eSIM for IoT

Business and architecture

An eSIM architecture guide for IoT decision makers

Volume 1, May 2026 · melita.io

eSIM education series

GLOSSARY

Key terms

Terms	Description
Profile	The data and configuration on a SIM-card that enables the SIM-card to connect to the mobile network and behave like it does.
UICC	The physical SIM-card
eUICC	It is the software that runs on the SIM card chip, but the profile stored on it can be changed remotely over the air.
Bootstrap profile	A profile provisioned on the eUICC at manufacture. Used to download the operational profile once the device is in the field.
Operational profile	The actual working profile — the one that connects the device to the target network.
eSIM	The capability to remotely manage mobile network profiles on an eUICC over the air, without physically replacing the SIM card.
Network bearer	The specific radio connection established between your device and the mobile network to carry the data. E.g. LTE or 5G.
CMP	Connectivity Management Platform provides unified visibility, control, and reporting across one or more mobile operator connections. Used by enterprises to manage IoT device connectivity at large scale
MNO	Mobile Network Operator
UEM	Unified Endpoint Management. A modern term for device management platforms that control and configure connected devices remotely. UEM evolved from earlier Mobile Device Management (MDM) systems and now covers a broader range of device types including IoT.

OVERVIEW

Executive summary

This whitepaper is the first in the melita.io eSIM for IoT series taking IoT decision makers from foundation to full deployment readiness. It covers the business drivers, standards evolution, and two reference architectures for eSIM in IoT.

The most important thing to understand before reading further: adopting eSIM in IoT does not require SGP.32. SGP.22 profiles are always the foundation — what differs between architectures is how those profiles are managed. This paper presents two paths: the device-integrated approach using a UEM (Unified Endpoint Management) on top of SGP.22 and the standardised SGP.32 approach using an eIM (eSIM IoT Remote Manager). Which path fits your organisation depends on device type, fleet scale, and compliance requirements — not on which standard is newest.

Using eSIM in IoT is taking off. eSIM connections in IoT are forecasted to grow 240% CAGR to 2028 — from roughly 5 million deployments today to approximately 193 million — and by 2030 practically every new non-consumer cellular machine is expected to use the eSIM standard (Kaleido Intelligence, 2025). IoT connections globally surpassed 23 billion in 2025.

There are four key business reasons to move towards eSIM in IoT. **Global rollouts:** permanent roaming restrictions now affect Brazil, India, Turkey, China, and others — a global roaming SIM alone is no longer a viable long-term strategy. **Resilience:** for mission-critical deployments, downtime has a direct cost — a payment terminal offline for one hour loses between €200 and €800 in transactions. **Cost:** matching the right profile to the right bearer (NB-IoT, LTE-M, 5G) reduces both data cost and power consumption. **Compliance:** data sovereignty requirements are expanding, and the regulatory pressure to manage connectivity locally will only increase.

Strategically, the move towards eSIM shifts control from the mobile network operator to the enterprise by making a physical product digital. This introduces new business models for existing and new organisations in the IoT value chain. A new role emerging from this shift is the eSIM Orchestrator — both existing players and new specialists are offering enterprises a single point of control for managing eSIM profiles across multiple operators.

The journey from the original M2M standard to today involved three GSMA standards. SGP.02 (2013) introduced remote SIM provisioning for M2M but created operator-controlled lock-in. SGP.22 (2017) was designed for consumers; IoT adopted it anyway to escape SGP.02. SGP.32 (2023) was purpose-built for IoT: built for screenless, low-power devices deployed at industrial scale. Crucially, the profiles managed by SGP.32 are SGP.22 profiles — operators do not necessarily need to rebuild their backend infrastructure.

The question for any IoT decision maker is not "which standard." It is: which deployment model, for which device, at which scale, with which commercial and compliance requirements? This paper provides the foundation. Volume 2 goes deeper into deployment models and market dynamics.

BUSINESS CASE

Why eSIM: The business case

Global IoT deployments often need to consider multiple factors, including coverage, legal footprint, and commercial terms in every country. eSIM addresses this structurally — but the business case spans strategy, resilience, cost, and compliance.

Strategic: Taking back control

With a physical SIM, the operator is hardwired into the SIM. The enterprise has no leverage. eSIM offers the possibility of shifting control from the MNO to the enterprise: profiles can be changed OTA without physical access. This is not just a technical upgrade — it is a strategic shift in who controls connectivity.

