

# Realising the Benefits of GSMA's eSIM IoT Specification (SGP.32)

Version 1.0

**Copyright © 2024 Trusted Connectivity Alliance Ltd.**

The information contained in this document may be used, disclosed and reproduced without the prior written authorization of Trusted Connectivity Alliance. Readers are advised that Trusted Connectivity Alliance reserves the right to amend and update this document without prior notice. Updated versions will be published on the Trusted Connectivity Alliance website at <http://www.trustedconnectivityalliance.org>



**Intellectual Property Rights (IPR) Disclaimer**

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance’s website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below. Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON- INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER’S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.

## Contents

1.	Introduction: The Emerging IoT Opportunity	05
2.	Understanding the Drivers of SGP.32	06
3.	SGP.32: Key Features and Updates	09
4.	Understanding the Benefits of SGP.32 for IoT Use-Cases	12
5.	Testing and Compliance	14
6.	Conclusion: Preparing for SGP.32	17
7.	About Trusted Connectivity Alliance	18

# Glossary of Terms

 <b>Term</b>	 <b>Definition</b>
<b>eSIM</b>	eSIM is the generic term applied to devices and eUICCs that support Remote SIM Provisioning as defined by GSMA.
<b>eUICC</b>	A UICC which enables the remote and/or local management of profiles in a secure way that meet GSMA requirements for Remote SIM Provisioning and are certified in accordance with the GSMA compliance programme. The term originates from “embedded UICC”.
<b>Operator</b>	A mobile network operator or mobile virtual network operator; a company providing wireless cellular network services. An operator owns one or more international mobile subscriber identity (IMSI) ranges.
<b>Profile</b>	A combination of data and applications to be provisioned on a UICC or an eUICC for the purpose of providing connectivity to mobile networks.
<b>Remote SIM Provisioning</b>	The process of downloading, installing, enabling, disabling, and deleting a profile on an eSIM in accordance with GSMA Specifications.
<b>SIM</b>	A generic term for the application(s) residing on the UICC that identify a subscriber and allow them to securely access a mobile network (e.g. 4G or 5G). SIM is sometimes used interchangeably with the term UICC or SIM card.
<b>SIM Card</b>	A SIM that has one of the physical plug-in form factors as defined by ETSI (i.e. plug-in, micro-SIM, nano-SIM).
<b>TRE (Tamper Resistant Element)</b>	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.
<b>UICC</b>	The platform, specified by ETSI, which can be used to run multiple security applications. These applications include the SIM for 2G networks, USIM for 3G, 4G and 5G networks, CSIM for CDMA, and ISIM (not to be confused with integrated SIM) for IP multimedia services. UICC is neither an abbreviation nor an acronym.

# 1. Introduction: The Emerging IoT Opportunity



**Connected IoT devices from smart meters, to sensors, asset trackers and smart labels, are transforming industries. Verticals such as automotive, smart cities, utilities, logistics and manufacturing are now all benefiting from the new use-cases, insights and efficiencies the IoT enables.**

Given the need for truly trusted, reliable and secure mobile connectivity across many of these use-cases, cellular and cellular low-power wide-area network (LPWAN) technologies – such as LTE-M and NarrowBand-IoT – are increasingly being leveraged to connect IoT devices.

Global cellular IoT connections grew by 27% year-on-year in 2022 – significantly outstripping the overall growth rate – to account for nearly 20% of all global IoT connections ([Source: IoT Analytics](#)). Looking ahead, the number of deployed cellular IoT devices is set to continue to increase with the new features, enhancements and value-added services introduced in the latest 5G standards (3GPP Release 17 and 18). GSMA anticipates there will be 5.8 billion licensed cellular IoT connections by 2030 across all SIM form factors ([Source: GSMA Intelligence](#)).

As deployments increase, so too is the demand for eSIM technology to cut through complexity and promote simplified global connectivity and advanced security for the IoT. Growth is set to continue, with 83% of organisations identifying eSIM as important to the success of future IoT deployments ([Source: GSMA Intelligence](#)).

While eSIM technology is already utilised across IoT deployments, industry standardisation efforts now promise to address long-standing challenges that have tempered adoption to date. This marks a significant opportunity for stakeholders across the secure connectivity ecosystem to leverage eSIM technology to unlock the full, transformative potential of the IoT.

Key among these industry initiatives is the publication of GSMA's eSIM IoT Specification (SGP32), which introduces a dedicated Remote SIM Provisioning model tailored for IoT devices.

To support understanding of the drivers, implications and applications of the new specification, TCA has developed this paper to:

- 1 **Explain** why the growing deployment of 'constrained' IoT devices presents unique considerations that are not optimally addressed by the existing M2M and Consumer Remote SIM Provisioning Specifications.
- 2 **Identify** how new components and updates introduced in SGP32 simplify the deployment and management of constrained devices at scale.
- 3 **Summarise** key benefits across various IoT use-cases.
- 4 **Explore** how the supporting compliance programme promotes confidence for operators, device manufacturers and service providers.
- 5 **Reaffirm** the need for interoperability as industry adoption builds.

## 2. Understanding the Drivers of SGP.32



**A key benefit of eSIM technology is that it is supported by an advanced, mature infrastructure that promotes interoperability and security.**

Standardisation activity for eSIM has been led by GSMA, the global industry association. Namely, GSMA created the Remote SIM Provisioning Specifications for M2M and Consumer Devices to describe the process of downloading, installing, enabling, disabling, and deleting a profile on an eSIM.

### GSMA eSIM Solution for M2M (SGP. 02)

The eSIM M2M Specification addresses devices where the profiles are managed remotely by the operator, and not the end-user. The solution introduced two key components:

**SM-DP (Subscription Manager – Data Preparation)** – prepares the profiles to be securely provisioned onto the eUICC. It also manages the secure download and installation of these profiles onto the eUICC.

