CSL

Critical IoT
Connectivity
Experts

TECHNICAL WHITE PAPER

The Current State and Future Direction of eSIM, eUICC and iSIM

A Technical Guide for Decision-Makers
Featuring SGP.32, IFPP, and the April 2026
GSMA Standards Baseline

VERSION	DATE
1.5	April 2026

Executive Summary

The evolution of mobile connectivity is being shaped by standards-based technologies such as **eSIM, eUICC** and **iSIM**, alongside resilient connectivity approaches such as **rSIM®**, which together are changing how devices authenticate to networks and how connectivity is managed across their lifecycle. These technologies are reshaping consumer electronics, enterprise infrastructure, and industrial IoT.

The Challenge

Traditionally, the SIM card has been a fixed, operator-locked component, requiring manual replacement to switch networks. While this model continues to serve millions of deployed devices reliably, new global IoT deployments increasingly require multi-operator mobility, remote provisioning, and zero-touch lifecycle management.

Key Insights

- **eSIM Maturity:** eSIM adoption is well established in consumer devices and continues to expand across enterprise and IoT deployments, with more than two-thirds of mobile operators worldwide offering eSIM connectivity[2]
- **eUICC Capabilities:** Enables secure, remote lifecycle management of SIM profiles with multi-profile functionality
- **iSIM Innovation:** Integrates SIM functionality directly into the device's chipset. Juniper Research projects early iSIM volumes in the low tens of millions by 2026[4]; iSIM remains at an earlier stage of commercial deployment than mainstream consumer eSIM
- **SGP.32 Progress:** SGP.32 v1.2, published on 27 June 2024, is the current GSMA IoT RSP technical baseline for constrained and UI-limited IoT devices. Commercial rollout timing should be treated as ecosystem and market commentary rather than a standards-defined milestone
- **IFPP Progress:** SGP.41 v1.0, published on 28 February 2025, defines the GSMA IFPP architecture and requirements. The associated technical specification, SGP.42, has not yet appeared in the current GSMA released specification set; industry sources describe it as under development. Implementation timing should therefore be treated as dependent on vendor readiness, interoperability evidence and ecosystem maturity rather than fixed by the standards roadmap

What This Paper Covers

- **Definitions:** eSIM, eUICC, iSIM distinctions and capabilities
- **Standards:** GSMA RSP specifications (Consumer: SGP.21/22, IoT: SGP.31/32, IFPP: SGP.41)
- **SGP.32 Deep Dive:** Architecture, interfaces, announced ecosystem activity, and deployment status
- **Security:** ETSI standards, Common Criteria / eSA evaluation, TRE vs TEE, and integrated eUICC assurance paths
- **Compliance Roadmap:** SGP.24 compliance process, declaration types, and AN-2025-07 requirements
- **Market:** Current status, growth projections, adoption trends
- **Challenges:** Technical, operational, and regulatory barriers
- **Recommendations:** Actionable guidance for technical leaders

Strategic Imperative

Embedded connectivity is no longer just a hardware choice. It changes how organisations provision, secure, and manage device identity over the full product lifecycle. With SGP.32 v1.2 now established as the GSMA's IoT RSP technical baseline, organisations designing **new** long-life connected products should ensure their device and platform decisions are compatible with the relevant GSMA provisioning model (consumer RSP, IoT RSP, or IFPP) and evaluate iSIM where SoC integration, footprint, power profile, and certification path make it appropriate. CSL's rSIM is aligned with SGP.32; existing connectivity estates remain fully supported and fit for purpose throughout their operational lifecycle.

At a Glance: Standards Roadmap

SGP.32 v1.2 (June 2024): Current GSMA IoT RSP technical baseline

SGP.41 v1.0 (Feb 2025): Published IFPP architecture and requirements

SGP.42: IFPP technical specification, not yet in the current GSMA released set; industry sources describe it as under development

SGP.24 (2025): RSP Compliance Process: v3.2.1 Consumer (SGP.21/22 v3.x); v2.6.x Consumer (v2.x) and IoT RSP (SGP.31/32 v1.x)

SGP.25 v2.1 (Feb 2025): eUICC Protection Profile (Consumer + IoT)

AN-2025-07 (25 June 2025): eUICC Profile & Java Card security advisory

Definitions and Key Concepts

What is eSIM?

eSIM (embedded SIM) is a form factor where the SIM chip is soldered directly into a device's motherboard. It replaces removable SIM card trays, reducing physical vulnerabilities and enabling smaller device designs. The standard MFF2 package measures 5mm × 6mm × 0.9mm.

What is eUICC?

eUICC (embedded Universal Integrated Circuit Card) is the capability within a SIM secure element that enables remote download, activation, and lifecycle management of operator profiles. Unlike traditional SIMs, an eUICC can:

- Store multiple profiles simultaneously
- Enable remote provisioning and switching
- Support lifecycle management (download, enable, disable, delete)
- Comply with GSMA standards (Consumer: SGP.21/22, IoT: SGP.31/32)

What is iSIM?

iSIM (integrated SIM) embeds SIM functionality directly into the device's **System-on-Chip (SoC)**, eliminating the need for a separate SIM package or discrete eUICC component. The SIM functionality is housed in an **Integrated Tamper-Resistant Element (Integrated TRE)** within the processor's secure hardware, as defined by GSMA SGP.08/SGP.18.

Technology Comparison

Feature	Traditional removable SIM / UICC (single-profile)	eSIM (eUICC)	iSIM
Removable	Yes	No	No
Remote Provisioning	No	Yes	Yes
Multi-Profile	No	Yes	Yes
Hardware Security	Discrete chip	Secure element	Integrated TRE in SoC (SGP.08 / SGP.18 paths)
Integrated into SoC	No	No	Yes
Form Factor	2FF/3FF/4FF	MFF2	N/A (in silicon)
Power Consumption	Standard	Standard	Lower; implementation-dependent

Key Distinction

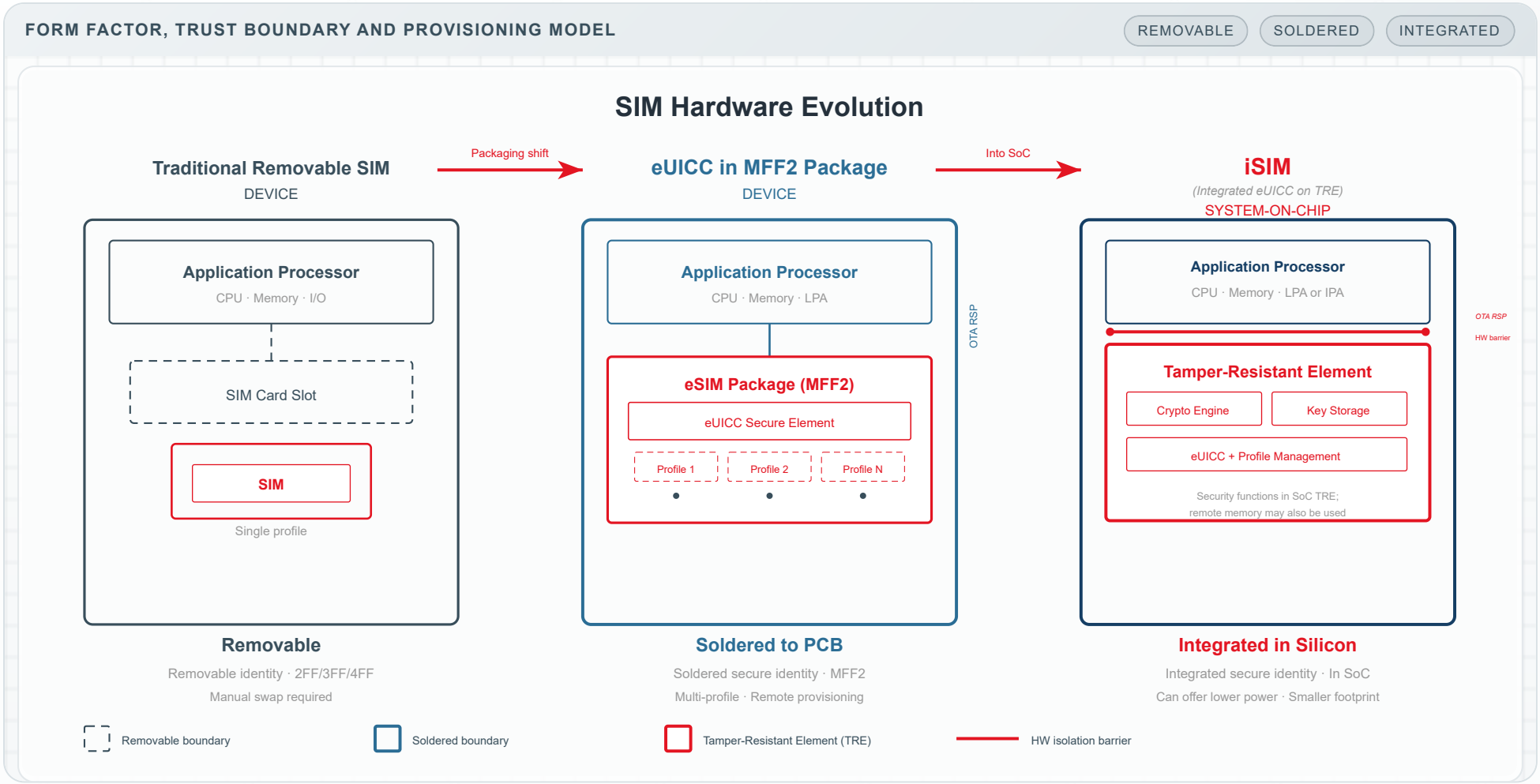
In common usage, 'eSIM' refers to an embedded SIM supporting *eUICC remote provisioning*. The **eUICC** enables RSP, while eSIM describes the form factor. iSIM integrates eUICC functionality into the SoC's secure hardware environment, typically via an Integrated TRE under the GSMA certification model.

