TRUSTED CONNECTIVITY ALLIANCE

IoT eSIM (SGP.32): A Technical Guide

Version 1.0
October 2026

Copyright © 2026 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. References 05
2. Abbreviations 06
3. Key Definitions 07
4. Introduction 09
5. Understanding the eSIM for IoT Architecture, Key Entities, Concepts and Data Exchanges 10
   - 5.1. SGP.32 Architecture 10
   - 5.2. Key Responsibilities of the eIM 11
   - 5.3. Key Responsibilities of the IPA 12
     - 5.3.1. IPA in the IoT Device (IPAd) 13
     - 5.3.2. IPA in the eUICC (IPAe) 13
     - 5.3.3. Co-existence of IPAd and IPAe 13
   - 5.4. Key SGP.32 Concepts 13
   - 5.5. Key Data Exchanges 14
6. SGP.32 – Key Deployment Options and Considerations 15
   - 6.1. Profile Download Modes 15
   - 6.2. eIM Packages 17

Contents

6.3. eUICC Packages 17

6.3.1. Structure of eUICC Package 18

6.3.2. Structure of Signed eUICC Package 18

6.4. Profile State Management Operations 18

6.4.1. Structure of eUICC Package Containing PSMOs 18

6.4.2. Enable Profile 19

6.4.3. Disable Profile 19

6.4.4. Delete Profile 19

6.4.5. Configure Immediate Profile Enabling 19

6.4.6. Setting and Unsetting the Fallback Attribute for the Target Profile 20

6.5. eIM Configuration Operations 20

6.6. Connectivity Parameters 21

7. Security and Certification 22

7.1. eUICC Certification 22

7.2. eIM Certification 23

7.3. IPAd Certification 24

7.4. Opportunities to Increase Interoperability 24

8. Conclusion and Next Steps 25

9. About Trusted Connectivity Alliance 25

1. References

GSMA	SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification Version 4.3	January 2023
	SGP.22 RSP Technical Specification Version 2.7	April 2026
	SGP.24 RSP Compliance Process Version 2.7	July 2025
	SGP.25 eUICC for Consumer and IoT Devices Protection Profile Version 2.1	February 2025
	SGP.31 eSIM IoT Architecture and Requirements Version 1.3	May 2026
	SGP.32 eSIM IoT Technical Specification Version 1.3	May 2026
	SGP.33-1 eSIM IoT Test Specification for the eUICC Version 1.2	January 2025
	SGP.33-2 IPA Test Specification Version 1.2	January 2025
	SGP.33-3 eUICC IoT Manager Test Specification Version 1.2	January 2025
TCA	eUICC Profile Package: Interoperable Format Technical Specification Version 3.4.1	May 2025

2. Abbreviations

3GPP	**3**rd **G**eneration **P**artnership **P**roject
APN	**A**ccess **P**oint **N**ame
BIP	**B**earer **I**ndependent **P**rotocol
CoAP	**C**onstrained **A**pplication **P**rotocol
eCO	**e**IM **C**onfiguration **O**peration
eIM	**e**SIM **I**oT Remote **M**anager
eIMID	**eIM Id**entifier
eSA	**GSMA e**UICC **S**ecurity **A**ssurance Scheme
EUM	**eU**ICC **M**anufacturer
EUCC	**EU C**ybersecurity **C**ertification Scheme on Common Criteria
FQDN	**F**ully **Q**ualified **D**omain **N**ame
GCF	**G**lobal **C**ertification **F**orum
GSMA	**G**lobal **S**ystem for **M**obile Communications **A**ssociation
ICCID	**I**ntegrated **C**ircuit **C**ard **Id**entifier
IoT	**I**nternet **o**f **T**hings
IPA	**I**oT **P**rofile **A**ssistant
IPAd	**I**oT **P**rofile **A**ssistant in the **d**evice
IPAe	**I**oT **P**rofile **A**ssistant in the **e**UICC
LPA	**L**ocal **P**rofile **A**ssistant
LwM2M	**L**ight**w**eight **M**achine-**to**-**M**achine
MQTT	**M**essage **Q**ueuing **T**elemetry **T**ransport
PIR	**P**rofile **I**nstallation **R**esult
PSMO	**P**rofile **S**tate **M**anagement **O**peration
PTCRB	**P**CS **T**ype **C**ertification **R**eview **B**oard
OMA	**O**pen **M**obile **A**lliance
OTA	**O**ver **t**he **A**ir
RSP	**R**emote **S**IM **P**rovisioning
SAS-SM	GSMA **S**ecurity **A**ccreditation **S**cheme for **S**ubscription **M**anagement
SAS-UP	GSMA **S**ecurity **A**ccreditation **S**cheme for **U**ICC and eUICC **P**roduction
SM-DP+	**S**ubscription **M**anager **D**ata **P**reparation +
SM-SR	**S**ubscription **M**anager **S**ecure **R**outing
TCA	**T**rusted **C**onnectivity **A**lliance
TRE	**T**amper **R**esistant **E**lement