**SM-SR (Subscription Manager – Secure Routing)** – securely performs functions of platform management commands and the transport of profile management commands. It is the ‘control centre’ that decides which and when profiles are used in the eUICC.

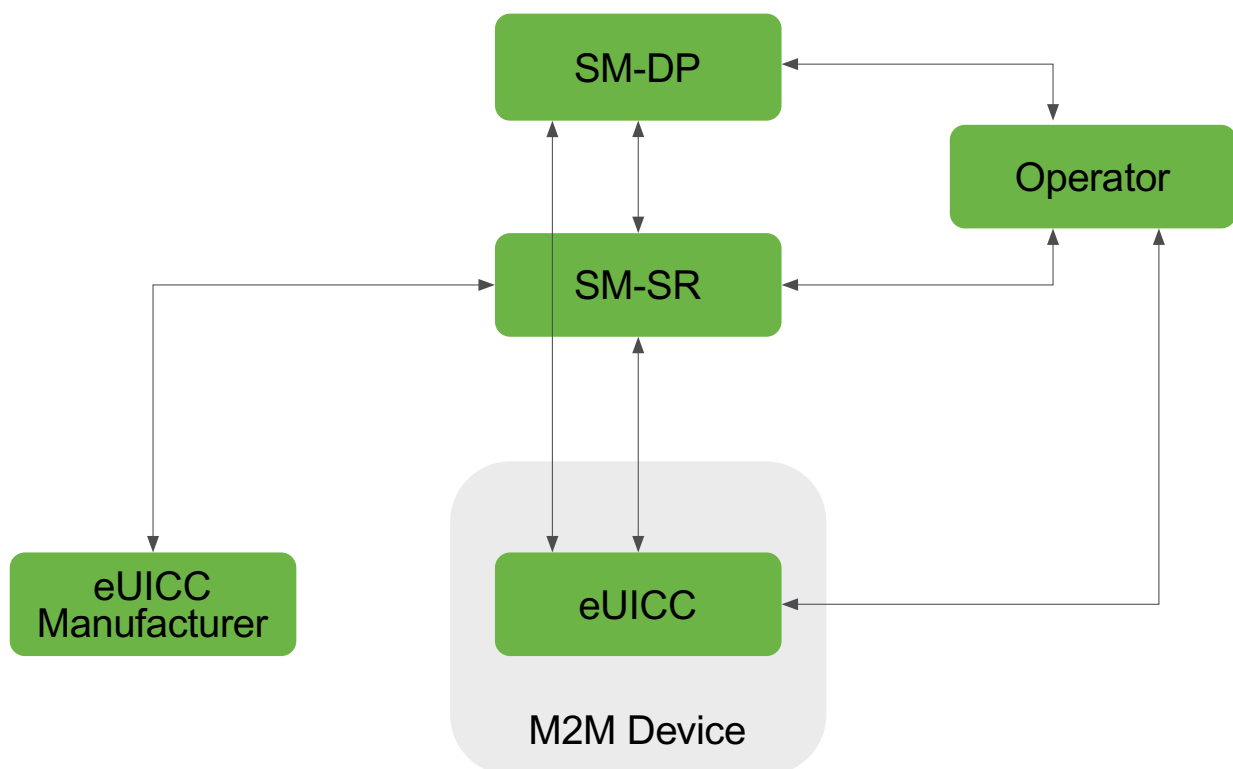


Figure 1 – Simplified Diagram of GSMA eSIM Solution for M2M (SGP.02) Architecture

The eSIM M2M architecture has been designed to be highly resilient and includes mechanisms to ensure recovery of connectivity if lost (through rollback and fallback mechanisms), as well as support for emergency calling.

Solutions based on the eSIM M2M architecture have been widely deployed all around the globe, mostly across the automotive and smart metering segments. It is less widely deployed, however, across other IoT verticals.

### GSMA eSIM Solution for Consumer Devices (SGP. 22)

The eSIM Consumer Specification addresses smartphones and other consumer devices (such as smart watches and connected laptops) where the end-user activates the profile or switches operator. The solution introduced the following components:

**SM-DP+** – responsible for the creation, download, remote management and protection of the profile. The ‘+’ indicates that it fulfils the functions of both the SM-DP and the SM-SR from the M2M solution.

**LPA (Local Profile Assistant)** – a set of functions typically within the device (or possibly in the eUICC) responsible for enabling the download of encrypted profiles to the eUICC. It also provides a user interface (UI) to allow end-users to manage the status of profiles on the eUICC.

**SM-DS (Subscription Manager – Discovery Server)** – provides a means for an SM-DP+ to reach the eUICC without having to know which network the device is connected to.