Technical Glossary

Term	Definition
EID	eUICC Identifier, a globally unique 32-digit ID
SM-DP+	Subscription Manager Data Preparation
SM-DS	Discovery Server
LPA	Local Profile Assistant (device-side, Consumer RSP)
IPA	IoT Profile Assistant (SGP.32)
eIM	eSIM IoT Remote Manager (SGP.32)
TRE	Tamper-Resistant Element
IFPP	In-Factory Profile Provisioning (SGP.41/42)

TECHNICAL DIAGRAM

Figure 1: SIM Hardware Evolution



The progression from removable SIM to eSIM and then iSIM is a shift in packaging, trust boundary, and where the secure domain lives inside the device. Form factor and eUICC capability are independent: an eUICC can also ship in a removable (plug-in) form factor and still support remote provisioning; SGP.32 explicitly addresses removable eSIMs. This diagram shows the mainstream packaging trajectory.

Current Market Status

Consumer eSIM is now an established part of the market, with broad operator support and growing device adoption. By contrast, SGP.32-based IoT RSP is still emerging: the technical baseline is published (v1.2, June 2024), but broader deployment depends on vendor readiness, interoperability evidence, and operator enablement.

Key Market Indicators

- **441+ operators** offered eSIM services by mid-2024 (GSMA tracking data)[2]; more than two-thirds of operators worldwide reported to offer eSIM smartphone connectivity[2]
- **9 billion** xSIM-capable devices (eSIM and iSIM) projected to ship by 2030 (Counterpoint Research forecast)[3]
- **~70%** of all cellular devices shipped forecast to support eSIM/iSIM by 2030 (Counterpoint Research)[3]
- **2.36 billion** IoT eUICC/RSP-capable connections forecast by 2032 (Transforma Insights)[1]

Consumer Device Adoption

eSIM adoption in consumer devices has accelerated, led by flagship smartphone adoption and growing operator support. The introduction of eSIM-only smartphone models from 2022 onward was a significant market signal, but adoption remains uneven by geography, device category, and operator readiness.

Adoption in wearables and laptops has also grown, with embedded connectivity offering seamless activation, improved form factors, and international roaming capabilities.

SGP.32 Announced Ecosystem Activity

MARKET COMMENTARY • VENDOR AND ANALYST REPORTING

Public analyst reports and vendor announcements indicate growing claimed SGP.32 ecosystem activity in 2025–2026. Deployers should validate scope, interoperability status and commercial availability directly with suppliers and current GSMA materials:

- **Published baseline:** SGP.32 v1.2 was published on 27 June 2024; related testing and ecosystem-readiness work has continued since then
- **Compliance and assurance** *(CSL guidance)***:** Relevant GSMA compliance and security-assurance frameworks exist across Consumer eSIM, eUICC security, and integrated-eUICC evaluation; applicability and programme status for specific IoT roles and products should be validated against current GSMA and vendor materials
- **Early ecosystem announcements** *(vendor commentary)***:** Kigen announced what it described as the first market-ready eIM (October 2024); several vendors have announced certification-related and readiness milestones across eUICC, SM-DP+, IPA and related components; however, deployers should validate exact scope, interoperability status, and commercial availability directly with vendors and current GSMA materials
- **Early activity** *(market commentary)***:** Industry sources report SGP.32-related projects in planning or early stages with selected adopters; deployment scope and status have not been independently verified in this paper

Additional analyst commentary: ABI Research (September 2025) projected 2.9M SGP.32 profile downloads in 2025, growing to 194M by 2029[5]. Kaleido Intelligence (2025) forecasts approximately 50M SGP.32-compliant eSIMs managed globally by 2027[6]. These figures are gated research estimates and may not be independently verifiable from public sources.

MARKET COMMENTARY · VENDOR ANNOUNCEMENTS

Module Availability: Several vendors have publicly announced modules described as SGP.32-compliant, alongside IPA and eIM-related solutions. Prospective deployers should verify commercial availability, interoperability scope, and certification status directly with vendors and current GSMA materials.

Market Outlook and IoT Deployments

eSIM and eUICC solve many long-standing challenges in IoT deployment:

- Permanent roaming restrictions mitigated through dynamic profile switching
- Supply chain logistics simplified with single global SKU
- Zero-touch deployment enables field activation

Key Sectors

- **Smart metering:** Secure, long-life connectivity for utilities
- **Fleet/automotive:** Telematics, diagnostics, OTA updates
- **Point-of-Sale:** Portable connectivity across locations
- **Critical infrastructure:** Fire, security, healthcare monitoring

Growth Projections

Forecast note: The figures below combine estimates from different analyst methodologies and measurement frames (connections, shipments, operators). Forecasts vary materially by source, publication date and methodology; they should be treated as directional rather than directly comparable across categories. Shipment forecasts, installed-base connections, active devices and operator support should not be added together or treated as interchangeable.

Metric (unit)	Near-term	Forecast
eSIM smartphone connections (global)	~850M (2025) [2]	6.7B / 76% penetration (2030) [2]
IoT eUICC/RSP-capable connections	800M (2025) [1]	2.36B (2032) [1]
eSIM/iSIM-capable device shipments (cumulative)	4.2B (to 2025) [3]	9B (to 2030) [3]
Operators / providers offering eSIM	441+ (mid-2024) [2]	>two-thirds of MNOs globally [2]

Early iSIM outlook *(Juniper Research[4])*: ~10M iSIM devices projected by 2026; 210M iSIM connections by 2028. iSIM remains early-stage; these figures should not be compared directly with the eSIM connection and shipment metrics above.

Remote SIM Provisioning (RSP)

Remote SIM Provisioning allows secure over-the-air (OTA) management of operator profiles on eUICC-enabled devices. The GSMA defines distinct models for consumer devices, legacy M2M, and modern IoT.

RSP Standards

Standard	Purpose	Status
SGP.01/02	M2M RSP architecture & spec	Legacy
SGP.21	Consumer RSP architecture	Active
SGP.22	Consumer RSP technical spec	Active (v3.1)
SGP.31	IoT RSP architecture	Current
SGP.32	IoT RSP technical spec	Current (v1.2)
SGP.33-1	IoT eUICC test spec	Current (v1.2)
SGP.41	IFPP architecture	Published (v1.0)
SGP.42	IFPP technical spec	Not yet in GSMA released set; under development per industry sources
SGP.29	EID definition/assignment	Active

Consumer RSP (SGP.21/22)

- User-initiated profile management via device UI
- Introduces the Local Profile Assistant (LPA)
- Interfaces: ES9+ (LPA to SM-DP+), ES10 (LPA to eUICC)
- MEP support from SGP.22 v3.0+

M2M RSP (SGP.01/02) – Legacy

- Automated profile management without user interaction
- Components: SM-DP, SM-SR; Interfaces: ES2, ES3, ES5
- Relies on SMS or HTTPS for profile delivery; SMS dependence in particular is limiting for constrained LPWAN deployments

IoT RSP (SGP.31/32)

SGP.31 defines the architecture and SGP.32 provides the technical specification for modern IoT eSIM deployments.

Industry Transition: For new greenfield designs, the industry direction is toward IoT RSP (SGP.31/32). Existing M2M deployments using SGP.01/02 or Multi-IMSI continue to operate reliably and do not require immediate migration. SGP.32 uses IP-based communication models suitable for constrained IoT deployments, including devices using NB-IoT and LTE-M.

SGP.32 – eSIM IoT Technical Spec

Version 1.2 (June 2024). Defines ESipa, ES9+', ES11', ES10a/ES10b and ESep, with HTTP/TLS and CoAP/DTLS transport options for constrained IoT deployments.

Version Guidance

CSL Guidance: For new IoT deployments, CSL recommends SGP.32 v1.2+ as the forward-looking standard. Existing M2M estates (SGP.01/02) remain fully supported and do not need to be replaced on any fixed timeline. Consumer: target SGP.22 v3.0+ for MEP.

GSMA Specifications Overview

Consumer Specifications

SGP.21: RSP Architecture

Consumer RSP architecture. Defines SM-DP+, SM-DS, LPA, eUICC roles and security framework.

SGP.22: RSP Technical Specification

Consumer RSP technical details. Current: v3.1+ (MEP support). Interfaces: ES9+, ES10, ES11, ES12.

IoT Specifications

SGP.31: eSIM IoT Architecture

IoT RSP architecture. Introduces eIM and IPA. Designed for constrained and headless IoT deployments.

SGP.32: eSIM IoT Technical Spec

IoT RSP technical specification. Current baseline: v1.2 (June 2024). Defines ESipa, ES9+', ES11', ES10a/ES10b and ESep (SGP.32 §2.3, §5), with HTTP/TLS and CoAP/DTLS bindings (§6) for constrained IoT deployments.

In-Factory Provisioning (IFPP)

SGP.41: IFPP Architecture (v1.0)

Architecture and requirements for loading bound profile packages during device manufacturing. Published February 2025. IFPP can reduce reliance on first-boot OTA provisioning, which may be advantageous for tightly power-constrained deployment models, depending on device design and operating workflow.

SGP.42: IFPP Technical Spec

Technical specification for in-factory profile loading. SGP.42 has not yet appeared in the current GSMA released specification set; industry sources describe it as under development. Implementation planning should therefore be based on currently published GSMA documents and vendor-specific readiness statements.