Think of how the music industry changed when distribution moved from physical CDs to digital streaming: it was not just a format change, it restructured the entire value chain, empowering new players and diminishing the power of those who controlled physical distribution. eSIM does the same for IoT connectivity. Just as streaming created new platform intermediaries between labels and listeners, eSIM creates new roles between MNOs and enterprises. The enterprise is no longer captive to a single operator's commercial terms.

Business: Resilience

For mission-critical deployments, downtime has a direct cost. A payment terminal processes between **€5,000 and €20,000 in transactions per day** — that is **€200 to €800 in lost revenue for every hour offline**. A remote patient monitoring device losing connectivity is a patient safety issue. A smart meter going dark means lost billing data for the utility.

> *eSIM-enabled resilience works at the eUICC level: an eUICC can hold multiple profiles — a primary operational profile and one or more backup profiles. If the primary network fails, the device can be configured to activate a backup profile automatically.*

Business: Cost optimisation and bearer matching

Cost optimisation through selecting the right profile for the right country is ideal — effectively choosing the most attractive tariff per market.

But there is a more nuanced version: downloading the right profile for the right bearer. A low power device on LTE- or NB-IoT can only work on one of the IoT specific bearers. For these devices you need to take care a profile that that supports these bearers.

On the other hand, a device that needs high data speeds (e.g. a video camera) ideally has access to 5G. For these devices you need to enable a profile that supports this bearer.

> *At industrial scale cost and bearer matching becomes a material item – not a configuration detail.*

Business: Coverage

Multi-network access through eSIM means the device is not dependent on a single operator's coverage map. For global deployments, this is significant: a fleet deployed across 40 countries has the option of selecting multiple profiles based on the requirements and varying conditions.

Compliance: Permanent roaming restrictions

An important regulatory challenge for cellular IoT is permanent roaming — where a device uses a foreign provider's roaming agreement to remain continuously connected in a country where that provider is not licensed. Brazil, India, Turkey, and China have all implemented or tightened restrictions, citing regulatory compliance, national security, tax concerns or just restricted because of commercial reasons of the MNOs. Non-compliance can lead to disconnection. The expectation is that the number of countries restricting permanent roaming will grow.

Compliance: Market-specific requirements

Rules vary significantly by jurisdiction. Some examples from the current compliance landscape are:

Country / region	Requirement type	Rule summary
Brazil	Legal	Permanent roaming restricted; local profiles required for long-term deployments
India	Legal	Foreign eSIMs must switch to a local profile within 6 months of activation
Turkey	Legal	Local profiles mandatory; eSIM must re-home to local operator

*Source: **Transforma** Insights, "eSIM Orchestration: Driving the Next Wave of IoT Connectivity" (June 2025)*

Compliance: MNO-imposed commercial rules

Beyond legal regulation, some MNOs impose commercial constraints on permanently roaming IoT devices, even where not prohibited by law. These include quotas, time limits on sponsored roaming, and monthly "attach fees" — recurring charges per device per month simply for the right to connect while roaming. For large fleets with modest data consumption, attach fees can easily exceed the actual data cost. eSIM-based localisation eliminates these charges by converting the device from a roaming connection to a local one.

Compliance: Data sovereignty trends

The regulatory landscape is broadening beyond permanent roaming. The EU NIS2 Directive and growing data sovereignty requirements in China, Turkey, India, and beyond are creating pressure to manage IoT connectivity domestically. In the current geopolitical landscape, it is likely that the rules around local management of applications, data, devices and connectivity will become even more strict. An eSIM architecture enabling local profile deployment is not just a compliance tool for today — it is a future-proofing investment.

STANDARDS

Brief history of eSIM for IoT

To understand how the architecture delivers these benefits, it helps to see how the standards evolved. Three generations of GSMA specifications shaped the eSIM landscape that enterprises navigate today.

> *Technically to use an eSIM your device needs to have a physical SIM-card in it. Either soldered or in a SIM-Slot. On this SIM-card the digital SIM is programmable and is called eUICC.*
>
> *The profiles managed by SGP.32 are SGP.22 profiles. SGP.32 adds the standardized remote management layer on top — it does not replace the profile format.*