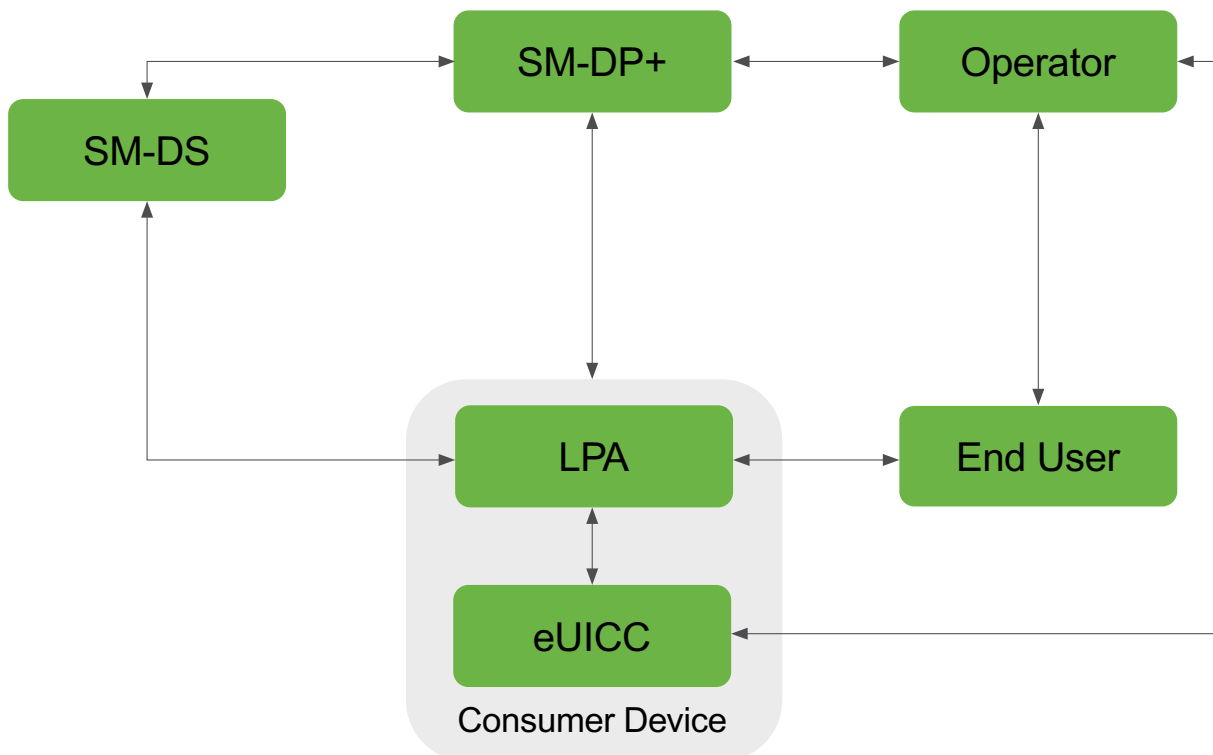


Figure 2 – Simplified Diagram of GSMA eSIM Solution for Consumer (SGP.22) Architecture

## 2. Understanding the Drivers of SGP.32

The eSIM Consumer solution has also been widely deployed worldwide, and is supported today by hundreds of mobile operators, with hundreds of millions of devices available from major smartphone, wearable and laptop / PC manufacturers. This wide deployment is supported by rapidly growing adoption, with [TCA's market data](#) showing that consumer eSIM profile downloads increased by 109% in 2023.

### Addressing the Unique Considerations of the IoT

The growth of the IoT ecosystem, however, presents unique considerations and challenges that are not optimally addressed by the existing M2M and Consumer Specifications.

Two primary challenges are the growth of constrained IoT devices and integration complexity:

**Constrained IoT Devices** – As the IoT ecosystem grows to encompass new verticals and use-cases, there are an increasing number of IoT devices deployed that have limited bandwidth (network constrained), limited or no UI (UI constrained), and limited power (power constrained).

In particular, network constrained and UI constrained devices across the IoT ecosystem present significant challenges as they cannot be optimally managed using the existing GSMA Consumer and M2M Specifications. For example, the M2M Specification requires an SMS or HTTPS connection for profile downloads and management, which network constrained devices cannot support. Similarly, many IoT devices lack a UI to enable an end-user to trigger or approve a profile download. However, IoT devices used in the B2B context are typically managed remotely, without an end user operating the device locally.

**Integration Complexity** – A challenge associated with the M2M Specification is that it requires complex bilateral integration processes between service providers and the different operators (as secure links must be established between the SM-SR and SM-DP), which makes it difficult to switch profiles between providers. While this model is highly resilient and works for verticals such as automotive, it is unsuited for multiple IoT use-cases.

The Consumer Specification offers a more streamlined and scalable approach as there is no need for pre-established links between the device and the SM-DP+.

### Why a New eSIM IoT Specification was Needed

The industry has recognised that enhancing the eSIM infrastructure to meet specific IoT requirements is crucial. The combined limitations of IoT (UI, bandwidth and power) demand a simpler model that is dedicated to the IoT – ensuring high resiliency and scalability, necessitating less computing power on the device, using less radio resources, and requiring zero or very limited user interaction.

In response to this need, GSMA has worked with industry stakeholders to develop a third Remote SIM Provisioning model. The result is that there is a current version 1.2 of the eSIM IoT Technical Specification (SGP.32) published in June 2024. This will enable the first commercial products to be brought to market.



### 3. SGP.32: Key Features and Updates



Before exploring the changes introduced, it is important to note that SGP.32 is not a completely new approach. Rather, it marks an evolution of the Consumer Specification (SGP.22), which itself was an evolution of the M2M Specification. A design principle for the development of SGP.32 was to leverage the well established SGP.22 infrastructure with its existing ecosystem components (SM-DP+) in order to simplify and accelerate deployments. SGP.32 builds upon proven elements of both the consumer and M2M specifications to simplify the adoption and integration process for device manufacturers and operators, while introducing new components and features to address the specific challenges and considerations associated with managing constrained devices across various IoT and B2B fleet management use-cases.

Two new components are introduced:

**eSIM IoT Remote Manager (eIM)** – the eIM is a standardised, remote provisioning tool that enables profiles to be downloaded and managed on a single IoT device or – crucially – a fleet of devices without the need for direct end user interaction. The eIM can also communicate with any IoT device or SM-DP+, removing the need for complex and inflexible individual integrations.

**IoT Profile Assistant (IPA)** – within the Consumer Specification, the LPA enables users to download a profile from the SM-DP+. The IoT Profile Assistant (IPA) replaces the LPA and provides the functions that enable the eSIM to be remotely managed using the existing SM-DP+ platform infrastructure and eIM platform infrastructure.

The IPA can either reside on the device (IPAd) or on the eUICC (IPAE). Both the eIM and SM-DP+ are agnostic to either the IPAd or IPAE, allowing IoT device makers to select the most appropriate IPA option (IPAd or IPAE) based on their requirements and expertise.

