Enabling Secure Connectivity for 5G Fixed Wireless Access to Homes

THALES

Building a future we can all trust

Executive Summary

This document highlights how Thales supports Original Equipment Manufacturers (OEMs) in meeting the specific requirements set by Mobile Network Operators (MNOs), when they build their Fixed Wireless Access (FWA) devices.

To capitalize on the expanding 5G Fixed Wireless Access (FWA) opportunity, MNOs are now supplying FWA CPE devices to support their FWA services to homes and small businesses. Their most important requirements for these connected devices relate to: ease of installation, provision of high bandwidth, security features and device lifetime in the field.

OEMs are responsible for incorporating these requirements into the FWA CPE devices they manufacture. When building these devices, these requirements must be catered for during the initial design stage for the overall system to work effectively and securely in the field.

Thales offers support to FWA CPE device designers through a framework called **Build, Run, Protect**. This framework assists device makers in meeting the demands of Mobile Network Operators (MNOs) while also allowing them to benefit from the advantages of new technologies. Of these, the Build stage is where the overall process starts and is where all the design decisions must be made. Thales has created a range of market leading products and services to implement these design decisions for each of the most important requirements of the MNOs across the whole FWA CPE solution.

The resurgence of FWA with 5G

Many operators have deployed FWA selectively for decades to offer customers internet service, typically in underserved areas where wired internet connections are unavailable. Until now, FWA has not achieved widespread operator adoption outside of a few countries such as Austria, Finland and the US. However, the introduction of 5G is changing that, with more governments now providing funding to address digital divides and the need for levelling up broadband access. In addition, more regulators are viewing 5G wireless as a real alternative to wireline connections for delivering broadband internet services.

It is often challenging to justify fixed line broadband investments in less populated areas with few paying subscribers or inaccessible terrains such as mountains or islands. In cities, while the population density is higher, the existing infrastructure and complex urban environments can also pose challenges. Local laws and regulations, such as permitting requirements or restrictions on infrastructure installation, can create barriers and increase costs. For example, regulations may require extensive permissions or impose high fees for digging up roads or laying cables, making fixed-line installations expensive and time-consuming.

While the challenges may differ between rural and urban areas, both scenarios can present their own unique obstacles to broadband connectivity. For these situations, 5G FWA can provide an economical solution. Being wireless, it can reduce the massive upfront cost and time needed to secure permissions, dig trenches, lay last-mile fiber, and deploy technician-installed equipment at households and businesses.

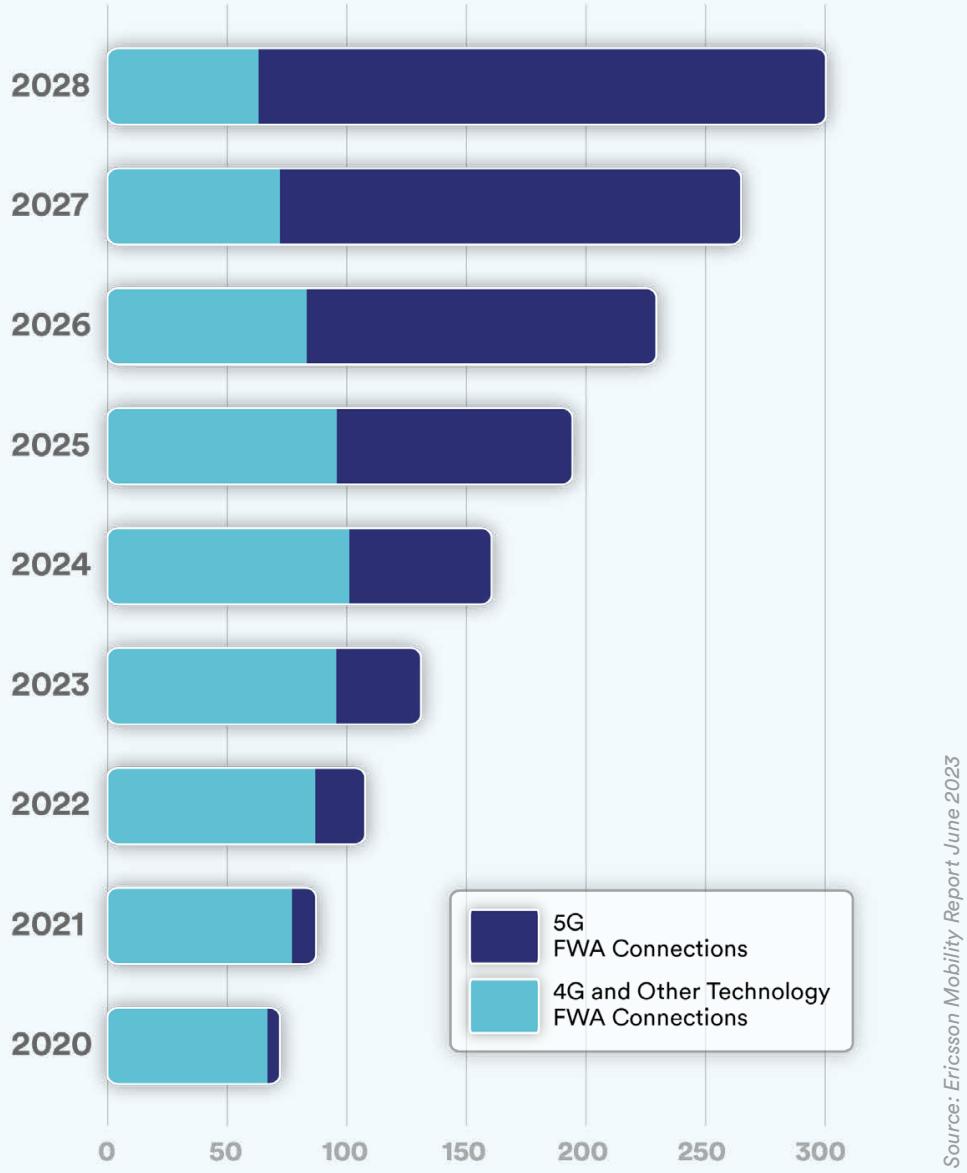
In addition, operators can look to roll out 5G FWA using their new 5G mobile wireless networks as they are deployed, speeding up market entry. Many network operators worldwide are viewing 5G FWA as a way to expand revenue opportunities and help monetize investments in 5G and wireless spectrum.