Terms	Description
RSP	Remote SIM Provisioning. The general term for the technology and ecosystem that enables eSIM profiles to be downloaded and managed over the air. SGP.02, SGP.22, and SGP.32 are all RSP standards.
SM-DP+	Subscription Manager — Data Preparation Plus. The cloud server that creates, encrypts, and delivers eSIM profiles to eUICCs. Both SGP.22 and SGP.32 use the SM-DP+ to deliver profiles.
LPA	Local Profile Assistant is a term used in SGP.22 the consumer eSIM standard. It is a small piece of software that lives on your device (or eUICC) and acts as the go-between between you (or a management system) and the programmable SIM-card (the eUICC).
IPA	IPA stands for IoT Profile Assistant. It includes the SGP.32 equivalent of the LPA — but designed for devices that are too small, too simple, or too power-constrained to run a full LPA. The IPA is a lightweight relay on an IoT device or on the eUICC that connects to the eIM when the device is awake, collects any pending instructions, and executes them on the eUICC.
eIM	The eSIM IoT Remote Manager is the cloud-based manager that stores pending profile instructions and delivers them to each device the moment the IPA checks in — every eUICC must have at least one eIM associated and can have more than one at a time.

2013
SGP.02

SGP.02 — The original M2M standard

Introduced in 2013, SGP.02 established the concept of remote SIM provisioning for M2M applications — the first-time profiles could be downloaded and changed over the air at large scale. Its core components were the SM-SR (Subscription Manager — Secure Routing), which managed the routing of profile packages to the correct eUICC, and the SM-DP (Subscription Manager — Data Preparation), which prepared and encrypted profiles for delivery.

The structural problem: the SM-SR was operated by MNOs. An enterprise using SGP.02 was dependent on its MNO to perform profile switches. Moving from one operator to another required bootstrapping through the existing operator — which created a commercial lock-in situation that proved painful in practice. SGP.02 is still widely deployed in utility metering and legacy M2M but is no longer the choice for new large-scale IoT projects.

2017
SGP.22

SGP.22 — Consumer eSIM repurposed for IoT

Published in 2017 and originally designed for consumer devices — smartphones, tablets, wearables, SGP.22 replaced the SM-SR/SM-DP pair with a single combined entity: the SM-DP+. The SM-DP+ can be operated by MNOs, MVNOs, or independent RSP platform providers.

With SGP.22 there is no lock-in with the MNO. The user initiates the download via the LPA.

Unlike SGP.02, the lock-in is broken not by who runs the SM-DP+, but by the pull-based model: the device or the LPA initiates the download, giving the user — not the operator — control over profile selection.

The IoT industry adopted SGP.22 pragmatically: it was better than SGP.02 for multi-operator scenarios, even though it assumed a device with a screen, a user, and adequate battery and compute resources. Many module vendors adapted SGP.22 for screenless IoT devices. SGP.22 is the current production standard for eSIM-capable cellular IoT modules for many module vendors and for mobile data routers.

2023
SGP.32

SGP.32 — Built for IoT

SGP.32 was first published by GSMA in 2023 and reached its current version (v1.2) in June 2024. It is purpose-built for IoT. The core innovation is the separation of the LPA function into two components: the IPA (IoT Profile Assistant), which lives on or in the device, and the eIM (eSIM IoT Remote Manager), which lives in the cloud and takes over the orchestration role previously handled by the end-user. In the field the IPA connects to the eIM when the device is awake — the eIM then delivers its instructions (if there are any available). An instruction could be to download a new profile.

> ***The profiles managed by SGP.32 are still SGP.22 profiles*** *— SGP.32 inherits and reuses the SM-DP+ profile infrastructure from SGP.22. Operators may not necessarily need to rebuild their backend systems; they need to integrate with eIM, not rebuild their SM-DP+.*

Standards at a glance

	SGP.02 (M2M)	SGP.22 (Consumer)	SGP.32 (IoT)
Published	2013	2017	2023 (v1.2: June 2024)
Profile management	SM-SR + SM-DP	SM-DP+	SM-DP+ and eIM
Profile type	M2M profiles	SGP.22 profiles	SGP.22 profiles
Device type	M2M / legacy	Consumer devices	IoT / constrained
LPA equivalent	SM-SR (operator side)	LPA (device side)	IPA (IPAd or IPAe)
Lock-in risk	High (MNO-controlled)	Low	Low
OTA bearer	IP (operator-managed)	HTTPS (pull model)	CoAP / DTLS / HTTPS
Screenless support	Yes (limited)	Workarounds required	Native

SGP.32 deployment readiness

For those asking whether SGP.32 is deployable today: yes. The first SGP.32-certified eUICC reached market in 1H 2025. The first commercial SGP.32 deployment went live in 1H 2026. SGP.32 is no longer a roadmap item — it is a production option.