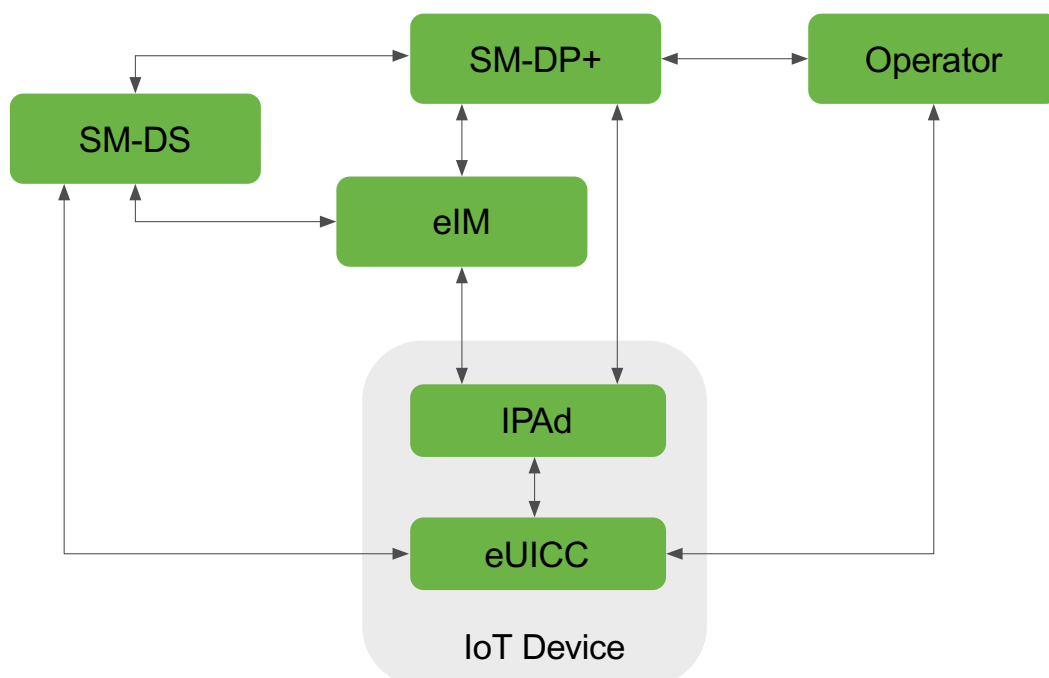


Figure 3 – Simplified Diagram of GSMA eSIM Solution for IoT (SGP.32) Architecture: IPAd

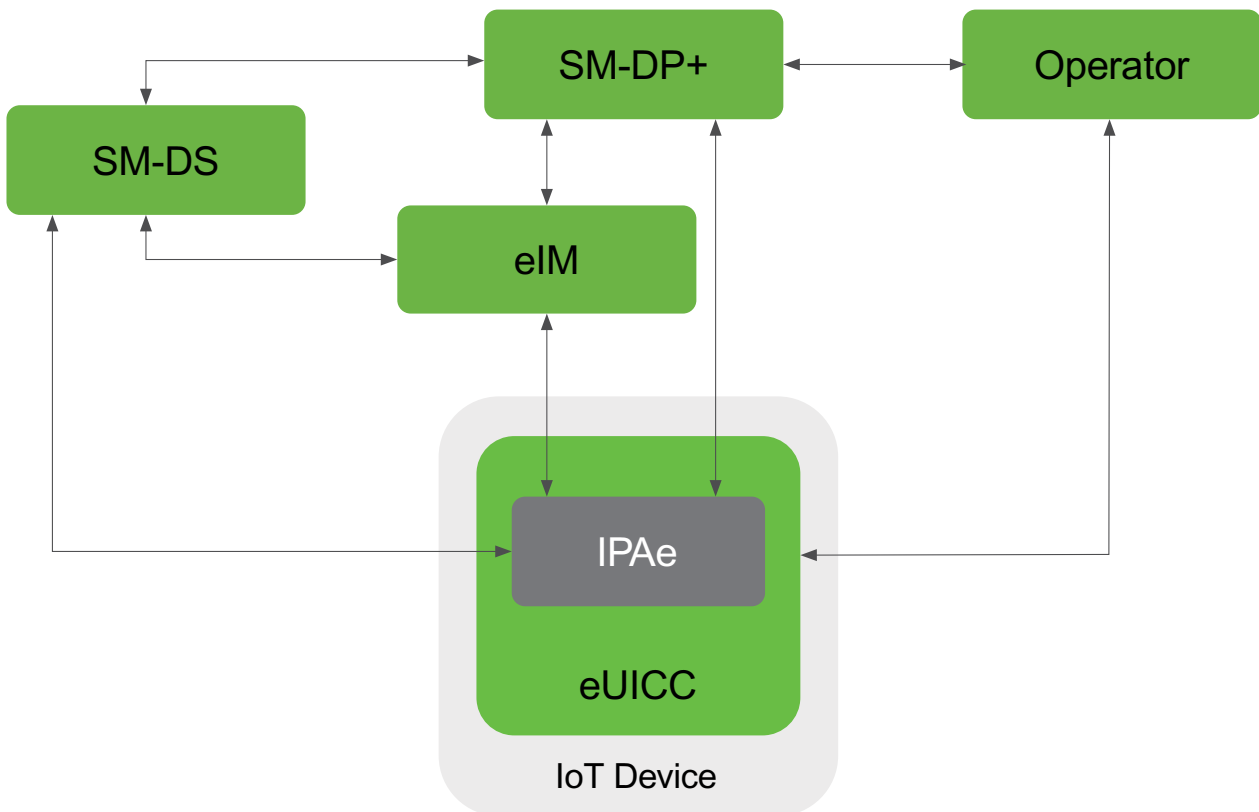


Figure 4 – Simplified Diagram of GSMA eSIM Solution for IoT (SGP.32) Architecture: IP Ae

**In addition to these new components, various other updates and additions have been made to address constrained IoT devices:**

**Lightweight communication protocols** – SGP.32 adds support for a wider number of lightweight, reliable and secure communication protocols to address network and power constrained IoT devices that cannot support SMS and HTTPs. Updates include the addition of Constrained Application Protocol (CoAP) as an alternative to HTTPs and the Datagram Transport Layer Security (DTLS) protocol as an alternative to the Transport Layer Security (TLS) protocol. Another option allowed by SGP.32 is the use of lightweight device management protocols (such as LwM2M) or lightweight publish-subscribe protocols (such as MQTT) over the air interface, for the transport of the eSIM management payload.