According to Ericsson's recent Mobility Report, dated June 2023, FWA connections are expected to grow from just over 100M in 2022 to 300M in 2028, an annual growth rate of 20%. By that time, 5G is expected to represent nearly 80% of the total. By 2028, 17% of fixed home broadband connections are expected to be FWA.

In fact, operators have many deployment options depending on their service area demographics, spectrum availability, and technology portfolios. For example, in dense city locations, 5G FWA can be used to augment existing fixed or mobile phone networks to offer pop-up wide area networks, such as for small or medium businesses networks, live events, or construction sites. It also can enhance redundancy and surge capacity. As the recent pandemic has shown, using wireless connections as a gap filler and backup for fiber to provide uninterrupted internet access is growing in importance. FWA can also be offered more broadly as a competitive alternative to existing home internet, such as in a suburban area with no or few other options.

In most cases, operators will selectively roll out 5G Fixed Wireless Access (FWA) in areas where they have suitable spectrum, excess wireless network capacity, and adequate supporting infrastructure. This strategic approach aims to target locations where deploying fixed wireline connections is either uneconomical or slow. The implementation of 5G FWA is expected to significantly enhance internet services by offering dramatically higher speeds and greater capacity compared to 4G. This enables FWA routers to provide internet connections that can rival or even surpass traditional wired broadband connections. Users can benefit from faster download and upload speeds, lower latency, and more reliable connections. As a result, 5G FWA becomes a more appealing option for both residential and business customers.

Figure 1. *FWA connections (millions)*



Source: Ericsson Mobility Report June 2023

The top MNO requirements for FWA Customer Premise Equipment (CPE) design

There are a variety of different scenarios that might be appropriate for MNOs to offer FWA, for example:

- An MNO might offer FWA solutions by exploiting spare capacity on a temporary basis on the mobile network, without making significant network investments. In this scenario, the MNO probably does not have a long-term commitment to FWA users, and there is a possibility that those users may choose to switch providers over time.
- An MNO may offer FWA with superior speed compared with fixed line alternatives. This is a move to win over FWA customers permanently.
- An MNO with plans for a fibre rollout could use FWA to land-grab customers quickly before competitors move in—and then transfer those customers to fibre once its slower fibre rollout is complete.
- An MNO could use FWA to extend beyond its fibre footprint into outer regions surrounding fibre areas, such as suburban locations along streets into houses and businesses. This can be a long-term plan.
- An MNO can also use FWA as a way to disrupt cable business.
- An MNO could leverage FWA to target convenience-seeking or price-sensitive customers. For a variety of reasons, some customers prefer FWA even when a fibre solution is available. They might value the convenience of being able to take it to their vacation home, or its shorter contract period or lower price, or its simpler installation and setup. Targeting these customers can be either a long-term or a short-term plan but strongly depends on the preference of customers (and existing offers) in a specific market.

These scenarios are examples that emphasise the need for flexibility in the FWA offer. There is a significant opportunity for re-use of CPE over time, rather than expecting these units to remain in their initial locations indefinitely. Easy installation is a key requirement.

