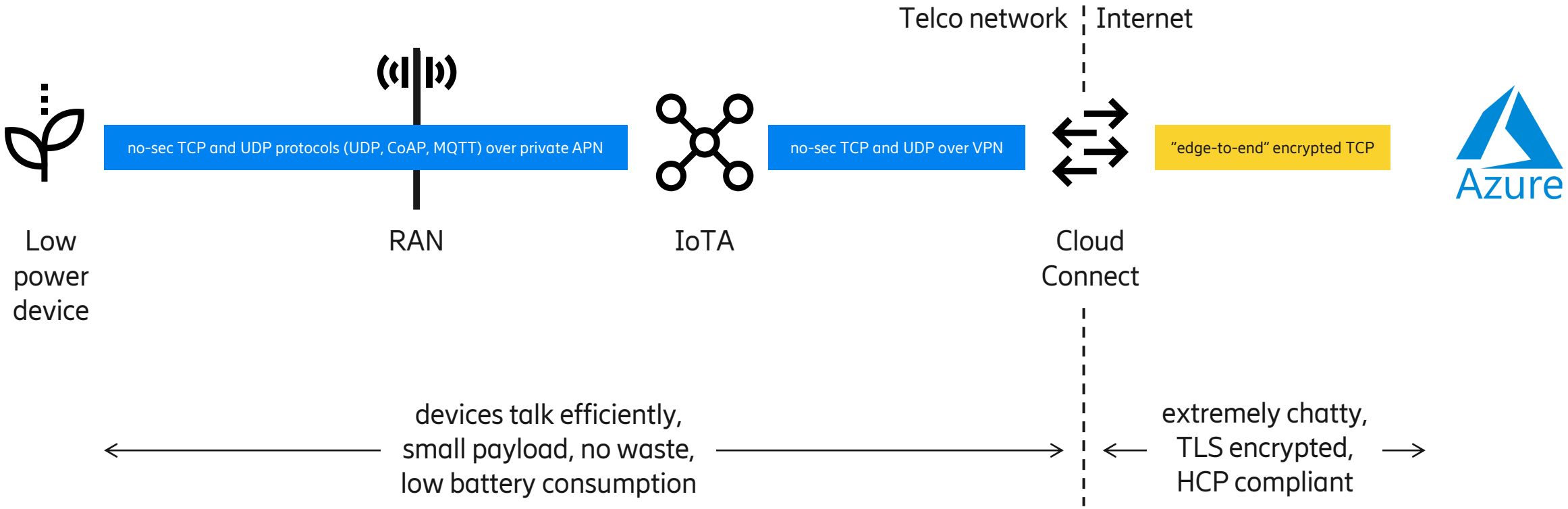
- The CA certificate needs to be installed on each device
- More configuration setup for each device
- The device now talks a lot more! Example: from 50 bytes to 10 Kbytes
- Consumption is much higher → Battery suffers greatly → Autonomy
- Some devices cannot even talk TCP protocols!

Cloud Connect solution

Shifting compliance from
“end-to-end” to “edge-to-end”