**Lightweight IoT Minimal Profile** – TCA's Interoperable Profile Package Specification – which is used in every eSIM deployed in the field – standardises the format used for the remote loading of subscriptions onto eSIMs across deployed devices. This enables mobile operators to load interoperable connectivity profiles in an eSIM, regardless of the SIM vendor.

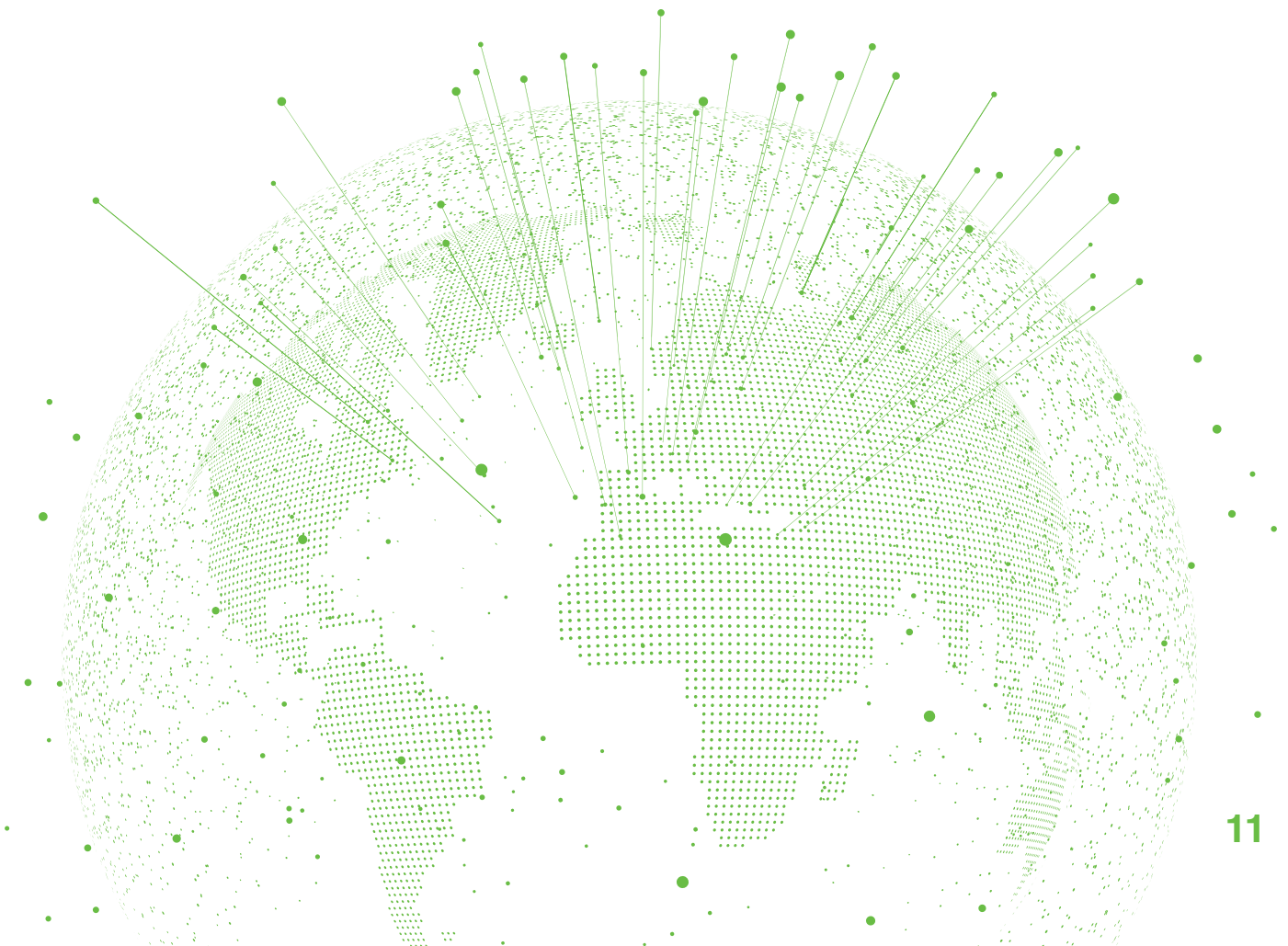
A key update in Version 3.3 of TCA's Interoperable Profile Package Specification is the definition of a 'lightweight' IoT minimal profile to address the challenge of remotely managing network constrained IoT devices. Profiles developed according to Version 3.3 can be as small as a few hundred bytes. This is in comparison to tens of kilobytes for those used for M2M or Consumer devices. This makes it possible to provision a profile even when bandwidth is very limited (e.g. Cat-M, NB-IoT). Given these benefits, Version 3.3 is referenced in SGP.32.

**Rollback and fallback mechanisms / emergency profile operation** – while SGP.32 can be seen as an evolution of the Consumer Specification, it also includes features from the M2M Specification to enable more reliable and resilient connectivity to meet the demands of IoT use-cases. In the event of no network connectivity after enabling a new profile, the ‘rollback mechanism’ reverts back to the previously enabled profile. In addition, the ‘fallback mechanism’ is executed when the device loses network connectivity through the enabled profile. This activates the fallback profile.

Another feature carried over from the M2M Specification is the ability to automatically switch to a single, dedicated profile in the case of an emergency.

**Connectivity Parameters** – as a legacy from the M2M specification, SGP.32 introduces a procedure to allow the device to retrieve the connectivity parameters from the eUICC. This is needed for constrained IoT devices which may not include the list of APN parameters for all mobile operators.