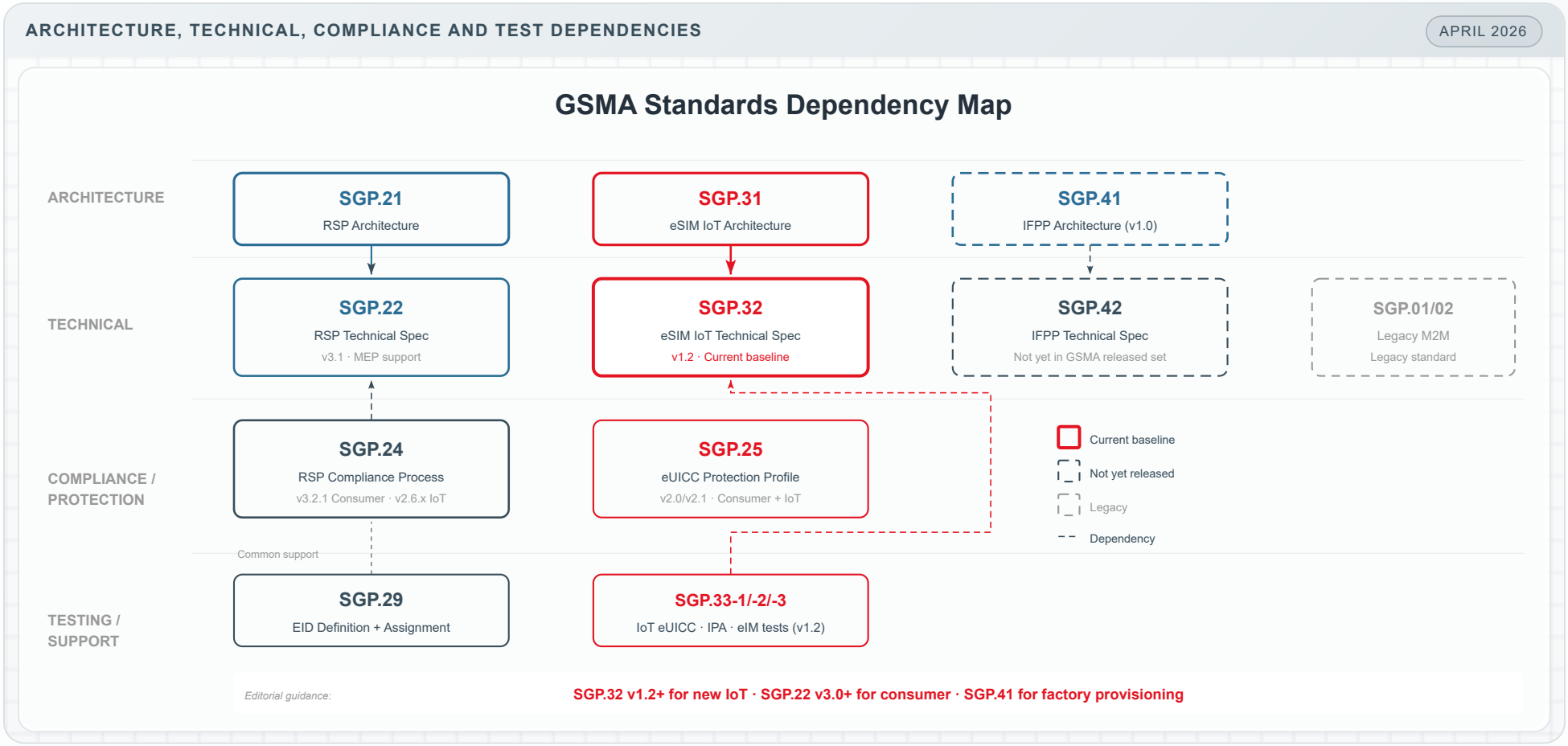
Supporting Specifications

- **SGP.29:** EID Definition and Assignment Process
- **SGP.24:** RSP Compliance Process, in two active branches: v3.2.1 covers Consumer eSIM (SGP.21/22 v3.x); v2.6.x covers Consumer eSIM (v2.x) and IoT RSP (SGP.31/32 v1.x), with IoT declaration templates for the IoT eUICC (A.8), IoT Device/IPA (A.7) and eIM (A.6) (SGP.24 §1.2, §3)
- **SGP.25:** eUICC for Consumer and IoT Devices Protection Profile (v2.0/v2.1, active from Feb 2025; v1.0 Consumer-only, sunset 2027)
- **SGP.33-1:** IoT eUICC Test Specification (v1.2, January 2025)
- **SGP.07:** eUICC Security Assurance Methodology (v2.3). Overarching framework governing eUICC security evaluation, covering both the PP-0084 and PP-0117 integrated eUICC certification paths
- **SGP.14:** GSMA eUICC PKI Certificate Policy (v2.2). Defines the PKI policy framework governing certificate issuance and management, lifecycle services, and related key-management and audit controls for eUICC deployments
- **SGP.08 / SGP.18:** Integrated eUICC security evaluation methodologies. SGP.08 covers PP-0084-based integrated eUICC evaluation; SGP.18 covers PP-0117-based integrated eUICC evaluation (for SoCs with integrated TRE)

Reading these together: Consumer (SGP.21/22) and IoT (SGP.31/32) are parallel RSP tracks; the supporting specifications above apply across both, scoped to the product and role being declared.

STANDARDS FRAMEWORK

Figure 2: GSMA Standards Landscape



Arrows show specification dependencies. SGP.32 is the current GSMA IoT RSP technical baseline.

SGP.32: eSIM IoT Specification

SGP.32 is the GSMA technical specification designed to enable eSIM functionality in IoT devices, focusing on Remote SIM Provisioning and addressing unique IoT challenges. First published in May 2023 and reaching v1.2 in June 2024, it represents a structural evolution in how IoT connectivity is provisioned and managed.

Purpose and Scope

- Provides the technical procedures, data structures, interface bindings and security mechanisms that implement the SGP.31 IoT RSP architecture and requirements
- Tailored for network-constrained or UI-constrained devices
- Designed to simplify operator switching, reducing business inflexibility
- Is intended to reduce dependence on legacy bilateral integration models when moving connections between providers
- Uses IP-based communication rather than SMS, with transport options suitable for constrained IoT deployments, including devices using NB-IoT and LTE-M

Key Components

- **IoT Profile Assistant (IPA):** Device-side component that manages profiles on IoT devices (SGP.32 §2.2). Can be embedded in the eUICC (IPAe) or in the device application processor (IPAd)
- **eSIM IoT Remote Manager (eIM):** Server-side platform ensuring secure operations and lifecycle management (SGP.32 §2.2). The eIM orchestrates remote profile-management operations and supports decisions about which profile should be enabled, disabled, downloaded or deleted for a given device
- **SM-DP+:** Reuses existing consumer RSP infrastructure for profile preparation and secure delivery

Interfaces and Protocols

- **ESipa:** eIM ↔ IPA interface for remote management (SGP.32 §5.14)
- **ESep:** Logical end-to-end eIM ↔ eUICC interface
- **ES10a/ES10b:** IPA ↔ eUICC device interfaces
- **ES9+' / ES11':** eIM interfaces to SM-DP+ and SM-DS
- RSP transports: HTTP/TLS (TCP) and CoAP/DTLS (UDP) (SGP.32 §6)
- Provides ASN.1 and JSON bindings for interface messages

Transport & Bindings: HTTP/TLS (TCP) for gateways; CoAP/DTLS (UDP) for NB-IoT/LTE-M with block-wise transfers (RFC 7959) and Connection ID (RFC 9146). LwM2M and MQTT may also carry ESipa messages (Annex B). v1.2 defines eIM support for *both* ASN.1 and JSON bindings on ESipa (SGP.32 v1.2 §6).

Security Features

- Implements TLS/DTLS secure communication protocols
- Uses ECDSA cryptographic mechanisms for authentication
- Certificate management for eIM with revocation provisions
- Provides robust security for IoT deployments

IoT-Specific Optimisations

- **Immediate Profile Enabling:** Fast activation for time-sensitive deployments
- **Fallback Profiles:** Recovery to an alternative profile where enabled by the profile, eUICC, eIM/IPA policy and device implementation
- **Emergency Profiles:** Critical scenarios for mission-critical applications
- **Profile Rollback:** Recovery mechanisms for installation failures
- **Test Profiles:** Support for development, certification, and repair