3. Key Definitions

Term	Definition
Connectivity Parameters	A set of data (e.g. APN, login, password) required by the IPA to open a communication channel (e.g. HTTPS, CoAP) on a dedicated network.
eIM Configuration Data	The data to be used by the eUICC to identify and authenticate the eIM commands.
eIM Configuration Operation	An operation related to eIM Configuration Data in the eUICC (e.g., add eIM Configuration Data, update/remove eIM Configuration Data).
eSIM IoT Remote Manager	Responsible for remote management of the eUICC and indirect Profile download.
eSIM	The generic term applied to devices and eUICCs that support Remote SIM Provisioning as defined by GSMA. This term is usually used to refer to the eUICC. The term originates from “embedded SIM”.
ESep	A logical interface between an eIM and an eUICC.
ESipa	A communication interface between an eIM and an IPA.
eUICC	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”.
eUICC Package	A package generated by the eIM in order to be executed by the eUICC. It’s either Profile State Management Operation or eIM Configuration Operation.
Fallback Profile	The Profile to be enabled if the IoT Device detects a permanent loss of connectivity using the currently enabled Profile.
IoT Profile Assistant	An entity that provides functions that enable the eUICC to be managed by the eIM and to be provisioned by the SM-DP+ for profile download.

Term	Definition
Operator	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.
Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing connectivity to mobile networks.
Profile State Management Operation	An operation related to the state update of a Profile on the eUICC (e.g., enable Profile, disable Profile, delete Profile, list Profile(s) information).
Remote SIM Provisioning	The process of downloading, installing, enabling, disabling, and deleting a Profile on an eUICC in accordance with GSMA specifications.
Rollback Mechanism	Re-enables the previously enabled Profile in case no communication between the eIM and IPA can be established right after profile enabling.
SIM	A generic term for the UICC and application(s) 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.
SIM Card	A SIM that has one of the physical plug-in form factors as defined by ETSI (i.e. plug-in, micro-SIM, nano-SIM).
Tamper Resistant Element	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.
UICC	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.

4. Introduction

The development of GSMA's eSIM IoT Technical Specification (SGP.32) is a transformative development in global connectivity. By introducing a dedicated Remote SIM Provisioning (RSP) model tailored for IoT devices, SGP.32 promises to further accelerate the adoption of eSIM technology across established and emerging IoT verticals.

The industry is now working to turn this promise into reality. Trusted Connectivity Alliance (TCA) market data shows that the market transition to SGP.32 is already well underway, evidenced at this early stage of deployment by a strong increase in the number of eSIM Subscription Manager (SM-DP+) platforms that support profile downloads in accordance with the specification.[1]

The Need for Interoperability as Adoption Builds

In the white paper *"Realising the Benefits of GSMA's eSIM IoT Specification"*[2], TCA explored the marketplace drivers behind SGP.32. To support understanding of the implications and applications, TCA also examined why the growing deployment of a vast range of IoT devices presents unique considerations that are not optimally addressed by GSMA's existing M2M and Consumer RSP technical specifications (SGP.02 and SGP.22), and why new components and updates were introduced in SGP.32 to simplify the deployment and management of IoT devices at scale.

But as marketplace adoption of SGP.32 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 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.

To support this need for interoperability, there is also demand across the industry for more technical guidance. As with any new major technology initiative in the early stages of adoption, ecosystem stakeholders are still working to understand how to best optimise deployments to meet their specific requirements.

This technical paper aims to address this collective industry need. Developed by TCA's IoT RSP Working Group[3] – which comprises leading industry experts directly involved in the development of the SGP.32 specification within GSMA – it aims to support all interested stakeholders by:

- Providing an overview of the SGP.32 ecosystem, outlining the considerations posed by architectural changes, the introduction of new entities, new and inherited concepts, and key data exchanges.
- Offering technical guidance to address key operations and deployment scenarios.
- Explaining the role of the supporting testing and compliance programme, and the potential for future enhancements to the SGP.32 testing infrastructure.

Target Audience

It should be noted that this document is mainly addressed to actors interested in deploying an IoT service using 3GPP network technology (e.g. 3G, 4G, 5G), which in some cases could be a constrained network technology (e.g. Narrow Band 4G network for IoT [NB-IoT] or Reduced Capabilities 5G network for IoT [RedCap]) and the device has limited or no user interface (UI).

Applicable Versions of IoT eSIM

This document is based on SGP.32 v1.3, the latest version recently published by GSMA which defines technical implementation for the requirements defined in SGP 31 v1.3. Note that v1.3 implements technical enhancements on top of v1.2, which was the first version of the specification used in deployed products in the market.

[1] Trusted Connectivity Alliance, *Trusted Connectivity Alliance Members Confirm Acceleration of Global eSIM Growth in 2025,* March 2026

[2] Trusted Connectivity Alliance, *Realising the Benefits of GSMA's eSIM IoT Specification (SGP.32),* September 2024

[3] Trusted Connectivity Alliance, *Working Groups,* June 2026

5. Understanding the eSIM for IoT Architecture, Key Entities, Concepts and Data Exchanges

GSMA has now defined multiple specifications for eSIM technology, enabling RSP across different device categories. The following specifications have evolved in line with market needs and technological advancements:

- **eSIM for M2M devices (2014)** – SGP.02
- **eSIM for Consumer devices (2016)** – SGP.22
- **eSIM for IoT devices (2024)** – SGP.32

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 (SGP.02). A design principle for the development of SGP.32 was to leverage the well-established SGP.22 infrastructure and build upon proven elements of both the Consumer and M2M Specifications to simplify the adoption and integration process for device manufacturers and operators.