ARCHITECTURE

The building blocks

Understanding eSIM architecture requires knowing what each component does and how they interact. The following covers the key components for both SGP.22 (current production) and SGP.32 (next generation).

Components for SGP.22

- **SM-DP+ (Subscription Manager — Data Preparation Plus):** The central server that stores, prepares, and delivers SGP.22 profiles. Operated by RSP platform providers. This is the "profile warehouse and delivery engine."
- **LPA (Local Profile Assistant):** Software on the device that communicates with the SM-DP+ to download and activate profiles. In smartphones, the LPA is part of the OS and is technically called LPAd since it is in the device. There is also an LPAe (the LPA lives inside the eUICC).
- **eUICC:** It is the software that runs on the SIM card chip, but the profile stored on it can be changed remotely over the air. The eUICC is certified against GSMA specifications.

Components for SGP.32

- **eIM (eSIM IoT Remote Manager):** The new orchestration entity in SGP.32. The eIM manages the profile lifecycle for IoT device fleets — triggering downloads, enabling/disabling profiles, handling fleet operations — without requiring the enterprise to interact directly with each MNO's SM-DP+. This is the element that replaces the MNO lock-in from SGP.02.
- **IPA (IoT Profile Assistant):** The SGP.32 equivalent of the LPA, designed for constrained devices. Two variants: IPAd (on the application processor — for devices with separate modem and application processor) and IPAe (embedded in the eUICC itself — for the most constrained, single-chip devices). The choice between IPAd and IPAe is a hardware design decision made at the device design stage.
- **eSO (eSIM Orchestrator):** The entity that operates the eIM and provides higher-level services: compliance policy enforcement, network selection logic, device awareness, billing consolidation. Transforma Insights coined this term to describe the new market role that SGP.32 creates.
- **SPOG / CMP (Single Pane of Glass / Connectivity Management Platform):** The operator or aggregator platform providing unified visibility and management across multiple MNOs. The SPOG provides a single invoice, single API, and single support interface for an enterprise fleet that may span dozens of national operators.

Architecture diagrams

The two diagrams below illustrate the two principal paths to eSIM management for IoT fleets: the standardised SGP.32 architecture with SPOG/CMP, and the device vendor–integrated approach.