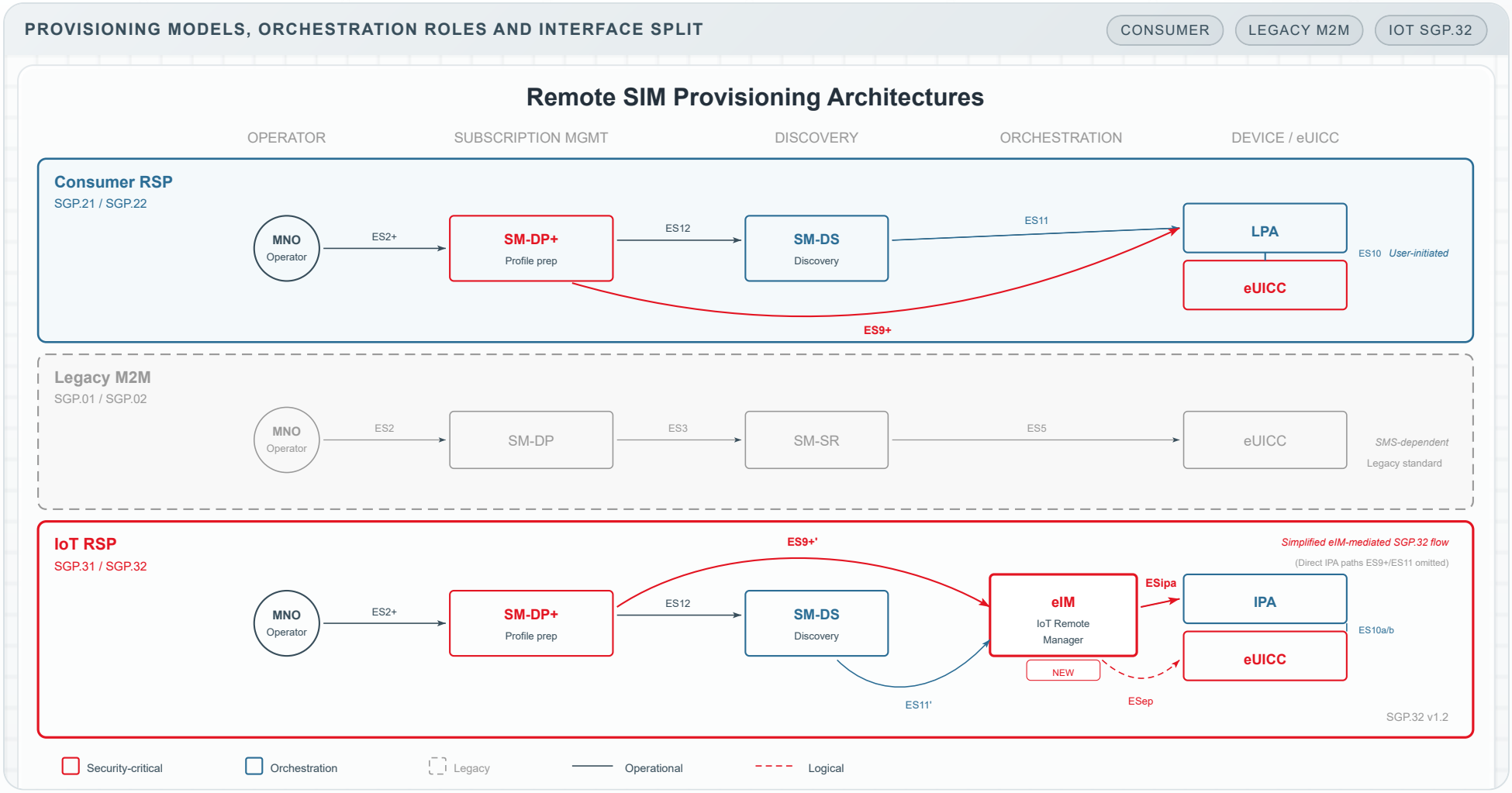
Profile and Device-State Features

- **IoTSpecificInfo:** IoT-specific profile metadata including fallback and emergency support indicators
- **Device Change:** State-change notification mechanisms for defined contexts (e.g. removable eSIM device changes)

SGP.32 Context: SGP.32 was developed to address gaps in earlier provisioning models. Legacy M2M eSIM (SGP.02) relied on operator-controlled server-initiated provisioning with SMS-based OTA, which was incompatible with LPWAN technologies such as NB-IoT and LTE-M. Consumer eSIM (SGP.22) assumed a user-facing device with an LPA, making it unsuitable for headless IoT. SGP.32 introduced the eIM and IPA model to support constrained, UI-less devices with IP-based provisioning.

TECHNICAL DIAGRAM

Figure 3: Remote SIM Provisioning Architectures



Simplified eIM-mediated view of SGP.32 IoT RSP. Direct IPA paths (ES9+, ES11) also exist but are omitted for clarity. Consumer ES9+ terminates at LPA per SGP.22.

eUICC Standards and Security

eUICC is the core enabler of programmable and remotely manageable eSIM and iSIM technologies. It introduces the ability to download, store, and switch between multiple operator profiles without physically replacing a SIM.

Security and Compliance

Security is a cornerstone of eSIM, eUICC and iSIM architecture:

- Addresses identity tampering, cloning, and physical/logical attacks
- Security evaluation depends on the product architecture and applicable protection profile. **Discrete eUICC** products follow the relevant eUICC product-security route, including SGP.25 and applicable platform protection profiles. **Integrated eUICC** products follow the GSMA integrated-eUICC evaluation methodologies: SGP.08 for the PP-0084-based path, or SGP.18 for the PP-0117-based path. These evaluations assess resistance to a defined attack potential and should not be read as an absolute security guarantee
- **Secure Hardware:** Integrated eUICC implementations rely on a tamper-resistant hardware subsystem. Assurance is strongest where SIM functionality is anchored in an integrated TRE; TEE-based approaches provide logical isolation but should not be presented as equivalent to TRE-based protection
- Relies on defined cryptographic mechanisms (including ECC and AES), certificate-based authentication, and TLS/DTLS-secured communications where specified; profile protection inherits relevant SGP.22 security mechanisms
- **Certificate Management:** X.509 certificates for authentication

GSMA eSA Certification Scheme

GSMA eSA (eUICC Security Assurance) is the GSMA security-assurance scheme referenced for eUICC evaluation and certification routes where applicable. It provides a structured assurance route for eUICC security evaluation. For integrated eUICC implementations, GSMA also references SGP.08 and SGP.18 methodologies, depending on the protection profile and evaluation path used.

Application Note AN-2025-07

Published 25 June 2025, this advisory addresses the risk of malicious Java Card application installation via publicly known RAM keys in test profiles. The application note recommends that profile owners keep RAM keys confidential regardless of profile class, that eUICC manufacturers not mix test CI and live certificates on end-user devices, and that all Java Card applications pass bytecode verification. SGP.24 v3.2.1 integrates AN-2025-07 statement and verification into the eUICC compliance declaration process (Annex A.3, via CR0236R01).

Key Provisioning Components

- **SM-DP:** Prepares, encrypts, and delivers operator profiles securely
- **SM-SR:** Manages secure OTA channel and lifecycle operations
- **SM-DP+:** Combines SM-DP and SM-SR functions into a unified system
- **SM-DS:** Facilitates discovery of available profiles

Profile Management

eUICC supports multiple operator profiles; traditionally one active at a time, though MEP devices (SGP.22 v3.0+) support multiple. Lifecycle: download, install, enable, disable, delete.

ETSI Standards

ETSI TS 102 221

Physical and logical characteristics of UICCs/eUICCs. UICC-terminal interface specification.

ETSI TS 103 383

eUICC requirements: security, functional capabilities, and compliance criteria.

ETSI TS 102 223

Toolkit for smart card applications including UICCs. Enables application-level functionality on secure elements.

iSIM Security Architecture

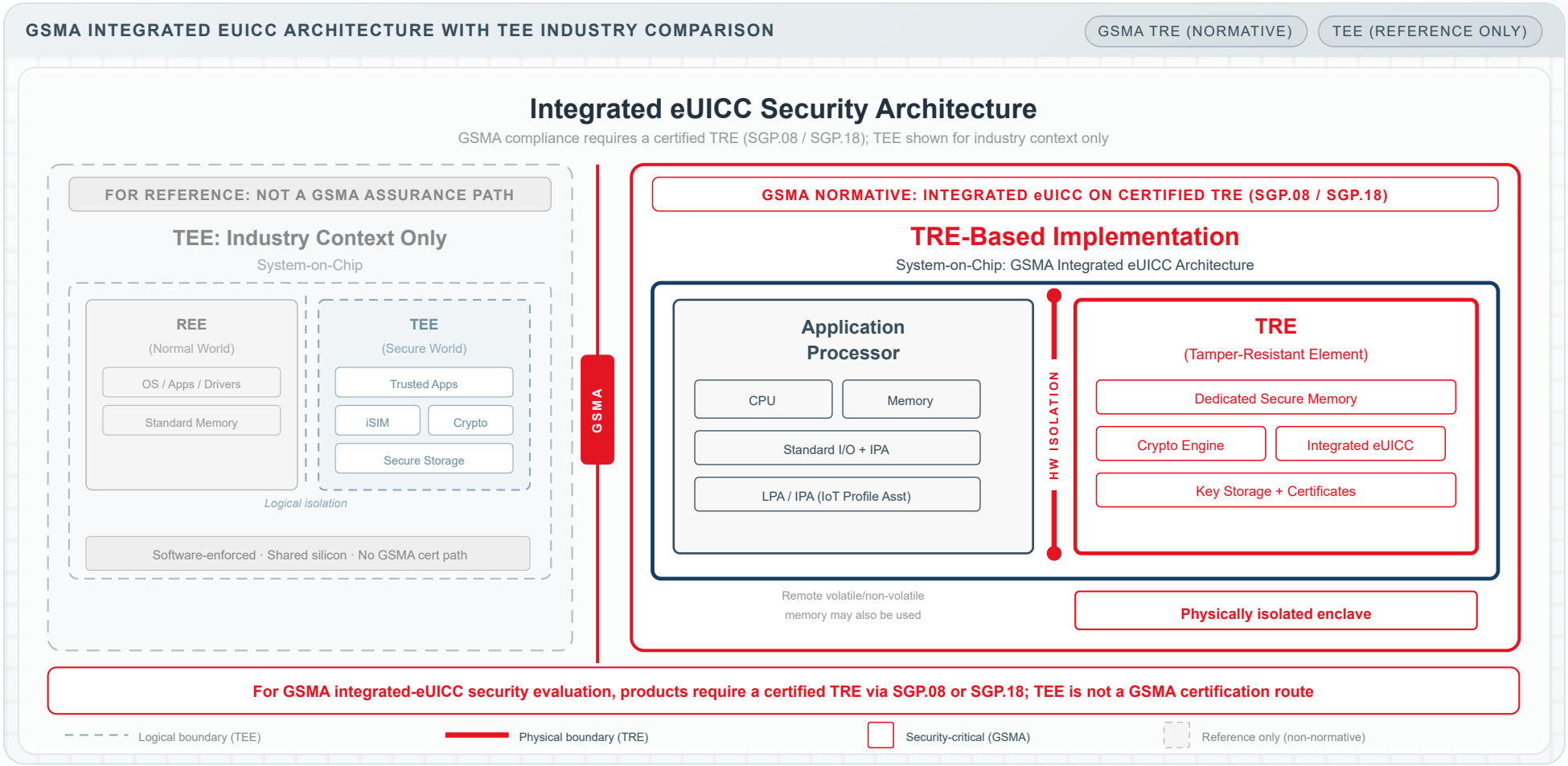
iSIM security depends on the SoC isolation mechanism:

Feature	TEE-Based	TRE-Based
Isolation	Software-defined secure zone	Dedicated tamper-resistant hardware boundary
Attack Resistance	Implementation-dependent; generally not equivalent to a certified TRE path	High (physical tamper protection, where certified)
Security evaluation	Depends on protection profile scope claimed	Integrated eUICC evaluation under SGP.08 or SGP.18; may reference GSMA eSA
Typical Use Case	Industry-specific designs outside the GSMA integrated-eUICC certification path	GSMA integrated-eUICC certification paths
Compliance dependencies	Product security evaluation, functional compliance, and relevant SAS-UP / SAS-SM site accreditation requirements all contribute to GSMA compliance status	

Key Distinction: SGP.08 and SGP.18 are integrated eUICC security evaluation methodologies tied to different protection-profile paths. Both are TRE-centric. GSMA integrated-eUICC compliance requires a certified TRE. TEE-based approaches exist in the wider industry but are not the certification path described by GSMA SGP.08 / SGP.18 for integrated eUICC. Compliance status depends on product evaluation, functional compliance, and applicable SAS site requirements.

TECHNICAL DIAGRAM

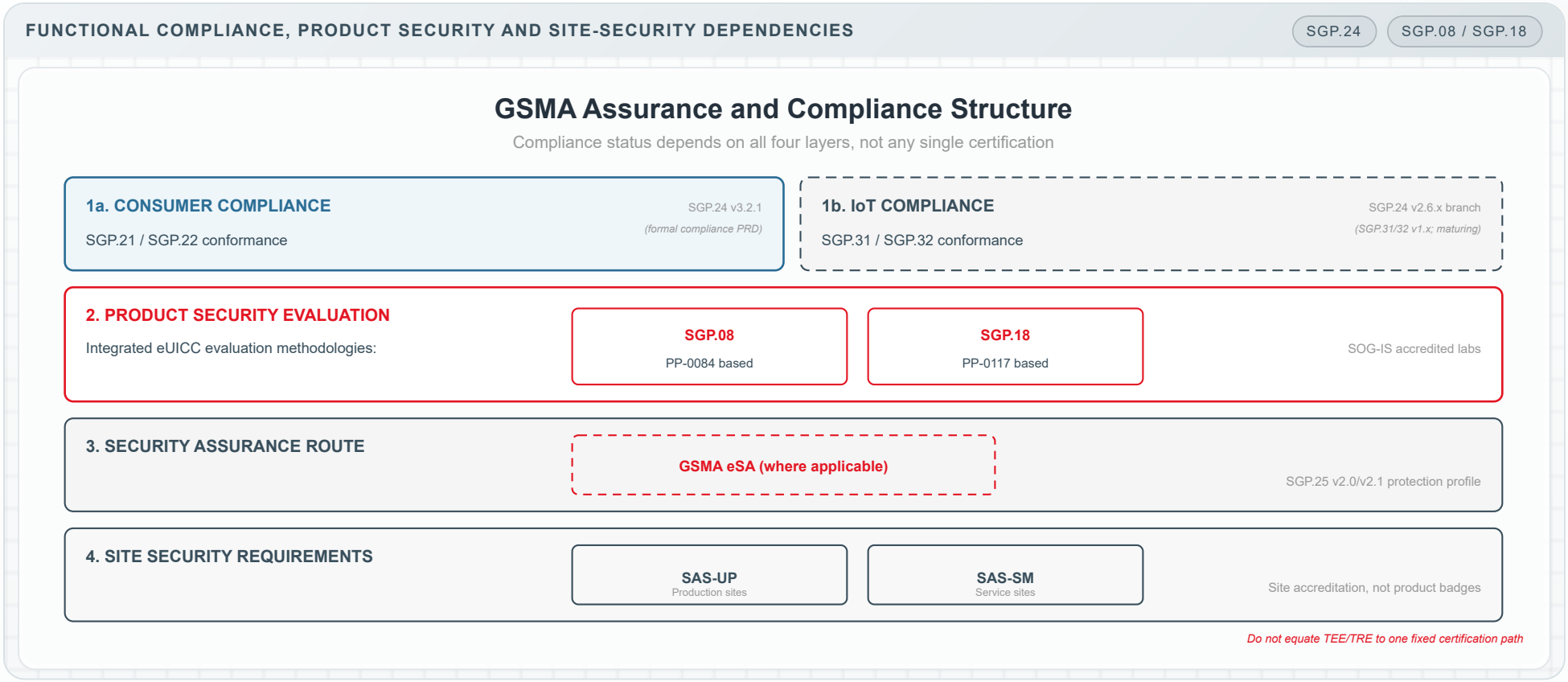
Figure 4: GSMA Integrated eUICC Architecture



GSMA integrated-eUICC compliance requires a certified Tamper-Resistant Element (TRE) via SGP.08 (PP-0084) or SGP.18 (PP-0117). The TEE-based approach is shown for industry context only and is not a GSMA-defined certification route for integrated eUICC.

COMPLIANCE FRAMEWORK

Figure 5: Assurance and Compliance Stack



Compliance status depends on functional compliance, product security evaluation, and applicable site-security requirements, not any single certification.

Editorial note: *SGP.24 provides compliance branches for both Consumer (v3.2.1) and IoT RSP (v2.6.x). The IoT branch is operational, but some ecosystem elements (for example, GCF IoT device certification) are still rolling out, so certified-product availability continues to build.*

The Emergence of iSIM

While eSIM and eUICC have reshaped how mobile identities are managed, **iSIM (integrated SIM)** represents a further integration path: it embeds eUICC functionality directly into the device's **System-on-Chip (SoC)**, housed in an Integrated Tamper-Resistant Element (Integrated TRE), with potential advantages in footprint, integration, and power profile depending on device architecture and certification approach.

Benefits of iSIM

Miniaturisation

With no separate chip, iSIM helps manufacturers reduce board footprint, making it ideal for compact wearables, sensors, and medical devices.

Power Efficiency

iSIM can reduce power overhead relative to discrete implementations in some designs, depending on SoC architecture, radio behaviour, and provisioning workflow. This may make it attractive for battery-operated IoT devices, but benefits should be validated at platform level.

Cost Reduction

Eliminating a separate SIM package can reduce component count and simplify some manufacturing and logistics decisions, although overall cost impact depends on silicon integration choices, licensing, and production scale.

Tamper Resistance

When implemented as an Integrated TRE and evaluated under the relevant certification path, iSIM can provide strong resistance to physical and logical attack classes. The effective security posture should be assessed against the target protection profile and certified implementation rather than inferred from form factor alone.

Integrated TRE (GSMA) and TEE (Industry Context)

iSIM solutions rely on secure hardware environments. Two distinct security technologies are central:

Trusted Execution Environment (TEE): A secure area within a device's main processor providing isolated execution of trusted code. TEE-based approaches may be used for SIM-like functionality in some broader market implementations, but they are not the certification path described by GSMA SGP.08 / SGP.18 for integrated eUICC.

Tamper-Resistant Element (TRE): A hardened security enclave integrated within the silicon offering resistance to physical and logical attacks (fault injection, side-channel attacks, memory probing).

Key Distinction: GSMA integrated-eUICC compliance requires a certified TRE, evaluated under SGP.08 (PP-0084) or SGP.18 (PP-0117). The choice of security architecture should be assessed against the product's target protection profile, SoC design, and applicable compliance path.

iSIM adoption is in early stages, with several semiconductor vendors announcing compatible chipsets and development platforms.

In-Factory Profile Provisioning (IFPP)

SGP.41/SGP.42 represent the next major evolution in eSIM provisioning, enabling secure profile loading during manufacturing rather than over-the-air after deployment. SGP.41 v1.0 was published in February 2025, defining the architecture and requirements. The associated technical specification, SGP.42, has not yet appeared in the current GSMA released set; industry sources describe it as under development.

What is IFPP?

IFPP is a mechanism for the in-factory provisioning of bound profile packages onto eUICCs during the device manufacturing and/or order fulfilment process, based on characteristics such as device capabilities or the geographic location into which the device is expected to be deployed.

Key Benefits

- **Out-of-the-box connectivity:** Devices can ship pre-provisioned with an operational profile, ready for first network attach on power-up (subject to activation state and coverage)
- **Battery optimisation:** Can reduce or avoid OTA provisioning overhead for initial profile loading, depending on deployment model, which may be critical for devices targeting 10+ year battery life
- **Simplified logistics:** Removes the need to maintain large inventories of plastic SIM cards and reduces SKU complexity
- **Streamlined manufacturing:** Integrates into existing production lines with a single API or toolkit
- **Offline operation:** Can support disconnected or tightly controlled factory environments, depending on implementation architecture (SGP.41 notes that Esfac-related setup may require a setup disconnected from external networks)

SGP.41 Architecture (v1.0)

SGP.41 defines a common framework to enable the provisioning of Bound Profile Packages on eUICCs in a device factory environment (SGP.41 §3). Key architectural elements include:

- **SM-DPf:** Factory profile preparation server
- **Device Manufacturer:** Orchestrates factory provisioning workflow
- **FPA / FPA Services:** Factory-side provisioning agent and service layer
- **Interfaces** (SGP.41 §3.4)**:** ES2f, Esbpp, Esfac, ES10f, ES8f, Esci, Eseum, Esed1 and Esed2
- Supports in-factory loading of Bound Profile Packages for Consumer and IoT devices; M2M IFPP remains for further study (FFS) in SGP.41 v1.0
- Built on SGP.21, SGP.31, and SGP.01 architectures
- Applies equally to discrete eUICCs and integrated eUICCs (iSIM)

Relationship with SGP.32

IFPP and SGP.32 are complementary technologies. IFPP addresses the *initial* connectivity state at the factory, while SGP.32 provides ongoing lifecycle management in the field:

IFPP + SGP.32 Workflow

1. **Factory:** IFPP loads initial profile during manufacturing.
2. **Deploy:** Device connects on power-up.
3. **Field:** SGP.32 manages lifecycle changes.