The following sections examine how this approach has impacted the architecture, ecosystem entities, key concepts, and data exchanges.

5.1. SGP.32 Architecture

As the RSP specifications evolved to meet emerging needs and technologies, so too did the architecture of the ecosystem. Most notably, SGP.22 differs substantially from SGP.02, primarily because consumer devices such as smartphones, tablets, and wearables have a UI to enable the end-user to trigger actions. This is why SGP.22 defines a user-initiated mechanism for Profile management, where users download (e.g., by scanning a QR code or using an app) and enable Profiles through the device interface.

The widespread adoption of SGP.22 makes it a highly popular and compatible standard across a vast range of devices and service providers. That is why, from an architectural point of view, SGP.32 is primarily based on SGP.22.

While the SGP.32 architecture marks an extension of SGP.22, it is also designed to address the unique challenges of RSP for IoT devices that are either network or UI-constrained. To address these challenges, it introduces significant advancements, including server-initiated Profile management which allows Profiles to be remotely managed and updated without requiring direct user interaction with the device. This feature is crucial for large-scale IoT deployments comprising unattended devices, demanding bulk Profile management with seamless Profile switching.

A modular architecture is achieved with the introduction of two new roles – the eSIM IoT remote Manager (eIM) and IoT Profile Assistant (IPA) – that gives IoT service providers and IoT device owners control over RSP.

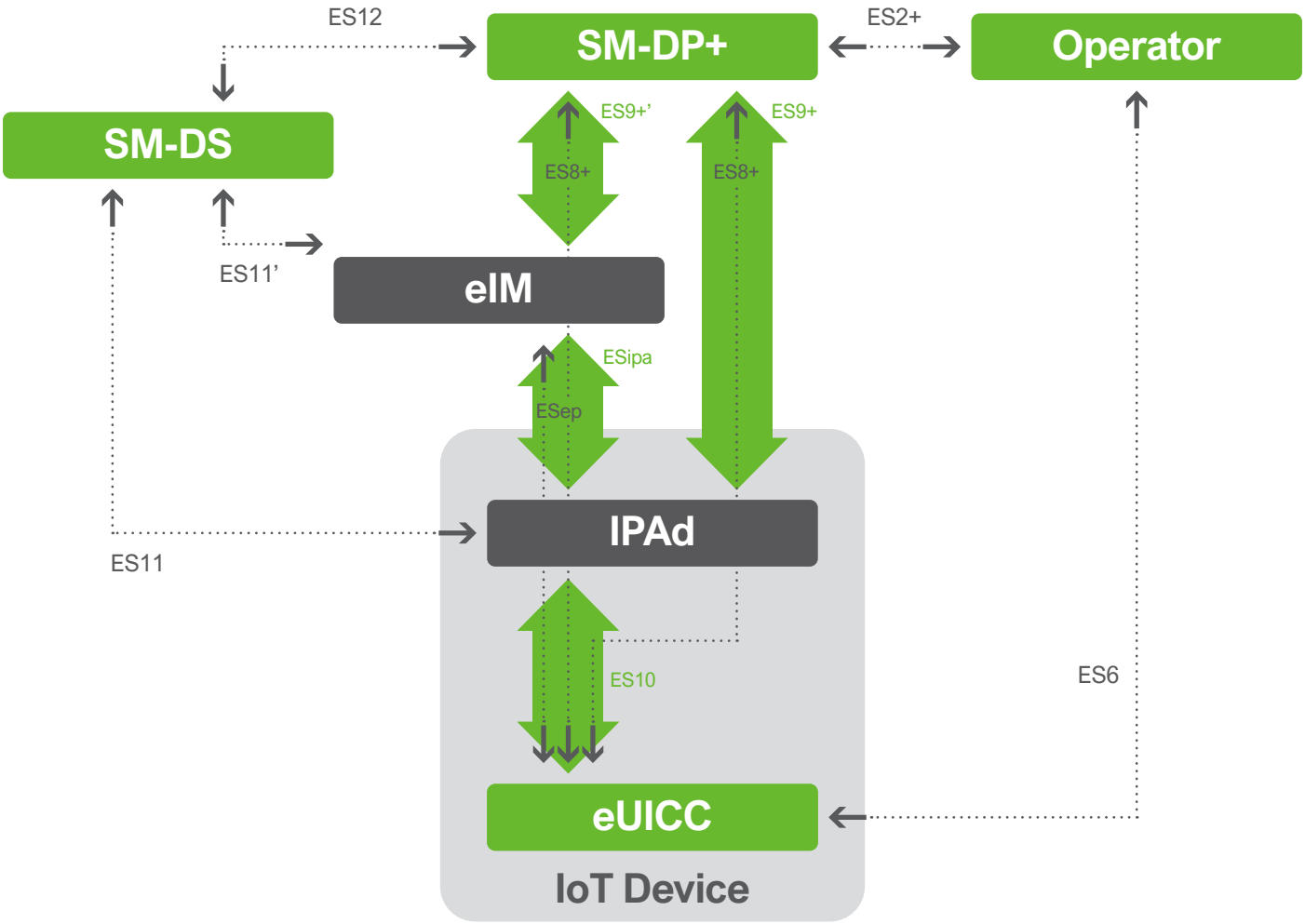


Figure 1. SGP.32 high level architecture with IPA in the device (see section 5.3.1)

The above diagram shows how SGP.32 introduces the new eIM and IPA entities, while also reusing elements from the Consumer eSIM architecture, namely the SM-DP+, which is the entity that prepares the eSIM Profile of an operator to be downloaded to the eUICC.