Finally, it should be noted that the importance of addressing reverse logistics cannot be overlooked, as it plays a crucial role in handling product returns and repairs.

MNO priorities for FWA CPE are then reflected in **Figure 2**. This details the top 10 business user requirements regarding IoT devices and connectivity, and the most important of these for FWA CPE.

MNOs have particular high importance requirements for FWA CPE:

- **Ease of Installation**
- **Bandwidth**
- **Security Features**
- **Device Lifetime**

Figure 2. *MNO top requirements for FWA CPE*

MNO Requirements	5G Fixed Wireless Access	Key Facts / Comments
Regulatory Compliance	Medium Importance	Compliance is mainly about Health & Safety in the home
Cost	Medium Importance	Cost of connectivity represents an important portion of overall TCO
Environmental Resilience	Low Importance	CPE is usually installed indoors so ruggedness not a high priority
Ease of Installation	High Importance	CPE must be easy and quick to install – preferably self-install – in customer homes and businesses, and easy to re-use
Bandwidth	High Importance	Provision of multiple streaming services into the home requires reliable high bandwidth to replace fixed fibre and cable
Security Features	High Importance	Critical as CPE are the single source of connectivity and therefore the single source of failure for many applications
Quality of Coverage	Medium Importance	Ensures continuity of service, especially for streaming services.
Interoperability	Low Importance	CPE not expected to move location often. May be reused in several different locations during its lifetime
Device Lifetime	High Importance	Long life essential, to ensure minimum maintenance for MNO. Efficient refurbishment and repair of CPE also required
Contractual Model	Medium Importance	Usually subscription model, where customers do not invest in the hardware. Contracts tend to be automatically renewed

Source: Beecham Research adapted from ADL

Regarding Ease of Installation, CPE devices must be easy and quick to install – preferably self-install with minimal or no user manipulation – in customer homes and small businesses. The CPE will usually be installed indoors so environmental resilience is not of primary importance, although the antennas used may need to be outdoor, and may therefore require professional installation. There is significant potential for refurbishing of the CPE depending on the scenario adopted by the MNO. Refurbished CPE must also be quick to install.

Regarding Bandwidth, ensuring reliable high bandwidth service is of course an essential requirement for FWA.

Regarding Security Features, each FWA CPE device must be secure. Each device can be the point of access for attack of the whole system.

The device lifetime of an FWA CPE device is typically 5 to 10 years with remote maintenance and remote updates as required utilising the connectivity. Depending on the scenario adopted by the MNO or for repairs, devices may need to be changed out several times in their lifetime, each reuse then requiring quick and easy installation.

Some of these requirements are highlighted in the following quote:

> ***"We see FWA as the biggest high speed user application for 5G, both for the home and small business. This needs a high network capacity and data throughput, because in the home scenario there are often many users – the parents need to work and the children need to do online studying. In addition, there is growing use of smart phones and many other devices. The streaming download and upload need to be in parallel – simultaneous use – for good quality. The massive data use is becoming more common and only 5G can support the data requirement. To put this in perspective, 4G can support up to 30 connections at the same time but with that many connected devices the service slows appreciably. 5G can support up to 100 connection devices at once so has considerably more capacity"***
>
> Senior executive in a global cellular module supplier

The challenge for OEMs designing these requirements into FWA CPE devices

For OEMs designing these MNOs' requirements into FWA CPE devices, the activities across the value chain that these devices serve need to be taken into account. As illustrated in **Figure 3**, these activities start with the Device itself – how the device is connected and secured involving choice of SIM*, chipset and cellular module. The choice of connectivity provider needs to take into account provisioning requirements and initial setting up, as well as requirements for network operation. The Platform covers the connectivity management, which will most likely be carried out by the connectivity provider, and the device management for each CPE device. Finally, processing and analysing the data from all of the CPE devices for maintenance and data analytics.

All of these activities must be capable of being carried out throughout the lifetime of the devices – and securely across the whole solution.

* Note that the word 'SIM' in this paper is used in a generic sense. Depending on requirements, the specific type of SIM used could be a ruggedised SIM, eSIM or iSIM.

Thales has responded to these needs with a process for CPE device designers called **Build** – **Run** – **Protect**, which is outlined in **Figure 4** (over).