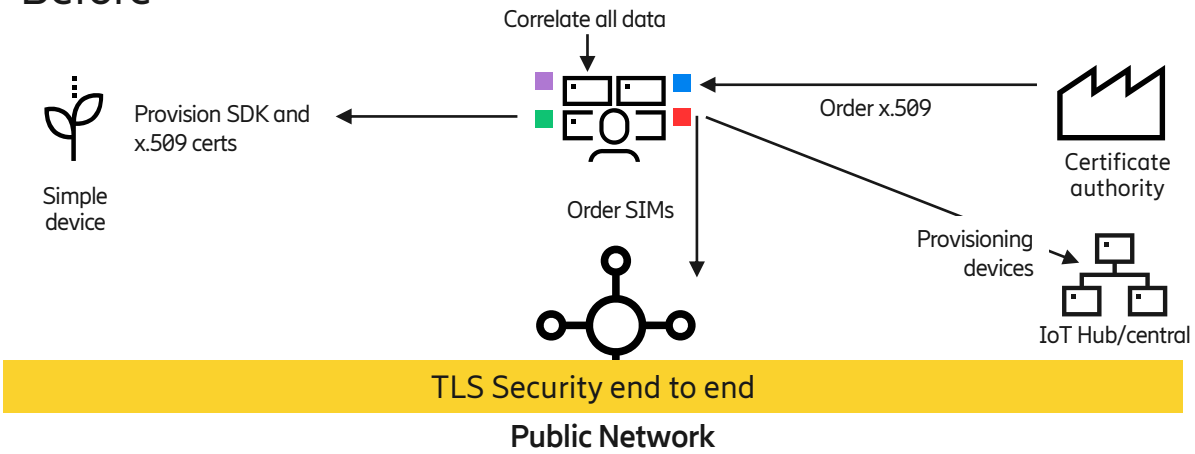


Cloud Connect solution

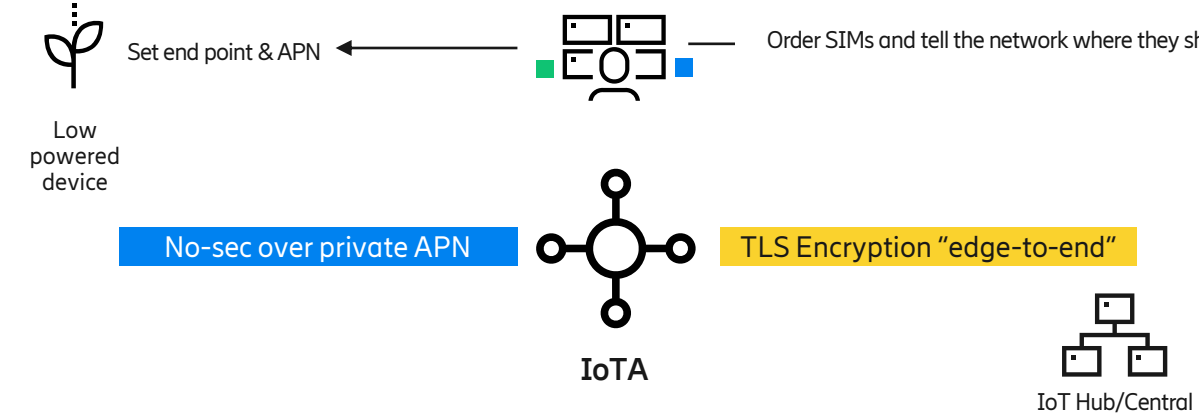


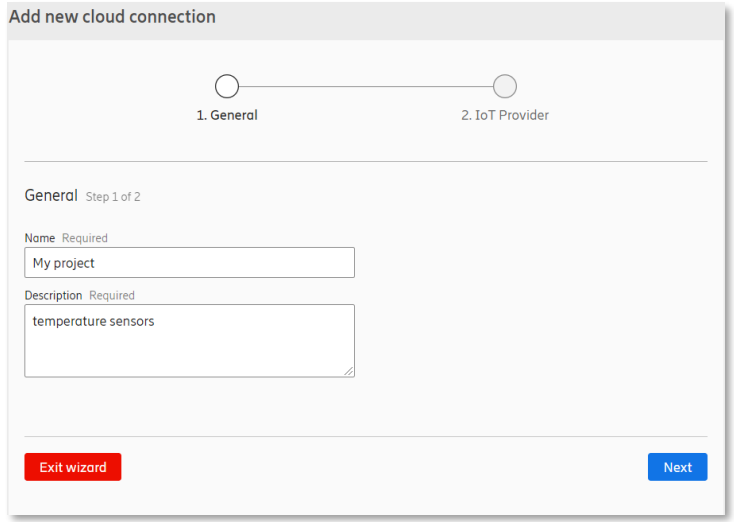
Before and after Cloud Connect

Before



With Cloud Connect





Connection steps – Comparison

Without Cloud Connect

- ✕ Only TCP ready devices
- ✕ Enough battery and CPU to run TLS e2e

1. Each device must have the SDK for Azure
2. CA certificate is needed on each device
3. Configuration is not trivial
4. A person must build a spreadsheet or database to document which device has which name and which certificate
5. Upload spreadsheet or database info into HCP
6. Turn device on → Connected to HCP