It should be noted that the SM-DS was added mainly for legacy reasons, but it may not be used in the context of IoT. This is because the role of the SM-DS is to allow the IoT device to find the right SM-DP+, but this role could be easily achieved by the eIM as it can already connect to both the IoT device and the SM-DP+.

5.2. Key Responsibilities of the eIM

The eIM is a central orchestrator in the SGP.32 architecture, handling the complexities associated with managing a large number of eUICCs in IoT environments. It acts as a remote control entity for Profile management operations and eUICC configuration management, especially when the IoT device or its IPA has limited capabilities.

The key responsibilities of the eIM are:

Secure communication with the IPA

- Communicating with the IPA over the ESipa interface (the communication interface between the eIM and the IPA).
- Sending signed packages over the ESep interface to the eUICC for execution through the IPA. (See section 6.3).
- Managing execution results and notifications from the IPA and eUICC.

Profile State Management Operations (PSMOs)

- Enabling, disabling, deleting a Profile.

eIM Configuration Operations (eCOs)

- Adding, updating, or deleting eIM Configuration Data – which contains the eIM identifier and credentials – on the eUICC.

Fallback Profile Selection

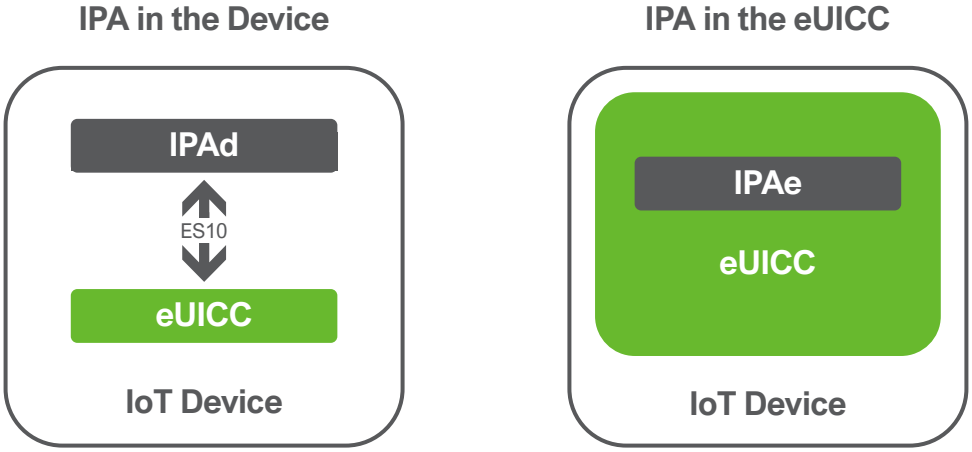
- Supporting configuration of Fallback Profiles. (See section 6.4.6).

Indirect Profile Download

- Acting as a proxy between the IPA and the SM-DP+ when the device cannot connect directly to the SM-DP+. (See section 6.1.2).

5.3. Key Responsibilities of the IPA and Deployment Models

The IPA, similar to the Local Profile Assistant (LPA) defined in SGP.22, facilitates the management of profiles and bridges the communications between the eIM and the eUICC. SGP.32 supports two IPA configurations – IPAd and IPAe.



5.3.1. IPA in the IoT Device (IPAd)

The IPA is implemented in the device's firmware or OS and communicates with the eUICC via specified interfaces in SGP.32. This is suitable for devices with some processing and networking capabilities.

5.3.2. IPA in the eUICC (IPAe)

The IPA is embedded within the eUICC. As this reduces dependency on the device OS, it is ideal for ultra-constrained devices or those with limited software flexibility. Note that the IPAe is covered by the security evaluation of the eUICC; making it highly-secure and suitable for sensitive use-cases.

5.3.3. Co-existence of IPAd and IPAe

The IoT device can select one configuration to use depending on the deployment scenario. If the IPAd is absent, however, the IPAe is automatically activated if supported by the eUICC.

5.4. Key SGP.32 Concepts

As noted previously, SGP.32 is a hybrid solution that integrates concepts from its Consumer and M2M predecessors, while introducing new ones to improve Profile management and address the specific needs of the IoT ecosystem. This section provides an overview of these key concepts.

5.4.1. Concepts Inherited from SGP.22

SGP.32 is predominantly based on SGP.22 and inherits many of its concepts. These are outlined below, with new considerations introduced in SGP.32 included for reference:

- **Profile Download:** This is the standardised mechanism to securely provision an operator subscription (Profile) to the eUICC. How operators can construct an interoperable Profile is defined in TCA's eUICC Profile Package: Interoperable Format Technical Specification. For security reasons, the Profile download procedure in SGP.32 is defined to provide authenticity, confidentiality and integrity between the eUICC and SMDP+, reusing the proven concepts defined in SGP.22.
- **Means to get eUICC information:** Retrieve information about the eUICC configuration and supported optional features. This will allow the SM-DP+ to verify the eligibility of the eUICC and prepare a suitable Profile package.
- **Profile State Management Operations:** See section 6.4 for a detailed explanation of the new considerations introduced in SGP.32.
- **eUICC Memory Reset:** Deletes selected subsets of the Profiles stored on an eUICC.