Figure 3. *Value chain for fixed wireless access CPE devices*

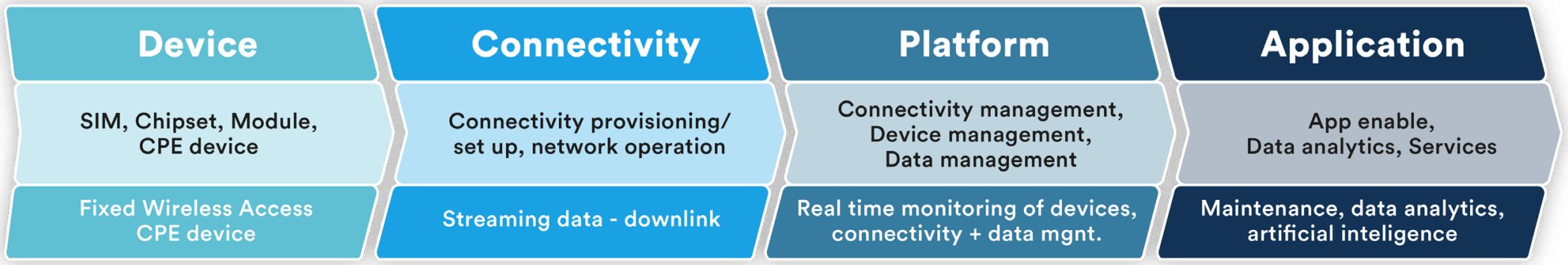
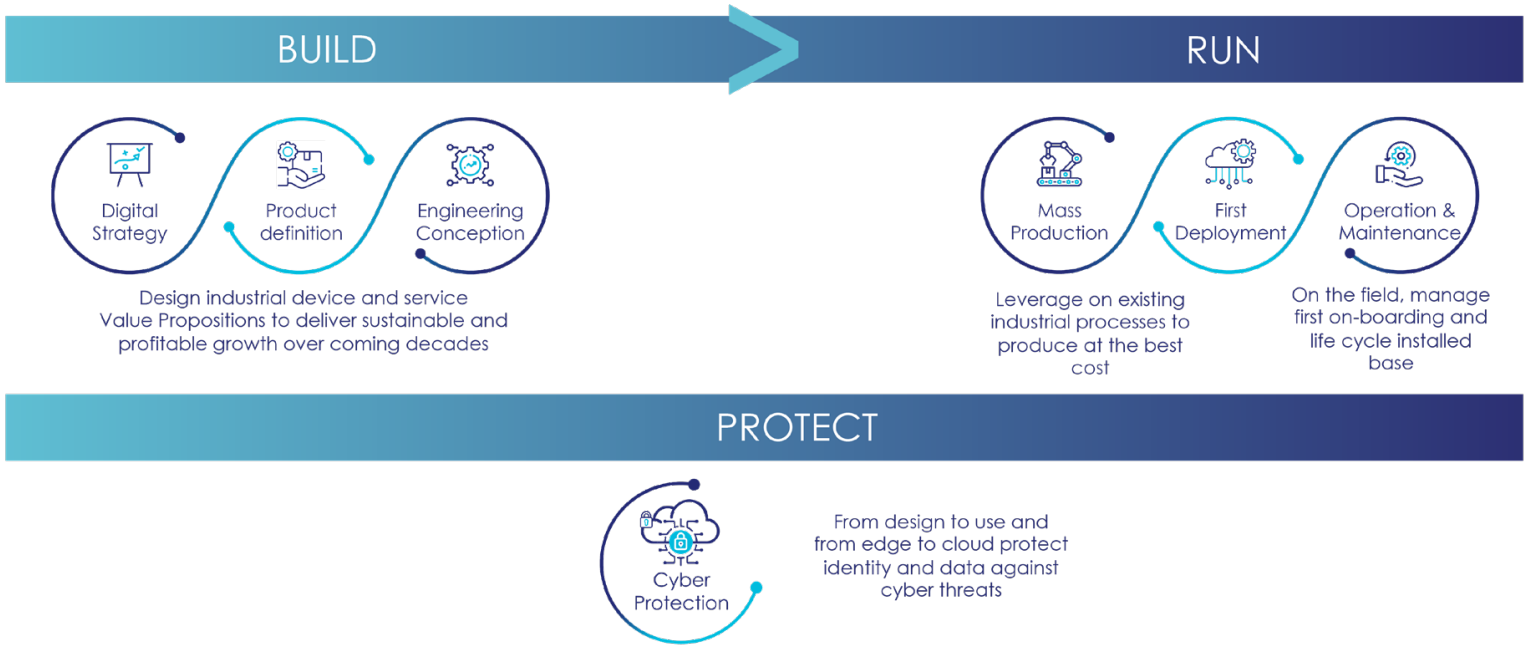


Figure 4. *Thales Build – Run – Protect process for fixed wireless access device designers*



Build is where the overall process starts and is where all the design decisions must be made, as it covers the initial digital strategy, product concept and engineering design. According to Kaleido Intelligence, 84% of firms agree that the initial hardware design is their number 1 IoT challenge. It is the key stage for defining the connectivity choice, the level of security and other requirements to meet the business needs of the CPE solution.
Thales offers a range of industrial grade, standardised and future proof hardware SIMs to meet the challenge for FWA CPE devices, in order to match the operational need for quick and easy installation, duration in the field ruggedness for repairs and refurbishments, and versatility while using cellular to securely connect the devices.