With Cloud Connect

- ✓ UDP/TCP ready devices
- ✓ Low-powered devices friendly

1. Set APN and Cloud Connect endpoint name
2. Grant permissions to Cloud Connect to provision all devices in the HCP (by running a simple script)
3. Turn device on → Connected to HCP

“edge-to-end” encryption benefits

Simplicity

- Security and complexity moved from device network’s edge
- No encryption or certificate management on the device

Interoperability

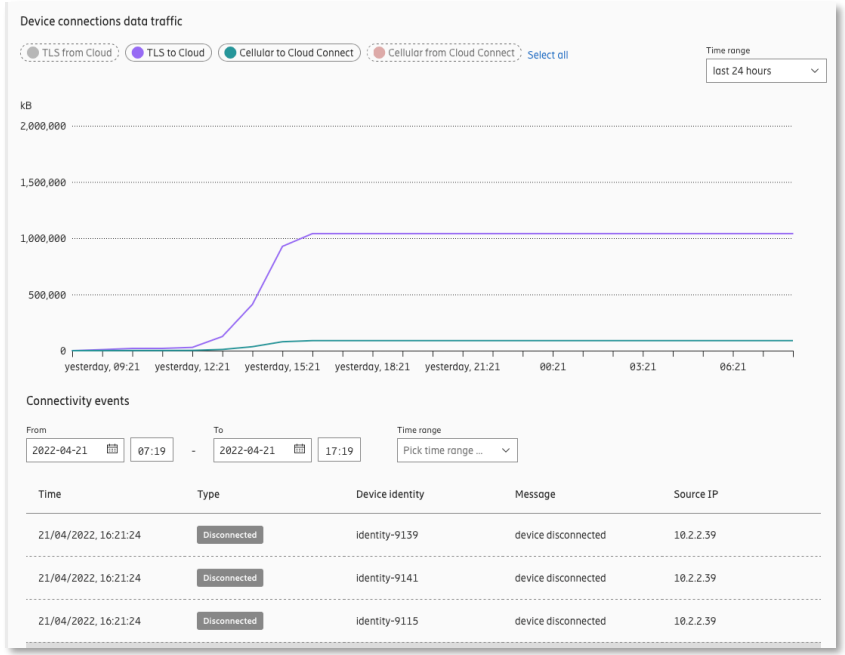
- Low-power cellular devices can now talk securely via simple UDP protocols with public cloud IoT endpoints
- This is done without added complexity, no middleware platform required

Better customer experience

- Seamless automated provisioning
- Faster setup
- Not limited to TCP protocols

Better performance

- Up to 50% less power consumption
- Up to 95% less data consumption
- Lower device memory and CPU reqs
- Lower battery requirements