5.4.2. Concepts Inherited from SGP.02

SGP.32 also inherits concepts from the SGP.02. Again, these are outlined below, with the new considerations introduced in SGP.32 included for reference:

- **Fallback Mechanism:** A mechanism to automatically switch to a pre-designated Fallback Profile when connectivity is lost. In SGP.32, the fallback mechanism is triggered from the IPA. The operator allows a Profile to be used as a fallback. The eIM sets the fallback attribute of a Profile, identifying the Profile to be enabled by the fallback mechanism. A single Profile can have fallback attribute set at any given moment.
- **Rollback Mechanism:** A mechanism, which in SGP.32 is triggered from the IPA, to re-enable the previously enabled Profile in case no communication between the eIM and IPA can be established right after Profile enabling. (See section 6.4.2 for more information). Note this is different from fallback mechanism. Rollback happens immediately after the Profile enabling operation when it is not possible to connect to the network using the enabled Profile, whereas fallback happens later in the process if the device loses connectivity. In rollback, the eUICC re-enables the previously enabled Profile; where in fallback the eUICC enables the designated Fallback Profile.
- **Emergency Profile:** A special Profile that can be enabled in critical situations. Once an Emergency Profile is enabled, it remains enabled until the IoT device disables it. Note that the presence of this Profile is related to regulatory requirements in some regions. It is not mandatory for any eUICC. It is different from eCall, however, where the device performs an emergency call using the currently enabled Profile.

5.4.3. Concepts Defined in SGP.32

In addition to the introduction of the eIM and IPA, SGP.32 also defines new, dedicated procedures to address specific IoT considerations. These mainly include:

- **Indirect Profile Download:** In this case, the eIM acts as proxy between the IoT device and the SM-DP+ (See section 6.1 for more information).
- **New Protocols for Constrained Devices and Networks:** New protocols introduced for constrained devices where the eIM plays the role of protocol translator between constrained IoT devices and the deployed SM-DP+.
- **Immediate Enable:** Profiles can be activated immediately after download without further eIM or SM-DP+ involvement.
- **Association of eIMs with the eUICC:** A single eUICC can be associated with multiple eIMs simultaneously (See section 6.5 for more information).

5.5. Key Data Exchanges

An important concept to understand within SGP.32 is the communication ‘container’ between the eIM and IPA / IoT device, which is called an eIM Package.

An eIM Package can target either the IPA or eUICC. When it targets the eUICC, it contains an eUICC Package, which itself contains either Profile State Management Operations (PSMOs) or eIM Configuration Operations (eCOs). An eIM Package is also used to send the Profile Download Trigger Request.

PSMOs are used to manage the state of the profile, such as enabling, disabling, deleting a Profile, or retrieving information about a Profile (see section 6.4). eCOs are used to manage the eIM configuration, such as adding, deleting, updating an eIM, or retrieving the list of associated eIMs and their configuration data (see section 6.5).

6. SGP.32 – Key Deployment Options and Considerations

SGP.32 marks an important step forward for managing IoT deployments. However, the introduction of new ecosystem roles, concepts and exchanges – as well as the retention and repurposing of elements from both SGP.02 and SGP.22 – presents new considerations. It is also important to note that the SGP.32 specification is flexible, which allows for multiple implementation options and deployment scenarios depending on the use-case and requirements.

To aid industry understanding and promote secure and interoperable SGP.32 deployments, this chapter provides detailed explanations of the most relevant mechanisms for IoT solutions and, where relevant, offers implementation guidance to address common industry questions and challenges.

The specific areas addressed within this section are as follows:

- **Profile download options;** including direct Profile download and indirect Profile download.
- **eIM and eUICC Packages**
- **Key PSMOs;** including enable Profile, disable Profile, delete Profile, configure immediate Profile enabling; setting and unsetting fallback attribute.
- **Key eCOs;** focusing on eIM association.
- **Retrieve Connectivity Parameters**

6.1. Profile Download Modes

Depending on the IoT use case and the architecture of the IoT ecosystem, there are different ways to download the Profile into the eUICC. Depending on the entity that communicates to the SM-DP+, the procedure can either be an indirect Profile download or a direct Profile download.

6.1.1. Direct Profile Download

For a direct Profile download, the device (through the IPA) directly communicates with the SM-DP+. The download may be initiated by the eIM (via eIM Package) or the device / IPA (e.g. if the IPA processes the AC or using default SM-DP+). This procedure is very similar to the one defined for the Consumer architecture, so the device connects to the SM-DP+ using HTTPs through the ES9+ interface (see Figure 2).

6.1.2. Indirect Profile Download

For an indirect Profile download, the eIM triggers the download procedure. Moreover, the eIM acts as a proxy between the IPA and the SM-DP+ to perform the download. This option is recommended if the eIM centrally manages a fleet of devices, especially if they are power or network-constrained. As seen in the Figure 2 below, by using the indirect Profile download option, the device manages one single channel (with the eIM) for the download flow. In this model, HTTPs and the Constrained Application Protocol (CoAP) are two possible transport protocols between the IoT device and the eIM. It is also possible to use the underlying transport layer implemented by the IoT device to communicate with the eIM (e.g Lightweight Machine-to-Machine [LwM2M] and MQTT).