Target Use Cases

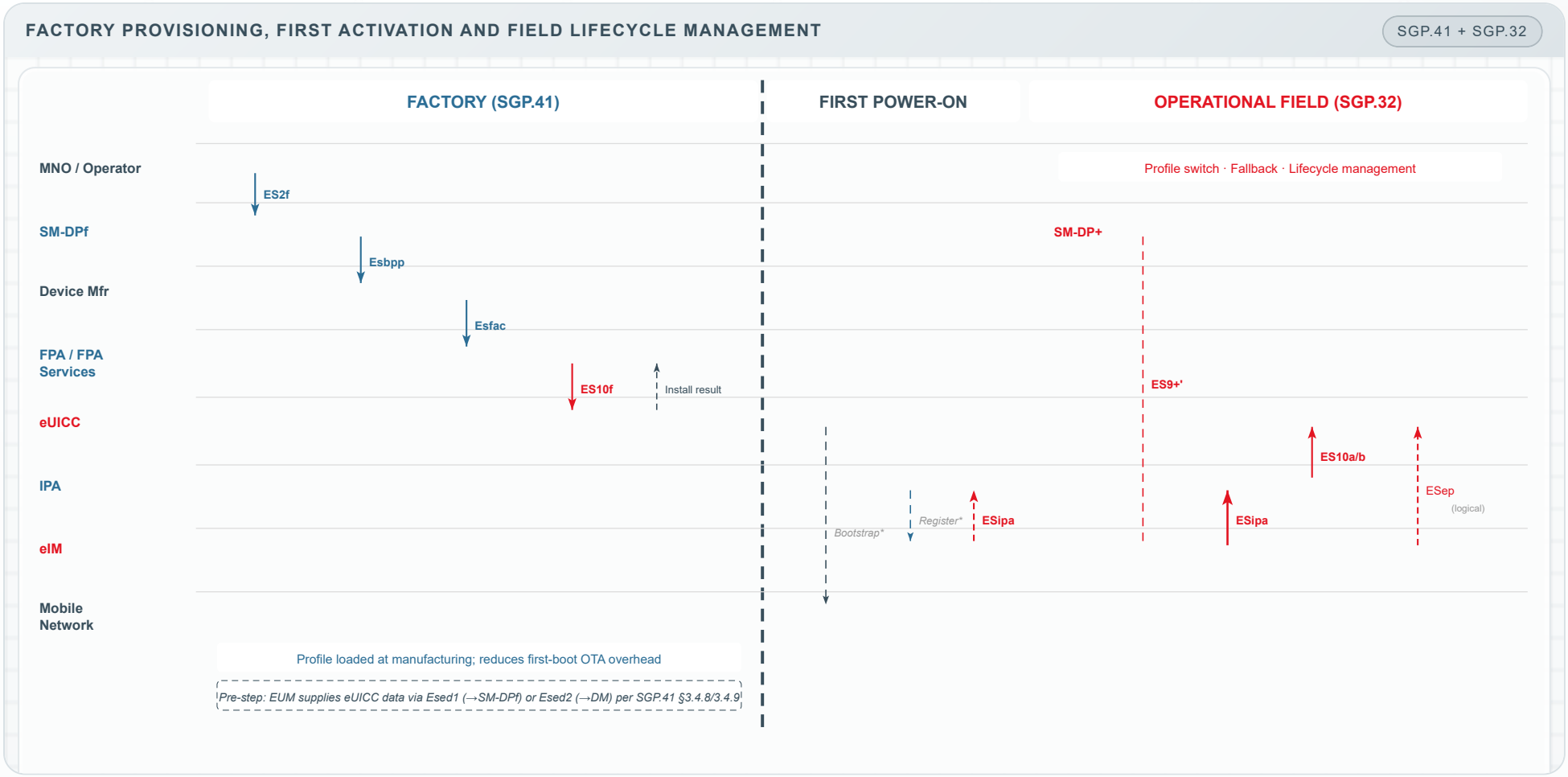
- **Smart metering:** Battery-powered devices with 10–15 year lifecycles
- **Asset trackers:** High-volume deployments requiring immediate connectivity
- **Automotive:** Profiles loaded during vehicle production for telematics
- **Fixed wireless access:** CPE devices pre-configured for regional networks
- **Consumer electronics:** Devices shipped ready-to-connect globally

Standardisation Timeline

Milestone	Status
SGP.41 v1.0 (Architecture)	Published Feb 2025
SGP.42 (Technical Spec)	Not yet in GSMA released set; industry sources describe it as under development
SGP.42 Expected Completion	2026–2027 (market expectation, not confirmed by GSMA)
Pre-standard IFPP Solutions	Available now from several vendors (market activity; not established by SGP.41)

Sustainability Impact: By potentially extending device battery life and reducing the need for premature replacements, IFPP can support ESG goals and help reduce e-waste. This is a compelling benefit for organisations with environmental commitments.

Figure 6: IFPP to SGP.32 Lifecycle Handoff



Illustrative lifecycle synthesis based on SGP.41 + SGP.32 (not a single normative GSMA process flow). IFPP (SGP.41) handles initial profile state at the factory; SGP.32 handles ongoing in-life orchestration. eIM and IPA are shown as separate swimlanes. ES10a/b connects IPA ↔ eUICC; ESep is the logical eIM ↔ eUICC interface. 'Bootstrap' and 'Register' are narrative shorthand, not formal GSMA interface labels.

Future Directions

The eSIM, eUICC and iSIM ecosystem is entering a more mature phase, with standards progress, vendor implementation activity and broader operator support beginning to address some of the barriers that have limited large-scale adoption to date.

Convergence Around SGP.32 for IoT

SGP.32 is the current GSMA IoT RSP technical baseline for new IoT deployments, with ecosystem convergence building around it:

- Unified IoT remote provisioning model, the long-term successor to M2M RSP (SGP.01/02)
- Simplified profile switching and fallback mechanisms
- More consistent interfaces for IoT platforms and MNOs
- Clear separation: Consumer RSP (SGP.21/22) vs IoT RSP (SGP.31/32)
- According to analyst commentary[5][6], broader commercial adoption activity may develop from H2 2026 onward, though timelines remain dependent on ecosystem maturation, cross-vendor interoperability validation, operator enablement, and product availability

Rise of iSIM in Power-Constrained Deployments

As chip-level integration becomes more feasible and secure, iSIM adoption is expected to expand first in device categories where footprint, power profile or board simplification justify the additional integration and certification effort:

- **Battery-sensitive applications** where 10–15 year battery life is required
- **Medical wearables** and personal safety devices
- **Industrial sensors** operating in remote or harsh environments

Public analyst forecasts suggest iSIM remains early-stage rather than mass-deployed today. Juniper Research projects over 10 million iSIM devices by 2026 and 210 million iSIM connections by 2028[4]. These figures should be treated as directional estimates subject to chipset availability, certification progress, and operator enablement.

Integration with 5G, NB-IoT and Private Networks

Next-generation connectivity models demand flexible identity management:

- **Dynamic provisioning** into local private 5G networks or MEC zones
- **Device mobility** across public/private spectrum
- **SIM-based authentication** for ultra-reliable low-latency communication (URLLC)

eSIM Orchestration

As eUICC becomes widespread, intelligent orchestration gains attention beyond basic provisioning:

- **Policy-based switching** (cost, location, signal strength)
- **Multi-profile activation** for different services
- **Cloud-native SIM management** with API access and analytics
- **Network abstraction** platforms for business logic focus
- **Failover automation:** Fallback to alternative profiles where supported by the profile, eUICC, eIM/IPA policy and device implementation

Future Directions (continued)

IFPP Implementation Outlook

(Market outlook, not standards status) In-factory provisioning activity is expected to grow as SGP.42 publication status evolves and vendor implementations mature:

- **Pre-provisioned devices:** Ship ready-to-connect, no OTA download required
- **Battery optimisation:** Critical for 10+ year device lifecycles
- **Implementation phase:** IFPP is moving from architectural definition toward broader implementation activity as SGP.42 publication status evolves and vendor implementations mature
- **Standards direction:** Treat current deployment models as implementation approaches rather than as a substitute for the formal SGP.42 technical baseline

Security Enhancements

Areas to watch in the broader security landscape include:

- Future use of stronger cryptographic approaches in profile provisioning and OTA management
- Enhanced **tamper detection** and secure execution models for integrated eUICCs
- More granular **access controls** and auditing for SM-DP/SM-SR
- Closer alignment between eSIM lifecycle controls and broader **zero-trust security architectures**

Items to Watch

Forward-looking practitioners should track these specific developments through 2026–2027 as the SGP.32 ecosystem and IFPP framework mature:

- **SGP.42 publication:** The IFPP technical specification has not yet appeared in the current GSMA released set; industry sources describe it as under development. Finalisation will trigger broader implementation activity beyond the SGP.41 architecture baseline
- **Annex C applicability updates:** The SGP.24 Annex C eSIM Certification Applicability table is revised periodically (V3.2.2 was the latest at the time of writing); expect ongoing updates as new SGP.06/07/08/18 versions become Active
- **eSA / iTRE certification milestones:** SGP.07 v2.3, SGP.08 v1.4 and SGP.18 v1.2 collectively introduced eSA-for-iTRE; product-level certifications under these paths will indicate ecosystem maturity
- **SGP.32 cross-vendor interoperability evidence:** Independent test reports across eUICC OS × eIM × SM-DP+ combinations are the leading indicator of commercial readiness
- **IoT RSP compliance maturity:** SGP.24 v2.6.x already provides the IoT RSP compliance process (SGP.31/32 v1.x), with declaration templates for the IoT eUICC, IoT Device/IPA and eIM and functional testing via SGP.33-1/-2/-3. The variable to track is ecosystem maturity (for example, GCF IoT device certification is still rolling out), plus Annex C applicability updates
- **Operator enablement of IoT RSP flows:** SGP.32 commercial value depends on MNO support for ESipa-mediated provisioning, eIM partnerships and operator-side test programmes

Strategic Outlook

The transition from fixed physical SIMs to more dynamic, software-managed identities is increasingly a question of where, when and under which operational constraints organisations should adopt the newer provisioning models. For new product designs, the SGP.32 technical baseline is established and IFPP standards work is progressing. CSL's rSIM is aligned with SGP.32, so existing rSIM deployments and new SGP.32-based designs follow a common technical direction rather than a legacy-versus-new divide. Established connectivity estates remain proven, fully operational, and fully supported by CSL throughout their operational lifecycle. Organisations can adopt new SGP.32-based platforms while continuing to rely on their current deployed estate.

GSMA eSIM Compliance Roadmap

eSIM Compliance: Consumer and IoT (SGP.24)

SGP.24 defines the GSMA RSP compliance process for both Consumer and IoT eSIM products, in two active branches: v3.2.1 covers Consumer products against SGP.21/22 v3.x, and v2.6.x (from 27 January 2025) covers Consumer v2.x and IoT RSP products against SGP.31/32 v1.x. Successful compliance is an eligibility prerequisite for the issuance of X.509 PKI certificates to eUICC manufacturers and subscription-management service providers (SM-DP+/SM-DS); LPA, IPA and eIM providers receive a Confirmation of Compliance but no GSMA-issued PKI certificate.

Three Pillars of Compliance

Every eSIM compliance declaration (Consumer or IoT) must satisfy requirements across three areas:

Scope note: SGP.24 covers both Consumer (v3.2.1) and IoT RSP (v2.6.x) compliance. The three pillars below apply across both; the applicable specification set and Annex C differ by branch and product role. Some IoT ecosystem elements (for example GCF IoT device certification) are still rolling out.

1. Site Security

Production sites must hold SAS-UP (eUICC Production) accreditation. Service sites operating SM-DP+ or SM-DS must hold SAS-SM (Subscription Management) accreditation. Site security lapses trigger a defined remediation timeline under SGP.24 §4.1.1.

2. Product Security (eUICC only)

Hardware platform certification under PP-0084 or PP-0035, plus eUICC-specific security evaluation under SGP.25 (v2.0/v2.1). Integrated eUICC products follow SGP.08 (PP-0084 path) or SGP.18 (PP-0117 path). Security recertification is required when the underlying platform changes or after a defined validity period (SGP.24 §4.2.2).

3. Functional Compliance

Demonstrated conformance to the applicable RSP requirements: SGP.21/22 (Consumer) tested via SGP.23, or SGP.31/32 (IoT) tested via SGP.33-1 (eUICC), SGP.33-2 (IPA) and SGP.33-3 (eIM). Achievable via industry partner certification schemes (e.g. GlobalPlatform, GCF, PTCRB) or vendor/third-party test plans (SGP.24 §4.3).

Declaration Process

The compliance lifecycle follows a structured path:

- **New Declaration:** Full evidence package submitted via GSMA declaration forms (Annex A templates). GSMA verifies all three pillars before confirming PKI issuance eligibility
- **Minor Update:** Incremental product changes that do not affect the security target or functional scope
- **Fast Track Update:** Streamlined process for certified eUICC products with limited scope changes (SGP.24 §3.1.5)
- **Self-Assessment:** Available for certified product updates within defined boundaries (Annex A.9)
- **Expiration:** eUICC compliance has a defined validity period; lapsed compliance requires re-declaration

AN-2025-07 Integration

SGP.24 v3.2.1 adds AN-2025-07 application note statement and verification into the eUICC compliance declaration (Annex A.3, via CR0236R01). Organisations preparing compliance declarations should review the application note for the specific attestation requirements covering eUICC profile security and Java Card application integrity.

IoT Compliance Status: SGP.24 v2.6.x (27 January 2025) extends the RSP compliance process to IoT RSP (SGP.31/32 v1.x), with declaration templates for the IoT eUICC (Annex A.8), IoT Device/IPA (Annex A.7) and the eIM (Annex A.6). IoT eUICC product security follows SGP.25 v2.0/v2.1 plus PP-0084/PP-0035 (or SGP.08/SGP.18 for integrated eUICC); functional testing uses SGP.33-1 (eUICC), SGP.33-2 (IPA) and SGP.33-3 (eIM). The framework is in place and operational, though some ecosystem elements are still maturing, with GCF IoT device certification shown as ongoing in Annex C. Confirm the applicable SGP.24 branch and Annex C for the role being declared.

Challenges to Adoption

While the promise of eSIM, eUICC, and iSIM technologies is significant, widespread adoption continues to face technical, operational, and market-level obstacles.

Fragmented Standards

Despite GSMA's leadership in defining provisioning standards, fragmentation persists in how operators and vendors interpret specifications:

- Multiple GSMA specifications and compliance requirements across M2M, Consumer, and IoT
- Which architecture to use (M2M vs. Consumer vs. IoT)?
- Inconsistent profile orchestration tools for multinational deployments

SGP.32 Ecosystem Maturity

While the specification is published and ecosystem activity is building, the SGP.32 ecosystem is still maturing:

- Cross-vendor interoperability testing across different vendor combinations is still at an early stage
- Broad commercial availability of SGP.32-native hardware across all module vendors is not yet universal
- Enterprise tooling and integration with existing device management platforms is still developing
- Broad commercial deployment timelines have shifted; according to analyst commentary[5][6], ecosystem participants now generally target H2 2026 onward, though timing remains subject to interoperability and product-readiness milestones

Interoperability Issues

Although eUICC is designed to be interoperable, some eSIM solutions still rely on proprietary orchestration tools:

- Profile portability and orchestration can be constrained by subscription-management platforms, commercial policies and legacy RSP architecture choices
- Commercial restrictions on profile switching
- Device substitution in global rollouts constrained

Provisioning Complexity

- Subscription-management services may require GSMA compliance declarations, PKI eligibility, functional testing and SAS-SM site accreditation depending on the RSP model and role
- Integration with billing, CRM, and policy engines needed
- Lack of familiarity with RSP platforms

IoT Compliance Maturity: A formal IoT RSP compliance path exists: SGP.24 v2.6.x covers IoT products based on SGP.31/SGP.32 v1.x (IoT eUICC, IoT Device/IPA and eIM declarations), with testing via SGP.33-1/-2/-3. The remaining variable is ecosystem maturity rather than the absence of a framework: for example, GCF IoT device (IPA) certification is still rolling out. Organisations deploying SGP.32-based solutions should confirm the applicable branch and Annex C and track interoperability and certified-product availability.

Regulatory Constraints

eSIM challenges the traditional telco regulatory model:

- Domestic profile storage mandates
- Cross-border profile download restrictions
- Data sovereignty requirements for SM-DP/SM-SR hosting
- Physical SIM requirements for lawful intercept compliance

Market Education

Many stakeholders still lack awareness of what these technologies offer:

- Confusion between form factors and capabilities
- Perception as high-end/experimental only
- Some MNOs view eSIM as threat to customer retention

iSIM-Specific Challenges

- Limited ecosystem maturity: only a small number of chipsets support iSIM
- Some early implementations are single-profile due to SoC constraints
- Toolchain integration: firmware, security, and RSP platforms must be adapted
- Many operators have not yet enabled iSIM-specific provisioning flows

Deployment Context Matters

Not all deployment models benefit equally from remote OTA provisioning. Installer-provisioned managed estates, single-operator environments, and products with established connectivity workflows may see limited near-term value from adopting the full RSP provisioning stack, particularly while the SGP.32 ecosystem continues to mature. The right connectivity architecture depends on the product lifecycle, installer workflow, operator landscape, and operational requirements of each deployment.

Recommendations

As embedded SIM technologies mature and SGP.32 ecosystem activity builds, technical leaders should plan how to capitalise on eSIM and eUICC (and, over time, iSIM) for new product lines while continuing to support and optimise their existing connectivity estates. CSL, as a managed connectivity provider, supports both: today's estates (including SGP.32-aligned rSIM) and new SGP.32-based designs.

For Enterprise and IoT Deployers

Begin eUICC Readiness Assessments

Evaluate your estate to determine which endpoints would benefit from remote provisioning, prioritising long-life, remotely deployed or globally distributed assets.

Design for SGP.32 Readiness Now

Even when deploying existing solutions in the short term, ensure new hardware designs remain SGP.32-compatible. As the GSMA's current published IoT remote-provisioning baseline, designing for compatibility now reduces future migration and interoperability risk.

Implement Orchestration and Lifecycle Tools

Adopt platforms (or work with a managed connectivity partner such as CSL) for profile orchestration and lifecycle management integrated with your existing device-management and cloud systems.

Evaluate iSIM for Future Designs

The integrated-eUICC (iSIM) path is defined, with security evaluation via SGP.08/SGP.18, but it is at an earlier commercial stage than eSIM. For new constrained or battery-sensitive designs, track chipset and module vendor iSIM roadmaps and adopt it where footprint and power genuinely justify it.