Microsoft Azure Integration Use Cases

TCP Devices

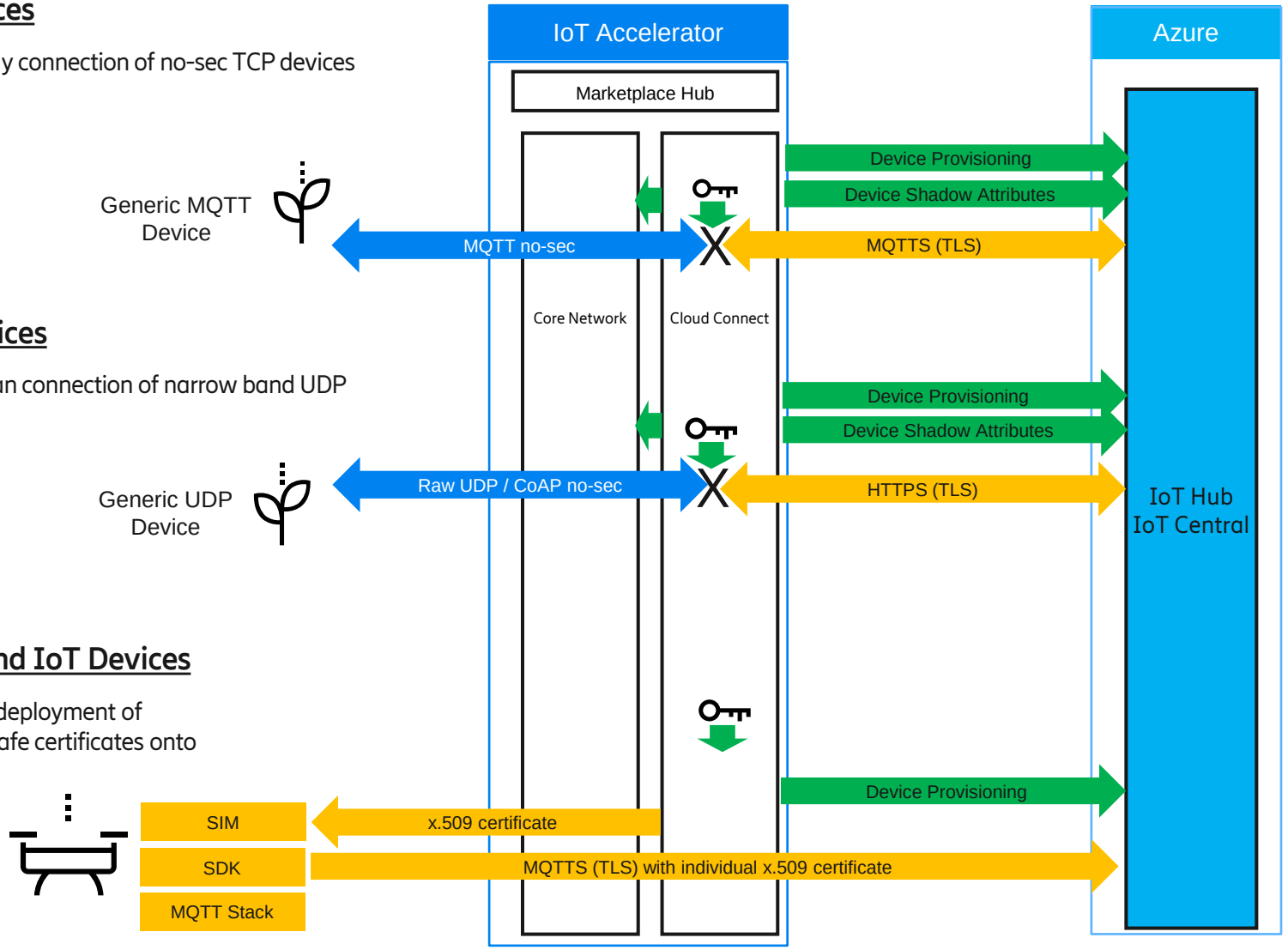
Plug and Play connection of no-sec TCP devices

UDP Devices

Plug and Plan connection of narrow band UDP devices

Broadband IoT Devices

Automated deployment of GSMA IoT Safe certificates onto devices



Customer Value:

— Connect devices without TLS or certificate management into Azure IoT Hub and IoT Central

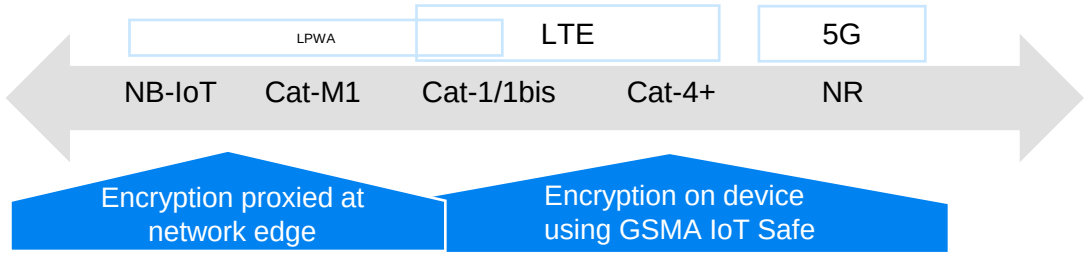
Customer Value:

— Support devices that are not compatible with Azure IoT Hub and IoT Central by simply plugging in a SIM

Customer Value:

— Dramatically simplify the rollout of high-volume devices that will directly connect with IoT Hub by letting IoTA manage certificate deployment and provisioning to the SIM secure store