6.1.3. Considerations for Direct and Indirect Profile Download

For both direct and indirect download, the eIM relies on the IPA capabilities to select the correct download procedure and the communication details.

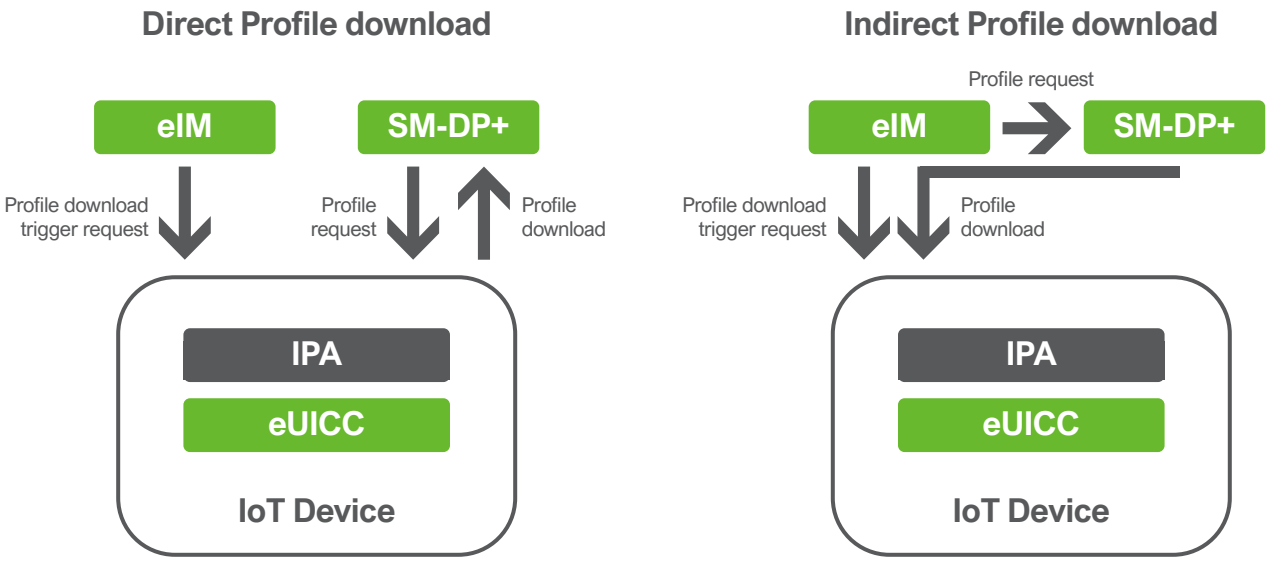


Figure 2: Comparison of direct and indirect Profile download

Depending on the way of retrieving the server address and the selected onboarding method, the download can be done:

- Via an activation code, which enables a controlled onboarding flow by delivering information to the eIM or device.
- Via the SM-DS, applicable to remote discovery onboarding scenarios.
- Via the default SM-DP+, which uses a pre-configured SM-DP+ address in the eUICC and allows immediate enabling of the installed Profile.

Depending on the device constraints and IPA capabilities, the download of the Profile can either be done via HTTPS only (used for a direct Profile download) or using the CoAP protocol (used for an indirect Profile download). The standard also allows other transport protocols to be 'piggybacked' when supported by the device, such as MQTT or LwM2M.

It is important to select the appropriate protocol to ensure the interoperability between the eIM and the IPA depending on the IoT device needs. In this case, the eIM may act as a protocol gateway to ensure full interoperability between the eUICC and SM-DP+.

In all of the cases above, the operator's backend prepares the Profile through its SM-DP+. Various verification steps are performed (like Mutual Authentication and Eligibility Check, as defined by SGP.32) which ultimately lead to sending the Profile Metadata and other significant information (for example: TransactionID, SM-DP+ signature) to the device in which the eUICC resides. The metadata is verified by the IPA (or in the case of an IPA with constrained capabilities, by the eIM), and after successful check the Profile is installed according to SGP.22 methods.

Once the eUICC has internally installed the Profile, it will generate a Profile Installation Result (PIR) that will be sent to the IPA. The IPA then forwards the relevant notifications to the notification receivers that were configured (for instance, the URL of the eIM or SM-DP+) to inform that the Profile is available in the targeted device. Once the notifications are successfully delivered and acknowledged, they are finally cleared from the IPA and the eUICC memory. The download procedure is then considered to be successfully completed and the eIM can perform PSMOs on the eUICC.

6.2. eIM Packages

An eIM Package contains a set of commands, generated by the eIM, to be executed either by the IPA or by the eUICC. When the package targets the eUICC, it is called an eUICC Package.

An eIM Package could be one of the following:

- An eUICC Package request: A request from the eIM to be executed by the eUICC. This is described in the following section.
- A data request to retrieve information related to the IPA or the eUICC. This could be, for example, to retrieve IPA capabilities or eUICC characteristics.
- An instruction to the IPA to start the Profile download procedure (Profile Download Trigger Request).
- Acknowledgements from the eIM to the IPA about the successful receipt of notifications.