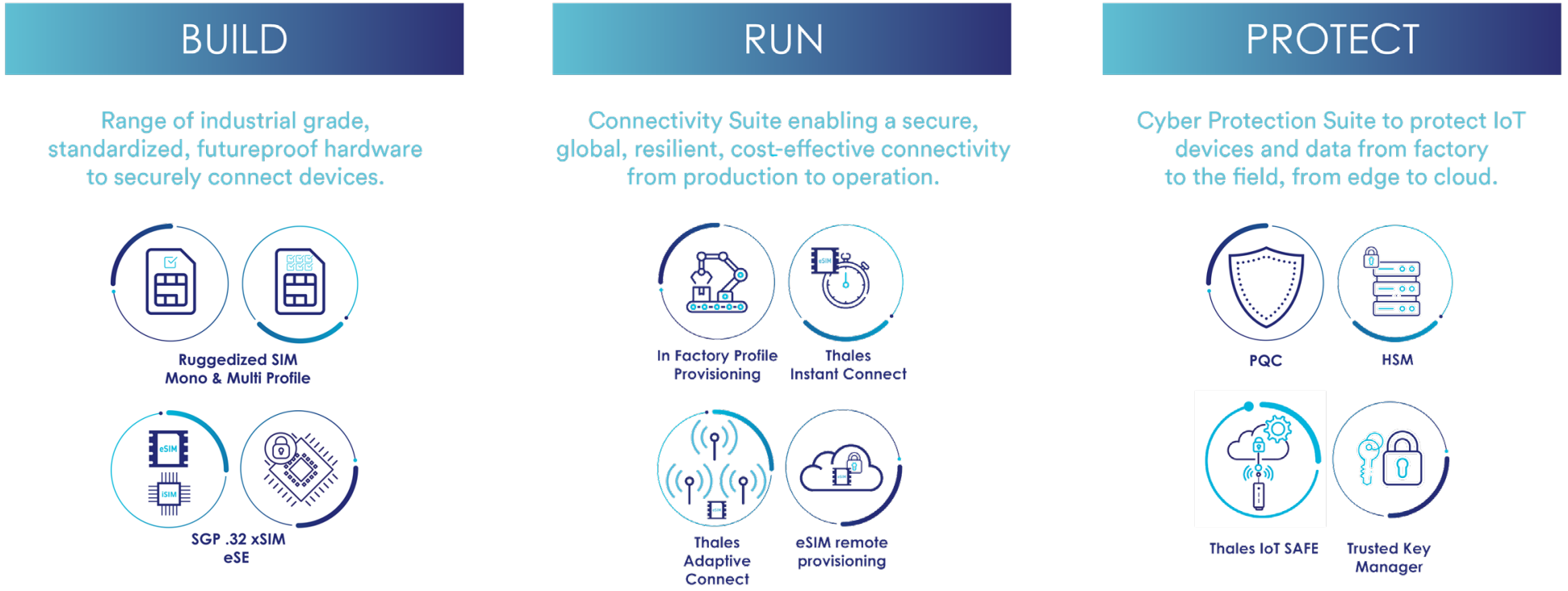
Run covers mass production, first deployment and then operation and maintenance for the device life in the field and subsequent decommissioning. According to Kaleido Intelligence, 51% of firms experience poor global connectivity with their IoT deployments. The need is for a solution allowing an efficient, open and resilient connectivity without impacting on manufacturing processes and costs. Thales SIMs and associated tools can simplify logistics with single Stock Keeping Units (SKUs) so that the SIM can be treated like any other discrete component for manufacturing purposes.

Protect covers the cybersecurity needs of FWA CPE devices and its data from the production line through to subsequent operation in the field. According to Kaleido Intelligence, 42% of firms consider that the security of devices through production and in the field is challenging. With large scale deployments of FWA CPE devices, the attack surface increases in line with the deployment size so the solution must be completely scalable. Thales offerings protect the device identity, shield data flows from edge to cloud and reinforce data sovereignty for critical assets.

How Thales meets FWA CPE top requirements

Figure 5 shows the Thales IoT portfolio that supports FWA device design requirements, comprising a wide range of SIMs, the Thales Connectivity Suite and the Thales Cyber Protection Suite.