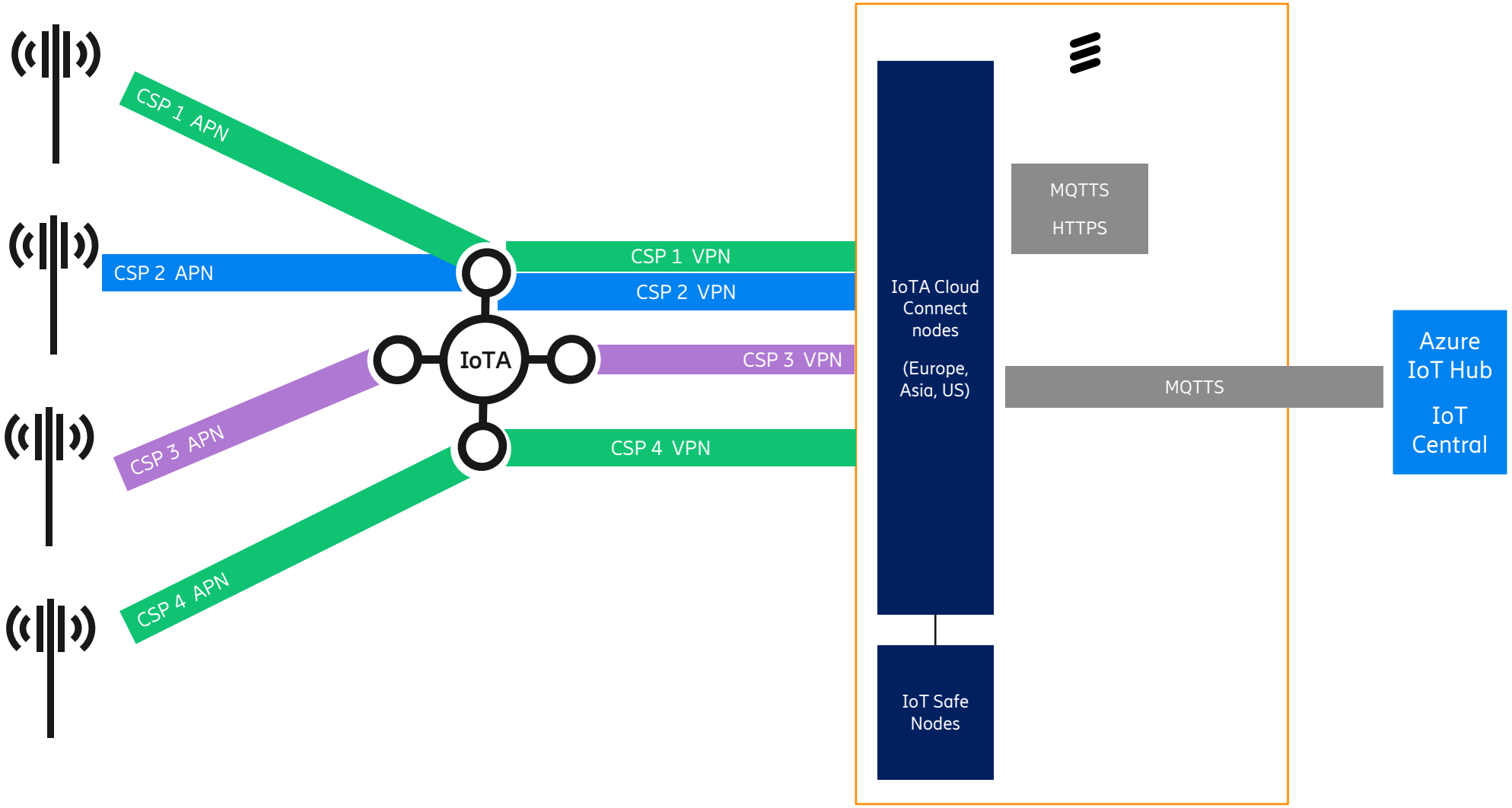
Target Segments and Technologies



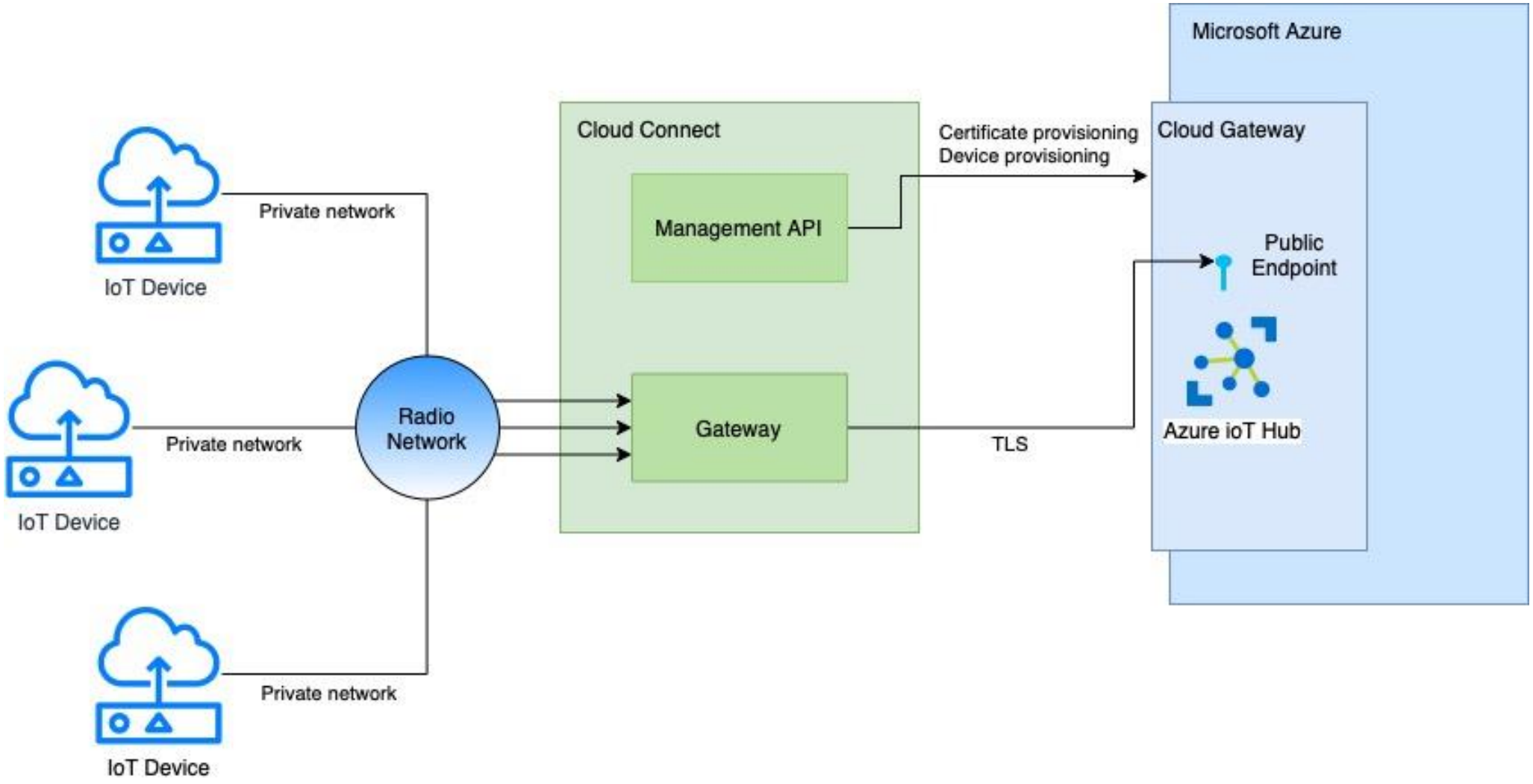
- Edge to End encryption
  - CAT M1/NBIoT devices where TLS /DTLS from device is problematic
- IoT SAFE encryption
  - Any device requiring X.509 root of trust certificate on the device

- Edge to End encryption:
  - Asset tracking and monitoring
  - Environmental monitoring
  - Gas and water metering
- IoT SAFE encryption
  - Industrial IoT
  - Micro-mobility and EV Charging
  - Security
  - Real estate and Smart Cities