6.3. eUICC Packages

An eUICC Package contains a set of commands, generated by the eIM, to be executed by the eUICC. As per the current version of SGP.32, it contains either Profile State Management Operations (PSMOs) or eIM Configuration Operations (eCOs). PSMO defines the operational remote mechanisms of Profile enabling, disabling, deletion, and configuration of fallback and immediate enabling features. This ensures efficient, secure, and policy-compliant management of profiles throughout the device lifecycle in UI-constrained and automated IoT environments. eCO defines the management of associated eIMs within the eUICC.

The eUICC package consists of either PSMOs or the eCOs. As per the current version of the specification, it is not possible to have PSMOs and eCOs in the same eUICC Package.

As introduced in section 6.4, PSMOs are initiated and controlled by an eIM. The overall workflow follows a chain of secure trust and interface communication:

1	2	3	4	5
The eIM prepares a signed data object known as an eUICC Package. This package contains either one or more PSMOs or one or more eCOs, each with a specific management command.	The eUICC package, end-to-end protected between the eIM and eUICC using the ESep interface, is transferred to the IPA via the ESipa interface. The IPA uses the IoT device interface (called ES10) to forward the package to the eUICC (see Figure 1).	The eUICC verifies the authenticity and integrity of the package by verifying the eIM's signature.	After execution, the eUICC creates a signed eUICC Package Result.	The result is returned to the IPA and then to the eIM. The eIM verifies the signature and matches the `eimId`, `eimTransactionId`, and `counterValue` to ensure authenticity and consistency.

Sections 6.4 and 6.5 provide an overview of key PSMOs and key eCOs, respectively.

6.3.1. Structure of eUICC Package

This request contains **`euiccPackageSigned`**, **`eimSignature`** (digital signature over the structure of **`euiccPackageSigned`**).

6.3.2. Structure of Signed eUICC Package

Any eUICC Package request generated by the eIM contains the eIM identifier to identify the eIM issuing the eUICC Package, the EID value to identify the target eUICC, the counter value used for anti-replay protection, and an optional transaction identifier to identify the session.

6.4. Profile State Management Operations

6.4.1. Structure of eUICC Package Containing PSMOs

All PSMOs are initiated when the eUICC receives a signed eUICC Package. Upon successful validation of the eIM signature, EID, and counter value, the eUICC identifies the target Profile using the provided ICCID.

PSMOs can include enable Profile, disable Profile or delete Profile (and are described in more detail in the following sections). It might also contain a request to list the different installed Profiles and their status.

Additional operations are also defined related to the fallback, rollback, and immediate Profile enabling.

If a **`rollbackFlag`** is set within the 'Enable Profile' command, the IPA can rollback to the previously enabled Profile if connectivity cannot be established with the new Profile.

To activate immediate Profile enabling – which means the eIM does not need to send an 'Enable Profile' command after the Profile is downloaded – the **`immediateEnableFlag`** must be present in the **`configureImmediateEnable`** command. command. To use immediate Profile enabling, the default SM-DP+ must be configured in the eUICC.

The **`setFallbackAttribute`** / **`unsetFallbackAttribute`** command configuration will designate the Profile that can be used as a Fallback Profile.

6.4.2. Enable Profile

The operation proceeds only if the Profile is in the “disabled” state.

If all conditions are met, the Profile status is marked as “to be enabled”, and any currently enabled profile is marked “to be disabled”. The eUICC generates a signed execution result indicating success or failure of the operation. The status will be effective at the end of the execution of all the PSMOs within the eUICC Package.

An additional feature is the ‘Enable Profile with Rollback’ mechanism, which extends the basic ‘Enable Profile’ procedure by allowing the eUICC to revert to the previously enabled Profile if needed.

In this case, before switching Profiles, the eUICC checks whether the use of the rollback mechanism is permitted. It then confirms that the target Profile is in a disabled state and there is a valid Profile currently enabled or marked to be disabled.

Upon validation, the system designates the target Profile “to be enabled”, the currently active one “to be disabled”, and records rollback context that allows returning to the previous Profile. This includes a reference to the disabled Profile and a flag authorising rollback.

A signed execution result is generated to indicate the outcome of the operation, including any errors such as missing rollback conditions or state mismatches.

6.4.3. Disable Profile

The command only proceeds if the Profile is currently in the “enabled” state. If the Profile is not found, or is not enabled, or if an enable or disable command has already been processed in the same package, the procedure results in a failure with the corresponding error.

When successful, the Profile is marked “to be disabled,” and a signed execution result is generated to reflect the outcome of the operation.

To maintain connectivity, a “Disable” command needs to be followed by an “Enable” command in the same eUICC Package.

6.4.4. Delete Profile

The Profile may only be deleted if it is in the “disabled” or “to be disabled” state. The Profile cannot be marked as “to be enabled” or referenced by the rollback or fallback mechanism. If those conditions are not met, the procedure results in a failure with the corresponding error.

On success, the profile is marked either “to be deleted” or “to be disabled and deleted,” and a signed execution result is generated and stored by the eUICC. The deletion of provisioning or test profiles is implementation-dependent and may not be supported.

6.4.5. Configure Immediate Profile Enabling

If the `immediateEnableFlag` is present and immediate enabling is not yet active, the feature is activated. If the flag is absent and immediate enabling is currently active, it is deactivated.