Figure 5. *Thales IoT Offer Portfolio for Build – Run – Protect*



With the high importance requirements that MNOs have for FWA CPE noted earlier in mind, Thales products and services that support these within the product design itself are as follows:

Ease of Installation. Use of eSIM together with TIC (Thales Instant Connect) provides a strong basis for meeting this challenge. eSIM are designed to optimise installation logistics and thereby assist the planning of consistent installation rates. TIC is a patented and proven solution, based on a specially designed app that is integrated in a Thales eSIM. This app operates in conjunction with a Thales server to provide initial connectivity for the FWA device and facilitates seamless download and activation of the MNO's permanent subscription.

This does not require MNOs to pre-insert a SIM card and/or pre-load a subscription prior to despatch to the end user. There is also no initial connectivity mechanism or 'bootstrap'. When the customer switches on their FWA device for the first time, the correct subscription is downloaded and activated automatically, remotely. Customers enjoy a true plug-and-play experience, straight out of the box.

Bandwidth. Thales eSIM are designed to work with 5G.

Security Features. Thales eSIM are designed to work seamlessly with IoT SAFE (SIM Applet For Secure End-to-End Communication) together with TKM (Trusted Key Manager) to extend the inherent security of the eSIM from chip to cloud. IoT SAFE together with TKM facilitate deployment and life cycle management of credentials, including enabling secure firmware updates, which is vital. As threats are evolving, so are security protection solutions.

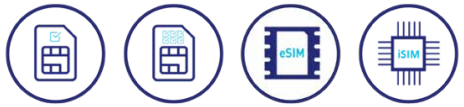
Device Lifetime. Thales Ruggedized eSIM have a very long lifespan that matches the requirements of MNOs. In addition, FWA devices in the field may need to be refurbished or repaired before being used in new locations. This requires the eSIM connectivity profile to be changed for the new location when returned to the field. eSIM with TAC (Thales Adaptive Connect) enables the ability to change the connectivity profile on a per device basis or at scale for fleets of devices as required.

Thales footprint

It should be noted that additionally, Thales has an extensive footprint with MNOs, worldwide with 450+ MNOS using our solutions.

Figure 6. *Summary of Thales offerings supporting MNO needs for fixed wireless access devices*

These Thales offerings in more detail:



1. Ruggedized SIM and eSIM/iSIM for the IoT

a. Key OEM and IoT SP challenges when designing, manufacturing and deploying cellular IoT devices:

i. Reliability, ability to operate over a long lifecycle without human intervention.

ii. Optimized BoM and space: need for an optimized design and gaining space within the device.

iii. Chip shortage: ability to manage this risk.

b. Key Thales product features that support these challenges:

i. eSIM/iSIM for IoT/MultiSIM: Fully GSMA certified multi-profile UICC with Remote SIM Provisioning (RSP) support.

ii. Dedicated & performant IoT eSIM/iSIM OS and chipset.

iii. Different form factors include Solderable (Quad) to ensure best fit with integration and operational needs.

iv. Services: end to end solution tested (hardware + connectivity enablement).

c. Why Thales is unique on the market: secure your FWA CPE deployments with Thales:

i. Long-standing IoT player, with over 600Mu embedded products shipped to mobile operators and OEMs, including automotive, smart utilities and more.

ii. Limit chip shortage risk due to Multi sourcing capabilities (chipset in-house design; several silicon sources).

iii. Benefit from unique expertise and support to integrate eSIM/iSIM in the devices.

2. Thales Instant Connect

a. Key Industrial and Consumer IoT OEM and module vendor challenges when manufacturing and deploying cellular IoT devices with eSIM and targeting multiple Telco Operators:

i. IoT devices are constrained, with no screen, no keyboard, it is not possible from the device itself to setup a Wifi connection or download an eSIM profile, among other actions. Devices need to come from the factory ready to connect, without human intervention.

ii. Ready to connect means, the device needs to come out of the factory with the Telecom Operator profile inside. This results in multiple eSIM SKUs, one per Telecom Operator.

iii. Multiple eSIM SKUs adds complexity and costs to the eSIM supply chain and stock management and device manufacturing and logistics.

iv. Slow device commercialization, as device manufacturing depends on knowing in advance the Telecom Operator for each device.

b. Benefits using Thales Instant Connect:

i. Simplification at every step, from the eSIM supply chain and stock management, to the device manufacturing and deployment, by having one eSIM SKU that can be integrated into all devices and containing Thales' initial worldwide cellular connectivity service.

ii. Flexibility and acceleration of device commercialization, by making devices more generic and suitable for multiple customers and Telecom operators.

iii. Best user experience, not dependent on Bluetooth, for Consumer IoT device activation.

iv. Save profile preloading costs: USD cost per eSIM typically charged by the eSIM vendors when supplying eSIM with preloaded profiles.

v. Avoid integrations and complexities linked to the activation/termination of the initial connectivity subscriptions.

vi. Simplifying your supply chain, with Thales as the one-stop-shop, providing both the eSIM and the initial connectivity.

c. Why Thales Instant Connect is unique:

Thales Instant Connect is a game changer for OEMs wanting to equip devices with eSIM. It helps them to stay focused in their core device-making activities rather than in the eSIM connectivity.