Evaluate IFPP for New Product Lines

For high-volume battery-powered or constrained IoT manufacturing, assess IFPP options: vendor implementations available today and the published SGP.41 architecture. SGP.42 is not yet in the current GSMA released set; industry sources describe it as under development. Plan around currently released GSMA documents plus vendor readiness and interoperability evidence.

Secure the Entire SIM Lifecycle

Implement security practices including trusted provisioning, profile certificate validation, and tamper resistance from factory to field.

Implementation Checklist

CSL Guidance: Technology selection should be driven by deployment context. Devices provisioned through managed installer channels, operating in stable operator environments, or deployed into estates with established connectivity workflows do not necessarily need the full OTA remote provisioning stack today. eSIM and eUICC remote provisioning models add the most value where zero-touch deployment, dynamic operator switching, or global SKU simplification are genuine operational requirements.

- Audit current device estate for eSIM/eUICC compatibility
- Evaluate SM-DP+/SM-SR platform options
- Assess MNO readiness for your target markets
- Review the applicable security and compliance path for your product type (e.g. SGP.24 functional compliance, SGP.06/07 assurance methodology, SGP.08/18 evaluation, SGP.25 protection profile, and relevant Annex C applicability windows)
- Review AN-2025-07 for guidance on preventing misuse of eUICC profiles and malicious Java Card application installation, and ensure any applicable assurance or compliance documentation addresses the relevant controls and attestations
- Develop profile orchestration and switching policies
- Evaluate SGP.32 readiness of chipset and module vendors
- Assess IFPP options for battery-sensitive device lines
- Track iSIM maturity and vendor roadmaps for future designs
- Engage a GSMA-aligned managed connectivity provider (such as CSL) matched to the chosen RSP model
- Create testing and validation procedures for RSP workflows
- Ensure cross-vendor interoperability testing is part of procurement criteria

Choosing Your Provisioning Path

Provisioning model selection should be driven by device class, deployment workflow and lifecycle requirements. The choices map directly to GSMA specifications:

Device / Use Case	Standards Path	Notes
Consumer smartphone, tablet, wearable with UI	SGP.21 / SGP.22 v3.x	User-driven LPA flow; MEP supported from v3.0+
UI-less or constrained IoT device (new design)	SGP.31 / SGP.32 v1.2+	eIM-mediated; HTTP/TLS or CoAP/DTLS transports
Pre-provisioned device shipping ready-to-attach	SGP.41 (architecture); SGP.42 not yet in GSMA released set	Loads BPP at factory; complements SGP.32 in field
SoC-integrated eUICC (footprint / power priority)	SGP.08 (PP-0084) or SGP.18 (PP-0117)	Composite eUICC over a certified Integrated TRE
Existing M2M / legacy proprietary estates	SGP.01 / SGP.02 (legacy); proven proprietary models	Continue to operate; no forced migration timeline

What This Means for Product Teams

For new connected products the key decisions are: which GSMA provisioning model applies (Consumer RSP, IoT RSP, or IFPP); whether SoC and module vendors support SGP.32 v1.2; the applicable security evaluation path for any integrated eUICC implementation (SGP.08 or SGP.18 depending on architecture); and whether IFPP via SGP.41 can reduce first-boot provisioning overhead. Existing deployed estates require no immediate migration; current solutions remain fully supported. Review analyst forecasts quarterly, as methodologies and denominators vary between sources.

Compliance & Assurance Map

Applicable assurance and compliance work depends on what is being declared and the architecture chosen. Treat the table below as an orientation aid; refer to the current SGP.24 Annex C for the authoritative applicability table.

Topic	Reference
Consumer eSIM RSP compliance process	SGP.24 v3.2.1; Annex C v3.2.2
IoT RSP compliance process	SGP.24 v2.6.x; Annex C v2.6.x
eUICC Protection Profile (Consumer + IoT)	SGP.25 v2.1
eUICC security assurance methodology	SGP.07 v2.3
Integrated eUICC, PP-0084 path	SGP.08 v1.4
Integrated eUICC, PP-0117 path (SoC iTRE)	SGP.18 v1.2
eUICC PKI Certificate Policy	SGP.14 v2.2
IoT RSP test specifications	SGP.33-1 (eUICC), SGP.33-2 (IPA), SGP.33-3 (eIM), all v1.2
Profile & Java Card application security	AN-2025-07 v1.0 (CR0236R01 in SGP.24 A.3)
Site accreditation	SAS-UP (FS.04) / SAS-SM (FS.08)

Key Takeaway

Embedded connectivity is changing how device identity and network access are designed and managed. With SGP.32 v1.2 published as the current GSMA IoT RSP technical baseline and SGP.41 v1.0 published for IFPP architecture and requirements, organisations should ensure **new** infrastructure and device platform decisions are compatible with the relevant provisioning model. Existing deployed connectivity estates remain reliable, supported, and fit for purpose throughout their operational lifecycle.

About CSL Group

CSL Group is a trusted provider of secure, reliable connectivity solutions for mission-critical applications across fire, security, healthcare, retail, transport and logistics, public sector, utilities, and industrial IoT sectors.

With over 30 years of experience in critical communications, CSL supports secure, resilient IoT connectivity for mission-critical applications, delivering **resilient SIM**, **eSIM**, and **IoT connectivity platforms** designed for always-on performance and compliance.

Our Commitment to Secure Connectivity

- **Multi-network, resilient SIM and eSIM solutions**
- **Remote provisioning and profile management at scale**
- **Works with customers and ecosystem partners to align connectivity deployments with applicable GSMA, ETSI and industry requirements**
- **Secure connectivity platforms** with built-in redundancy and compliance

Why Choose CSL

- Proven track record with **over 3.5 million managed connections**
- Trusted by **UK and European emergency services, healthcare providers, and national infrastructure**
- Aligned to the **GSMA eSIM specifications** covered in this paper, with products designed to meet applicable **ETSI** and industry requirements
- Backed by **24/7 support** and a commitment to innovation
- **Right technology for the right deployment:** CSL selects the optimal connectivity architecture for each product based on deployment model, installer workflow, operator landscape, and device lifecycle requirements

Legal Disclaimer

This document is provided for informational purposes only and does not constitute professional advice. While CSL Group has made every effort to ensure the accuracy of the information contained herein, no warranty or representation is made as to its completeness or accuracy.

The information in this document is subject to change without notice. CSL Group shall not be liable for any direct, indirect, incidental, consequential, or special damages arising out of or in connection with the use of this document.

Copyright Notice

Learn More: To learn how CSL can support your journey into eSIM, eUICC and iSIM adoption, visit **www.csl-group.com** or contact our team today.

References

Public Industry Analyst Sources

1. Transforma Insights: “eUICC to reach 2.4 billion by 2032”
2. GSMA Intelligence: “eSIM Market Progress and Adoption to 2030”
3. Counterpoint Research: “Over 9 billion xSIM-capable devices to be shipped by 2030” (July 2024)
4. Juniper Research: Global eSIMs & iSIMs Market 2025–2030 (January 2026)

Licensed Analyst Commentary

The following are gated research estimates cited as directional context. Readers should verify via licensed access.

5. ABI Research: SGP.32 Profile Download Forecasts (September 2025)
6. Kaleido Intelligence: SGP.32 eSIM Forecast (2027)

GSMA Standards & Specifications

7. GSMA SGP.32 – eSIM IoT Technical Specification v1.2 (June 2024)
8. GSMA SGP.21 – RSP Architecture v3.1 (December 2023)
9. GSMA SGP.22 – RSP Technical Specification v3.1 (December 2023)
10. GSMA SGP.29 – EID Definition and Assignment Process v1.1 (22 March 2024)
11. GSMA SGP.33-1 – eSIM IoT eUICC Test Specification v1.2 (January 2025)
12. GSMA SGP.33-2 – eSIM IoT IPA Test Specification v1.2 (January 2025)
13. GSMA SGP.33-3 – eSIM IoT eIM Test Specification v1.2 (January 2025)
14. GSMA SGP.41 – eSIM IFPP Architecture v1.0 (February 2025)
15. GSMA SGP.14 – GSMA eUICC PKI Certificate Policy v2.2 (27 January 2025)

GSMA Compliance & Security

16. GSMA SGP.07 – eUICC Security Assurance Methodology v2.3 (27 May 2025)
17. GSMA SGP.24 – RSP Compliance Process: v3.2.1 Consumer SGP.21/22 v3.x (July 2025); v2.6.x Consumer v2.x and IoT RSP SGP.31/32 v1.x (from 27 January 2025)
18. GSMA SGP.24 Annex C – eSIM Certification Applicability: V3.2.2 Consumer (July 2025); v2.6.x Consumer and IoT
19. GSMA SGP.25 – eUICC for Consumer and IoT Devices Protection Profile v2.1 (February 2025)
20. GSMA SGP.08 – eUICC Security Assurance Evaluation Methodology v1.4 for Integrated eUICC (PP-0084) (27 May 2025)
21. GSMA SGP.18 – eUICC Security Assurance Evaluation Methodology v1.2 for Integrated eUICC (PP-0117) (27 May 2025)
22. GSMA AN-2025-07 – Preventing Misuse of eUICC Profiles and Malicious Java Card Applications v1.0 (25 June 2025)

Source Access

All references checked April 2026. GSMA specifications (items 7–22) are published via the GSMA eSIM Specification page: https://www.gsma.com/solutions-and-impact/technologies/esim/esim-specification/. Analyst sources (items 1–6) are available from each publisher; items 5 and 6 are gated research and require licensed access. Readers should verify the latest version of each document at the time of use, as GSMA specifications and analyst forecasts are revised periodically.