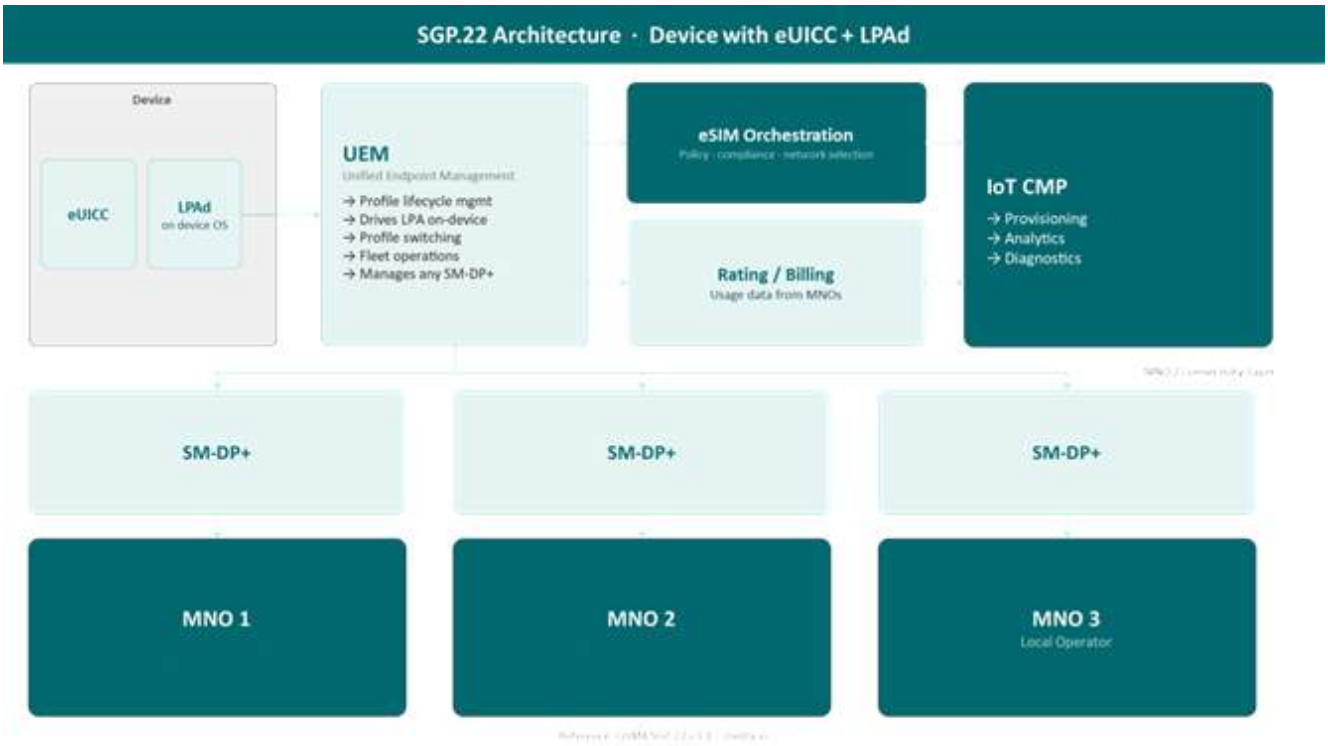

Figure 1 GSMA SGP.22 v3.1 - melita.io

Figure 1: *eSIM IoT deployment architecture following GSMA SGP.22 standard plus a proprietary SGP.22 management capability. The picture distinguishes between 1) MNO layer consisting of the MNO plus the SM-*

DP+, 2) orchestration layer consisting of the device specific Unified Endpoint Management platform + eSIM orchestration platform, device layer consisting of the eUICC plus LPA and the BSS layer consisting of the IoT CMP plus the billing. In practice the UEM can also take over functions of the eSIM orchestration. Note: the UEM and the LPAd will be device specific.

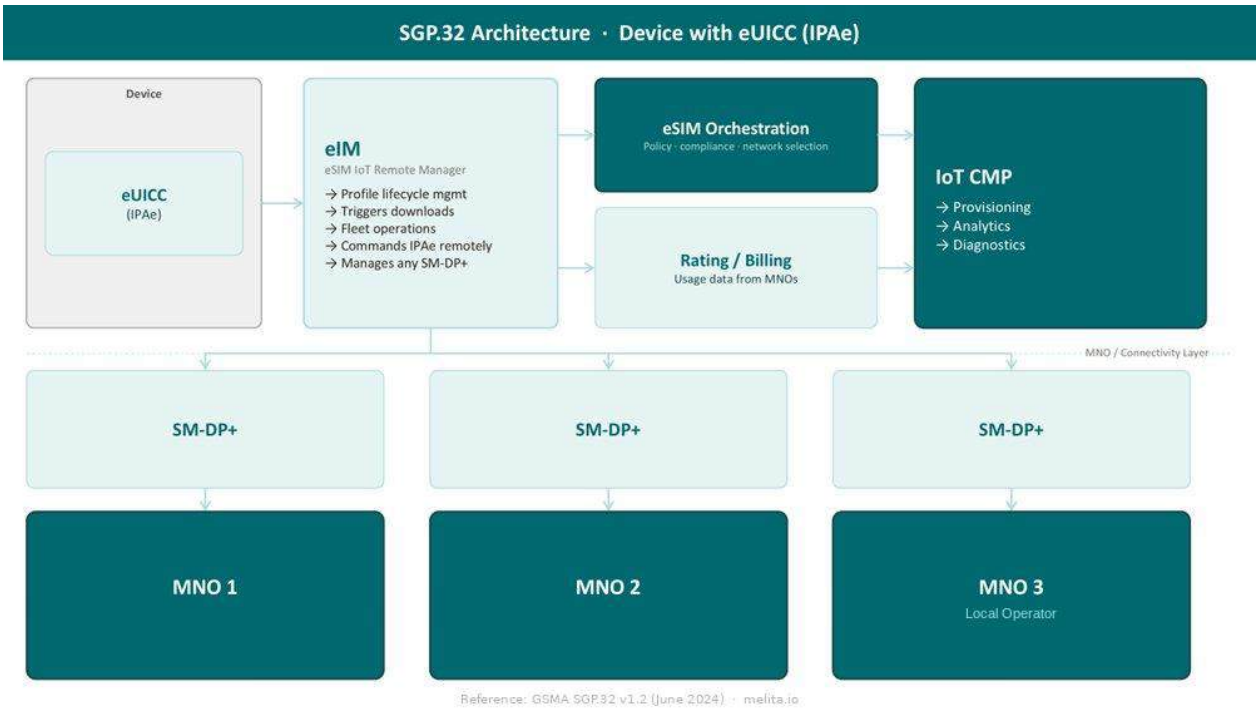

Figure 2 GSMA SGP.32 v1.2 (June 2024) - melita.io

Figure 2: *eSIM IoT deployment architecture following GSMA SGP.32 standard. MNO layer consisting of the MNO plus the SM-DP+, orchestration layer consisting of the eIM + eSIM orchestration platform, device layer consisting of the eUICC plus IPA and the BSS layer consisting of the IoT CMP plus the billing.*