**Security** – SGP.32 reuses the existing security defined for M2M and Consumer: the SM-DP+ shall always be GSMA Security Accreditation Scheme (SAS) certified. The eUICC shall always conform to the security certification according to the eUICC for Consumer and IoT Device Protection Profile (SGP.25). As SGP.32 introduced a new element in the eIM, there is a need for security protocols between the eIM and the eUICC. The eUICC will only accept requests from authorised and authenticated eIMs. It is also possible to securely configure a new eIM in the eUICC (or remove an existing one). The GSMA Specifications introduce the option to include the eIM within the scope of SAS certification.



## 4. Understanding the Benefits of SGP.32 for IoT Use-Cases



When taken together, the new components and features introduced in SGP.32 deliver various benefits across IoT use-cases that leverage constrained devices. These include:



**Increased scalability and flexibility** – SGP.32 streamlines the deployment and remote management of large fleets of IoT devices across different regions and networks.

### Use-Case: Logistics and Transportation

A logistics operator deploying asset trackers in shipping containers across multiple routes can flexibly connect to different network providers across jurisdictions.



**Increased network coverage, reliability and resiliency** – SGP.32 features fallback / rollback mechanisms and as a result allows connectivity in an emergency situation.

### Use-Case: Automotive

An automotive manufacturer can access a wider number of connectivity options with less bilateral integration efforts compared to deployments using the M2M Specification.



**Constrained protocols** – SGP.32 is suitable for network constrained devices such as electricity meters and water meters. This is possible thanks to the use of CoAP / User Datagram Protocol (UDP) between the IoT device and the eIM.

### Use-case: Smart Metering

A utilities provider deploying smart meters to monitor electricity flows across its offshore windfarms can ensure continuous connectivity over the full lifespan of the device.



**State of the art security** – SGP.32 ensures the confidentiality, accuracy and integrity of the data received and transmitted by IoT devices. The solution reuses all the secure communications defined in the Consumer Specification and defines new protocols to secure the communication between the eIM and IPA/eUICC in terms of integrity, authenticity, and confidentiality.

### Use-Case: Smart Cities

A municipality deploying IoT sensors for critical infrastructure such as a traffic management system can ensure that data is not compromised by bad actors.



**Optimised IoT device production** – SGP.32 simplifies and streamlines IoT device production to accelerate time-to-market. The eUICC could be provided without any initial eIM or profile for maximum deployment flexibility. The specifications allow for them to then be added in the field.

**Use-Case: Global IoT Device Manufacturer**

A device manufacturer deploying products globally does not have to select an operator during production, removing the need for multiple production lines to address different geographies.



**Operational efficiency** – SGP.32 ensures operational efficiency through wireless connectivity in challenging terrains.

**Use-Case: IoT in Different Segments of the Oil and Gas Industry**

A network of physical objects integrated with remote sensors, surveillance systems, machine learning, and cloud connectivity is deployed across all operational stages, including devices under high-temperature and human-inaccessible areas within oil fields.



**Real-time monitoring** – SGP.32 ensures the seamless connectivity for instant feedback and timely intervention.

**Use-case: IoT in the Healthcare Industry**

Provides real-time data, enabling timely interventions and improved patient outcomes, alleviating the strain on healthcare practitioners and facilities.



**Feedback control system** – SGP.32 ensures seamless connectivity for automation of real-time data.

**Use-Case: IoT in Building Management and SCADA**

Wireless communication enables IoT devices to transmit data wirelessly for facilitating Supervisory Control and Data Acquisition (SCADA) systems and enabling the implementation of closed-loop feedback control systems.

## 5. Testing and Compliance

The Consumer and M2M specifications are supported by GSMA eSIM Security Certification and Compliance Processes. These comprehensive, well-established certification and compliance schemes require that eSIM solutions are subjected to thorough assessment and testing to ensure they are just as secure and interoperable as traditional SIM. This promotes confidence for operators, device manufacturers and service providers.