The OEM simply embeds the eSIM during manufacture and does not need to take care of activating and terminating the subscriptions later on. This removes the implicit complexities of tracking which subscription is inside each device and their management. These two novelties are a game changer.

3. Thales Adaptive Connect

a. Key OEM and MNO challenges when manufacturing and deploying 5G FWA devices:

i. Keeping TCO under control: throughout manufacturing/logistics and refurbishment/repair processes.

ii. Multiple SKUs when using local connectivity per country/region, leading to increased logistic costs and reduced scalability.

iii. Future proof and scalable solution for usage and/or geographic evolution.

b. Benefits using Thales Adaptive Connect solution:

i. Automatic, transparent process to access the best connectivity makes it simple and fast to use: no technical integration process, saving costs and months of delay.

ii. Cost-efficient and streamlined operating model with single SKU approach: one single eSIM for all deployments able to swap quickly to the selected connectivity provider.

iii. Simple integration: Thales eSIM with IPAe removes the need for developing specific software in the device.

iv. Implements the new GSMA SGP.32 standard for IoT.

c. Why Thales is unique on the market:

TAC is the only commercial solution available that simplifies design, manufacturing and deployment of IoT devices to an unprecedent extent. The Thales eSIM-centric approach removes the effort of implementing specific software in the device, and the cost of investing in secure manufacturing while providing the full flexibility of eSIM for connectivity management.

4. Thales IoT SAFE

a. IoT SPs consider security as #1 challenge in IoT and OEMs struggle to respond efficiently:

i. Rapidly evolving security threats: increasing attack surface of connected devices leading compromised IoT devices being used to launch DDoS attacks, identity breaches, and data theft.

ii. Costly/Difficult to implement and maintain: traditional solutions are either not effective enough (software based) or costly in terms of resources, design, manufacturing (secure element based).

iii. Regulations are on the rise: initiatives in EU and US putting more emphasis on digital security in connected objects and liabilities of solution providers.

iv. Lack of skilled workforce: scarce availability and defocus from core business.

b. OEM-IoT SP benefits using Thales solution:

i. High security level: credentials stored in the eSIM, the industry acknowledged (and standardized) tamper resistant element (TRE).

ii. Cost efficient and hassle-free integration: no impact on BOM nor manufacturing infrastructure and processes as it reuses certified secure platform (eSIM or iSIM) already present in the cellular device.

iii. Multipurpose solution to protect device and identity breaches and data leakage all along device life cycle.

iv. Evolutive: to cope with cyber threats evolution and scalable with no impact on cost whatever the number of devices deployed.

v. Under OEM/IoT SP's control: security services independent from connectivity provider, secure cloud communication is always available.

c. Superiority: For large scale IoT deployment no more compromise over security and cost.

IoT SAFE and its touchless provisioning service by Thales is the only solution allowing IoT OEMs to manufacture highly secured devices without modifying their production infrastructure and processes and still get top-notch cyber protection in the field.

Thanks to Thales unique remote management expertise activate, customize and manage over time your cyber security credentials OTA once your device is in the field.

5. Trusted Key Manager

a. Challenges for CISO of companies using connected devices (whatever connectivity technology):

i. IoT Trust: Fleet of connected devices in the field expand the surface of attack. How to ensure we can trust device identity and security?

ii. Prevent Cyber Attacks: protect against increasingly malicious activities. Theft of data. Loss of business. Criminal or geo-political related hacking activities.

iii. To comply with regulations or obtain certifications, need to prove a correct level of long-term security on devices.

iv. Multiplicity of device vendors. Complexity is introduced with each device vendor's proprietary device security solution.

v. Long term cryptographic evolution. Ensure state of the art security for devices which will be deployed for the next 20 years or more.

b. Benefits of using Thales Trusted Key Manager:

i. Pre-built platform managing devices identities and secrets through a root of trust (PKI) and a comprehensive device identity database.

ii. Advanced state of the art security backed by Thales Luna HSM with ensured evolution of cryptography over time.

iii. Centrally generate, provision and manage device identities and secrets for the whole device life cycle.

iv. Control roles per use cases and multi-vendor schemes.

c. Why TKM by Thales is unique:

i. Most comprehensive, device vendor agnostic, IoT Cyber Security platform backed by the best-in-class HSM cryptography also by Thales.

ii. Pre-implemented flexible platform going from a KMS to a complete IoT device security system with Certification Authority and device security database. Avoids years of specific developments.