Azure Architecture



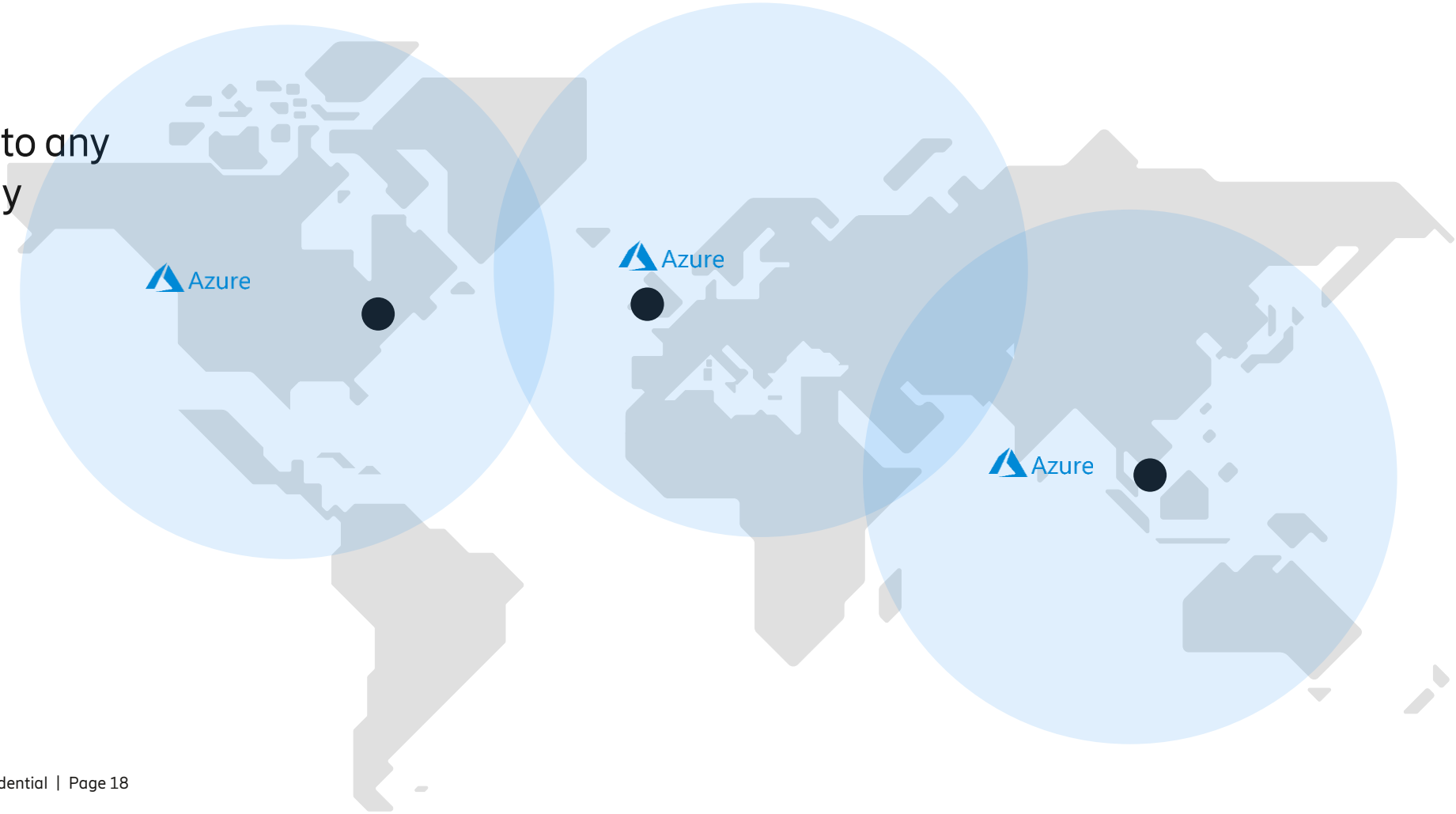
Azure Architecture cont.



Availability

- Three nodes covering three main regions

- Any node can connect to any availability zone on any cloud IoT endpoint



https://www.ericsson.com/en/portfolio/iot-and-new-business/iot-solutions/iot-accelerator/cloud-connect