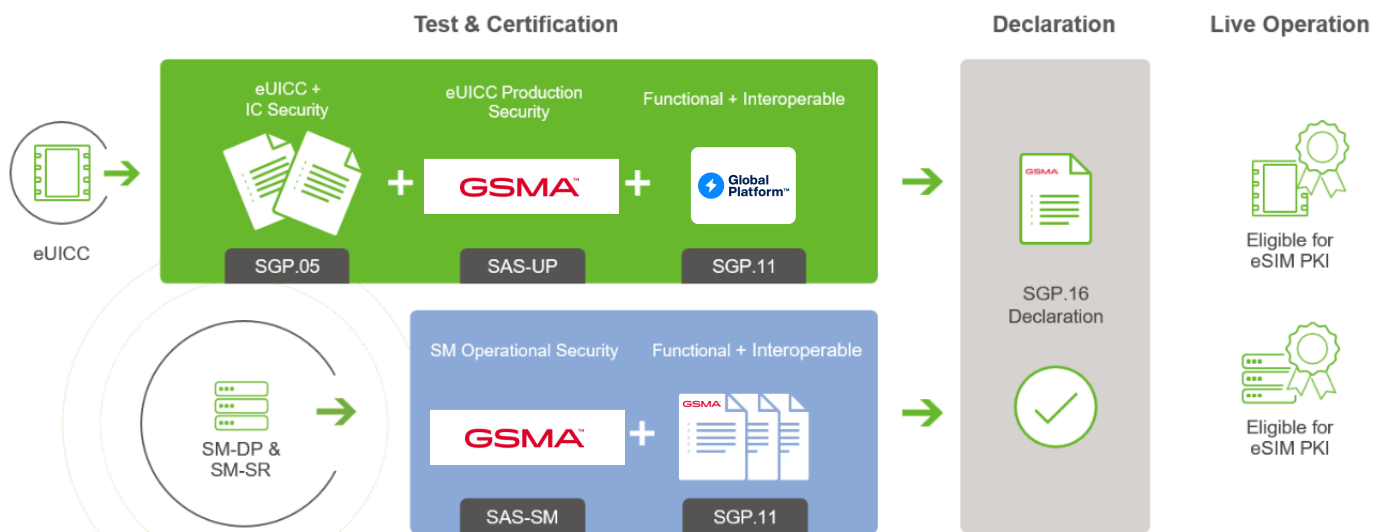


Figure 5 – Compliance Overview: M2M

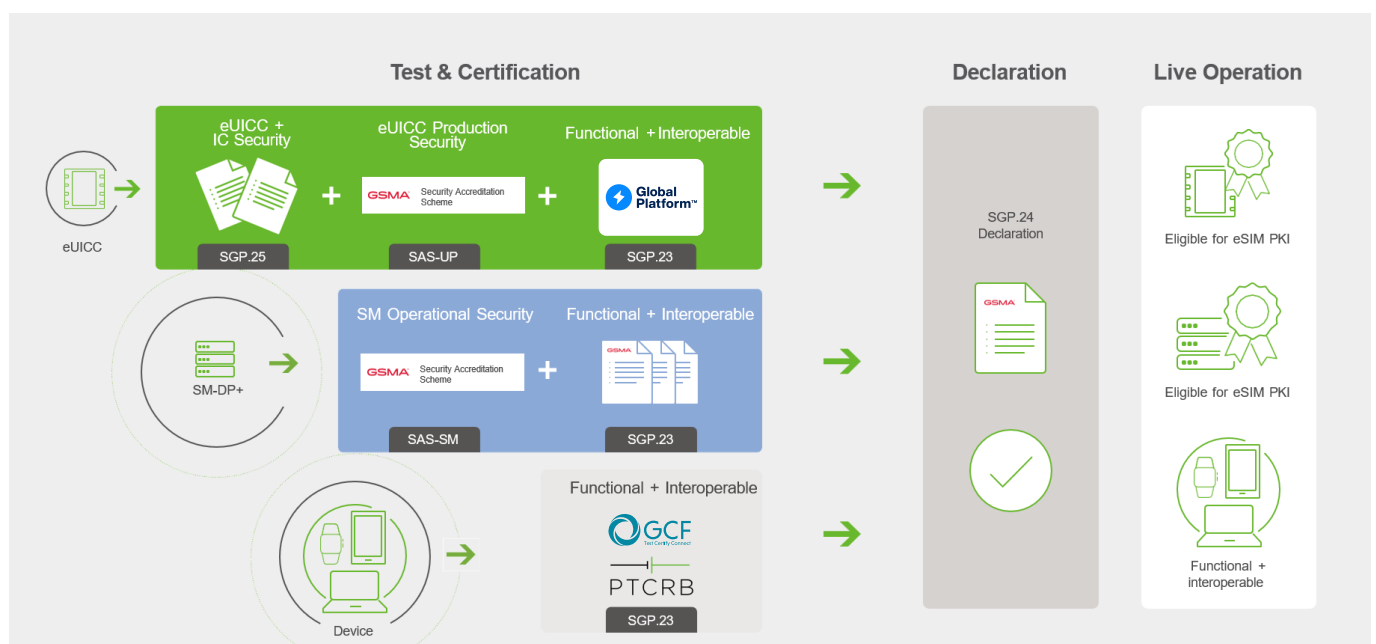


Figure 6 – Compliance Overview: Consumer

## 5. Testing and Compliance

Work has progressed on the associated test specifications and compliance programme for SGP.32 with the publication of the eSIM IoT Test Specifications (SGP.33) in January 2024:

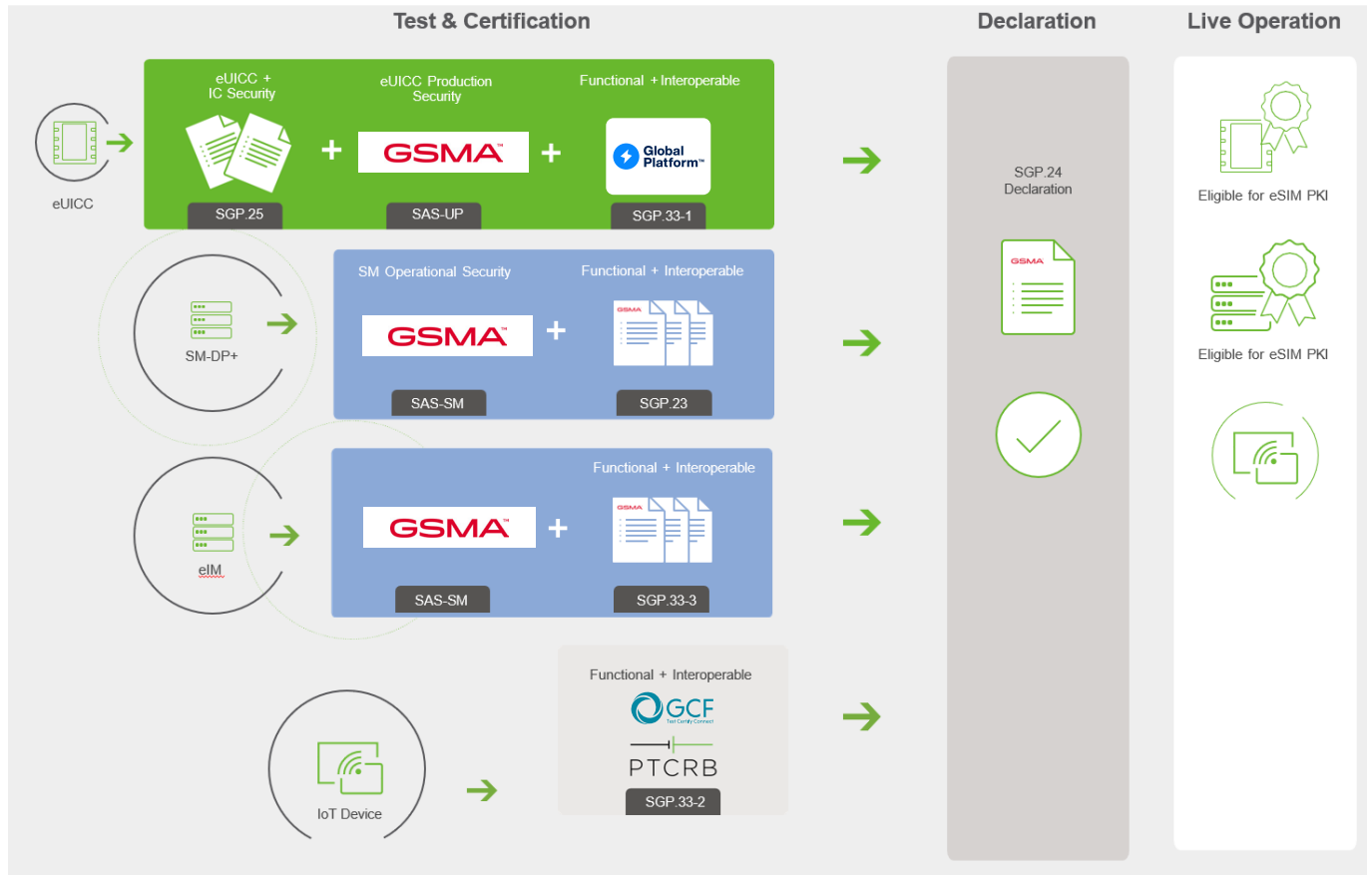


Figure 7 – Compliance Overview: IoT

### Interoperability Considerations: A Closer Look at Functional Certifications

Interoperability is critical for the eSIM ecosystem to enable connectivity across and between IoT devices and the enabling infrastructure. To realise the benefits of interoperability, GSMA has applied the following principles and processes:

- An eUICC / IoT device should work with any SM-DP+ and SM-DS, regardless of the supplier or operator who manages it. eUICCs and devices also need to be future-proofed so they can work with SM-DP+ and SM-DS's installed after deployment.
- Conversely, an SM-DP+ hosted by an operator should be able to create profiles for any eUICC with known capabilities, regardless of the eUICC manufacturer.
- Compared to the traditional SIM, achieving eUICC interoperability is more challenging. This is because a SIM operating system and the profile it hosts are designed by one SIM manufacturer selected by the operator, and functionally certified by the operator.

## 5. Testing and Compliance

The unprecedented interoperability level required by the IoT eUICC can only be reached by the following multi-faceted industry collaboration:

- GSMA, in addition to defining core eSIM specifications, designs and maintains the interoperability test specifications for the eSIM servers (SM-DP+, SM-DS), eIM, IoT devices and eUICCs.
- GlobalPlatform establishes the eUICC Functional Certification Programs based on the GSMA and TCA test specifications for eUICC. This includes the IP Ae.
- Global Certification Forum (GCF) and PTCRB establish Functional Certification Programs for the IoT devices in the eSIM ecosystem based on GSMA test specs for the IP Ad.
- TCA designs the eUICC Interoperable Profile Package Test Specifications, with the objective of testing if an operator profile is correctly interpreted and loaded onto an eUICC.

### Test Tools for IoT Products

Test cases and test tools for IoT eUICCs are validated by GlobalPlatform, based on the test specifications provided by GSMA and TCA. GlobalPlatform arranges a Test Fest where this validation happens. Different test tool vendors and eUICC manufacturers participate in the Test Fest, cross-test their products and compare the results. The outcome of the Test Fest is the validated test suite and the validated test tools.

The test cases and test tools for testing the IP Ad are validated by GCF and PTCRB. In GCF, the test tool vendors submit the results of test executions based on two products. Experts validate the results and if successful the test tool is validated.

Tools simulating RSP servers, eIM and OTA components enable the following testing scenarios in a lab environment:

- Provisioning and management of profiles on an IoT eUICC.
- Remote file and application management on an IoT eUICC.
- Scanning the IoT eUICC file system, security domains and applications.
- Verification of the IoT eUICC file system, security domains and applications against the content of a profile.



## 6. Conclusion: Preparing for SGP.32



The publication of a dedicated standard for remotely provisioning and managing IoT devices is a game-changing development that promises to accelerate the adoption of eSIM technology across established and emerging IoT use-cases.

Interoperability testing efforts have already started among SGP.32 technology vendors. Compliance programmes for IoT eSIMs will be ready by the end of 2024. It is expected that the first GSMA certified solutions will be launched in 2025, and that over half of active eSIMs across IoT deployments will be compliant with the new specification by 2028. ([Source: Kaleido Intelligence](#))

As adoption starts to build, promoting and maintaining security and interoperability must be a priority. There are a vast number of potential IoT use-cases and, to reflect this diversity, SGP.32 is intentionally very flexible to allow for multiple implementation options and various deployment scenarios. However, there needs to be a consistent baseline across all deployments to ensure the benefits are fully realised.

In response, TCA is committed to bringing together leading industry stakeholders to ensure SGP.32 deployments are underpinned by a strong foundation of security and interoperability. It is doing this by shaping the ongoing standardisation and enhancement of eSIM technology and the supporting infrastructure, continuing to be a key contributor to GSMA to further guide and support the development of its eSIM-related specifications and testing processes.

## 7. About Trusted Connectivity Alliance



Trusted Connectivity Alliance (TCA) is a global industry association working to enable trust in a connected future.

The organisation evolved from the SIMalliance, reflecting the continued expansion of the global SIM industry and the need for broader collaboration. Its members are leading providers of secure connectivity solutions for consumer, IoT and M2M devices. This spans Tamper Resistant Element (TRE) technologies including SIM, eSIM, integrated SIM, embedded Secure Element (eSE) and integrated Secure Element (iSE), as well as hardware and software provisioning and other personalisation services.

**TCA members are:**



[www.trustedconnectivityalliance.org](http://www.trustedconnectivityalliance.org)