Case Study – ZTE and Thales deliver effortless instant connectivity for Fixed Wireless Access (FWA)

ZTE and Thales have worked together to create a wireless Gateway Router, an FWA device that makes it easier than ever for Mobile Network Operators (MNOs) to enter this fast growing consumer IoT market. Thales Instant Connect (TIC) supports ZTE's innovative new Gateway Router solution, based on eSIM (embedded SIM technology) eliminating the need for MNOs to pre-load SIMs and subscriptions, or for end users to connect their devices to cellular networks via Bluetooth.

Addressing the challenges of instant connectivity

For MNOs, this new consumer IoT market offers considerable potential to address critical commercial objectives. Around the world, MNOs face an increasingly saturated market. Profit margins are under intense pressure. Significant investment is being committed to the roll-out of 5G networks. In response, MNOs are seeking to create new revenue streams, boost return on capital expenditure, and achieve greater differentiation. In theory at least, FWA ticks all these boxes.

However, FWA still presents MNOs with some significant challenges. These include the need to make connecting LWA (LTE-WLAN Aggregation) devices to cellular networks as straightforward and efficient as possible. Connectivity solutions also need to provide a smooth and seamless experience for end users.

Traditionally, MNOs address these issues by pre-loading a SIM and subscription into an FWA device before it is despatched to the end user. However, these must be adapted specifically to the country in which it is being used, and the customer who is going to use it. This adds considerable headwind to the MNO's logistics and supply chain. Multiple different combinations of SIMs, subscriptions and devices are required to target different markets. Costs are increased, and verifying each of these variants puts the brakes on time to market.

An alternative approach involves fitting devices with an initial 'bootstrap' connectivity mechanism. This is activated by the end user via Bluetooth and triggers the download of the MNO's permanent subscription. In this case, issues are encountered when the FWA device reaches the customer. Expecting the subscriber to use Bluetooth to activate th mobile subscription represents a far from ideal user experience. If the subscriber has difficulty setting up their device, the MNO is likely to see a costly increase in calls to its customer support team.

Thales Instant Connect: an out of the box solution for ZTE

ZTE, a leading global manufacturer of smartphones, tablets and mobile internet devices, collaborated with Thales to develop a new 'white label' solution that transforms the FWA experience for MNOs and end users alike. ZTE's new FWA design streamlines the MNO's supply chain and logistics, and simplifies activation of new subscriptions.

ZTE's new approach leverages the innovative Thales Instant Connect (TIC) service. TIC is a patented and proven solution, based on a specially designed app that is integrated in a Thales eSIM (embedded SIM). This app operates in conjunction with a Thales server to provide initial connectivity for the FWA device, and facilitates seamless download and activation of the MNO's permanent subscription.

Case Study – ZTE and Thales deliver effortless instant connectivity for Fixed Wireless Access (FWA)

As a result, ZTE's FWA device does not require MNOs to pre-load a SIM card and/or subscription prior to despatch to the end user. Moreover, there is no need for an additional and clumsy initial connectivity mechanism. When the customer switches on their FWA device for the first time, the correct subscription is downloaded and activated automatically, remotely. Customers enjoy a true plug-and-play experience, straight out of the box.

Streamlining logistics and optimising the user experience

The new ZTE device enables MNOs around the world to launch compelling, branded FWA services, quickly and efficiently. Thanks to TIC, the MNO provides a 'one touch' user experience that matches the highest expectations of today's consumers.

A single SKU (Stock Keeping Unit) can serve any number of different countries and customers. Product inventory is simplified and minimised.

The ZTE solution continues to deliver benefits throughout the product lifecycle. Subscriptions can be changed remotely at any time. In some countries, local regulations do not permit mobile subscriptions to be moved from one region to another. TIC provides the connectivity for seamless remote download of a new subscription. Similarly, if a customer chooses not to renew their FWA subscription, the ZTE device can be recovered by the MNO, refurbished, and despatched to a new customer. This optimises the return on their investment in FWA devices and minimises electronic waste.

Building the future of the consumer and industrial IoT

The eSIM and TIC will play a key role not just in the future of the LWA market, but throughout the consumer and industrial IoT ecosystems. Crucially, the combination of eSIM and TIC will provide the foundations for massive numbers of simple, remote devices to communicate securely and reliably via cellular networks, and for their mobile subscriptions to be managed efficiently over lifecycles that extend many years into the future. By providing the right solutions for OEMs, MNOs, IoT service providers and end users alike, the eSIM and TIC will help the IoT to flourish, and facilitate a world in which billions of devices as well as people are permanently connected to one another.