> *Both architectures manage SGP.22 profiles. The difference is whether management is standardised (SGP.32 + eIM) or vendor-proprietary (device platform). For multi-vendor fleets at scale, standardisation is essential.*

SUMMARY

Conclusion

eSIM is not a single technology decision — it is a portfolio of interrelated choices: standard, components, deployment model, orchestration layer, and compliance requirements — and the way those choices fit together determines whether your connectivity strategy holds up over the next decade.

The path forward depends on where you start — and what hardware you're working with. The eUICC is the foundational constant across all three standards: every remote provisioning architecture, whether SGP.02, SGP.22, or SGP.32, depends on it as the secure element that stores and manages operator profiles.

For enterprises moving from SGP.22 to SGP.32, the picture is mixed. On the server side, there is meaningful continuity: SGP.32 reuses the SM-DP+ infrastructure from SGP.22, which means profile delivery infrastructure does not need to be rebuilt from scratch. The eIM can communicate with existing SM-DP+ deployments. But device hardware is a different matter — an eUICC certified for SGP.22 cannot run SGP.32. Device refresh is required, even if the backend transition is less disruptive than starting from SGP.02. The move is less a migration than a phased replacement, with server-side continuity reducing some of the cost and complexity.

For those still on SGP.02, the transition is more involved on both fronts. The SM-SR architecture that underpins SGP.02 has no equivalent in SGP.32, so both backend components and device hardware require replacement. There is no standardised migration path, and enterprises managing large estates should plan for parallel operation across both standards during the transition period as device refresh cycles allow gradual movement.

Either way, the direction is clear. The question is how much of your existing estate — server infrastructure and device hardware — carries forward. SGP.22 paired with a UEM-based deployment remains a legitimate route for many enterprises today, particularly where devices are already in the field and profile changes can tolerate some degree of user or local interaction. SGP.32 with an eIM is the architecture for those that need fully server-orchestrated profile management at fleet scale, pushing changes to eUICC-equipped devices without any on-device interaction, across geographies, without touching the hardware after deployment.

Choosing between the two reference architectures is a business decision before it is a technical one — but eUICC certification across the device estate shapes how realistic each path is in practice, and what the true cost of transition looks like. The four drivers covered in this paper — global rollouts under tightening permanent roaming rules, resilience for systems like payment terminals and patient monitors, cost optimisation through bearer matching, and compliance with data sovereignty requirements — do not act in isolation. Most enterprises will face at least two of them within the same deployment. eSIM, underpinned by eUICC, is the mechanism that lets a single architecture answer all four.

At scale, eSIM management does not exist in isolation. Enterprises managing profiles across multiple MNOs quickly discover they also need a single pane of glass for visibility, a consolidated billing engine across all operators, unified provisioning, and coherent reporting. eSIM Orchestration is one piece of that stack — relevant when fleet size and business logic demand it — but the broader need is for a BSS layer that treats connectivity as a managed service rather than a collection of separate operator relationships.

SERIES

This paper is part of a series

Next up:

Volume 2 · eSIM for IoT: Deployment Models & Market dynamics · Q2 2026*Deployment models, market dynamics*

The first mile problem, Practical overview of deployment models

About melita.io

melita.io is the dedicated IoT brand of Melita Limited, backed by Goldman Sachs Alternatives Infrastructure. As a licensed MNO and IoT enabler with over 30 years of telecommunications experience, we deliver secure and resilient connectivity across more than 180 countries through over 300 active roaming agreements. We combine that reach with a growing ecosystem of trusted solution partners to take enterprises from connectivity to complete, production-ready deployment.

Our connectivity solutions offer multi-network access with automatic failover, ensuring devices stay securely connected wherever they are deployed. Our eSIM offering supports native SGP.22, and also SGP.32 functionality through our global platform.

Headquartered in Malta with offices in Germany and Sweden and representative offices across Europe, we are GSMA members and hold ISO/IEC 27001, ISO 14001 and ISO 45001 certifications, a reflection of our long-standing commitment to information security, environmental responsibility and the wellbeing of our people.