In all other cases, the current state remains unchanged. Additionally, if the **defaultSmdpOid** and/or **defaultSmdpAddress** are provided, they are stored for use in validating SM-DP+ identity during future profile downloads. The default address, if stored, is also made available for retrieval from the eUICC configuration.

A signed execution result is generated by the eUICC to indicate the success or failure of the operation.

6.4.6. Setting and Unsetting the Fallback Attribute for the Target Profile

The eUICC checks if it supports the Fallback Mechanism; if not, the operation is terminated with an error.

The eUICC then attempts to locate the Profile by the ICCID. If the Profile is found and already has the Fallback Attribute set, the operation completes successfully.

If not, the eUICC verifies that fallback is allowed (**fallbackAllowed** flag = TRUE) and that the Profile is not the Emergency Profile (**ecallIndication** = TRUE). The procedure also checks whether another Profile is currently marked as fallback. If a Fallback Profile exists and is enabled, the command fails. If it is disabled, the attribute is removed from the old Fallback Profile and assigned to the new one.

A signed execution result is generated by the eUICC to indicate the success or failure of the operation.

If the eUICC cannot find a Profile with the Fallback Attribute set, the operation will fail with a **noFallbackAttribute** error. If a Fallback Profile is present, its state is evaluated.

On successful completion of the **unsetFallbackAttribute** command, no Profile remains designated as the Fallback Profile, and the signed execution result is stored on the eUICC.

6.5. eIM Configuration Operations

An eIM needs to be associated to an eUICC to be authorised to manage it. Association is the process of adding the eIM configuration data to the eUICC, after verifying its compatibility with the target eUICC and IoT device. The eIM configuration data should include at least the eIM identifier and public key(s). Once configured at the eUICC level, this eUICC will trust any command sent by this eIM and signed by the eIM private key.

It is possible to associate several eIMs to a single eUICC. However, the communication order and priority with the different eIMs is not specified today in SGP.32 and it is up to the IPA logic to select the target eIM(s). Depending on market needs, this may be clarified in future versions of the SGP.32 specification.

The first eIM configuration may be loaded into the eUICC during eUICC manufacturing by the EUM. The eUICC may also be manufactured without any initial eIM. In this case, the first eIM is associated by the IPA by calling the “Add initial eIM” function. How the IPA receives the eIM configuration data to be set in the eUICC is OEM specific.

After the first eIM association, all further changes to the eIM configuration in the eUICC must always be done by an associated eIM. It is then possible to add a new eIM, remove an existing eIM, or update an existing eIM. An eIM swap can be performed by adding an eIM from the current eIM, followed by removing the previous eIM from a request by the newly associated eIM.

Note that the specification provides an option for the IPA to reset the eUICC by deleting all the eIM configuration data. The IPA can then re-add the first eIM by calling the “Add initial eIM”.

6.6. Connectivity Parameters

In order to communicate with the eIM and the SM-DP+, the IPA needs to establish a connection through the cellular network. This requires parameters such as an Access Point Name (APN).

Consumer devices such as smartphones and laptops store a long list of such parameters for the cellular networks within their memory, and support device management protocols to update them. However, many IoT devices are constrained in memory and protocols, and cannot support long lists or full device management protocols.

Therefore, SGP.32 introduces a mechanism to allow the IPA to retrieve the Connectivity Parameters from the currently enabled Profile. The structure of Connectivity Parameters is defined in TCA's eUICC Profile Package: Interoperable Format Technical Specification.

The IPAe can recover the Connectivity Parameters from the Profile through internal eUICC mechanisms (which are implementation specific). The IPAd can retrieve Connectivity Parameters through a command specified in SGP.32 called **`GetConnectivityParameters`**.

If the Connectivity Parameters are not set at the installation of the Profile, it is still possible to update them through the ES6 interface (the interface between the operator OTA service and the security domain of the operator in its Profile on the eUICC).

Once the IPAd or IPAe has retrieved the Connectivity Parameters, the IPA can use them to trigger the establishment of a connection to the eIM or SM-DP+.

Note that for private networks, the Connectivity Parameters, if not configured by the device, should be included by the mobile service provider in the Profile Package.

Notes:

- If there is no enabled Profile, SGP.32 does not currently describe what Connectivity Parameters can or should be used.
- The IPAe may always open a Bearer Independent Protocol (BIP) channel using the default bearer, leaving it up to the device the choice of Connectivity Parameters.
- It is implicitly assumed that Connectivity Parameters provided in the Profile should be able to connect with both the eIM and SM-DP+ at minimum. The device may use also these parameters for other applicative usages than RSP management.

7. Security and Certification

A key benefit of the Consumer and M2M Specifications is that they are supported by GSMA eSIM Security Certification and Compliance Processes. These comprehensive, well-established certification and compliance schemes require that solutions are subjected to thorough assessment and testing. This promotes confidence for operators, device manufacturers and service providers.

GSMA has now defined certification processes for all the components involved in eSIM IoT within the SGP.24 specification. This includes the following entities:

- eUICC
- eIM
- SM-DP+
- IoT device (IPA)

The following sections provide an overview of the processes for the eUICC, eIM and IPAd. Note there are no changes to the SM-DP+ process. The same SM-DP+ can be used with Consumer (SGP.22) and IoT (SGP.32) Devices, as IoT features were added on top of Consumer features.

7.1. eUICC Certification

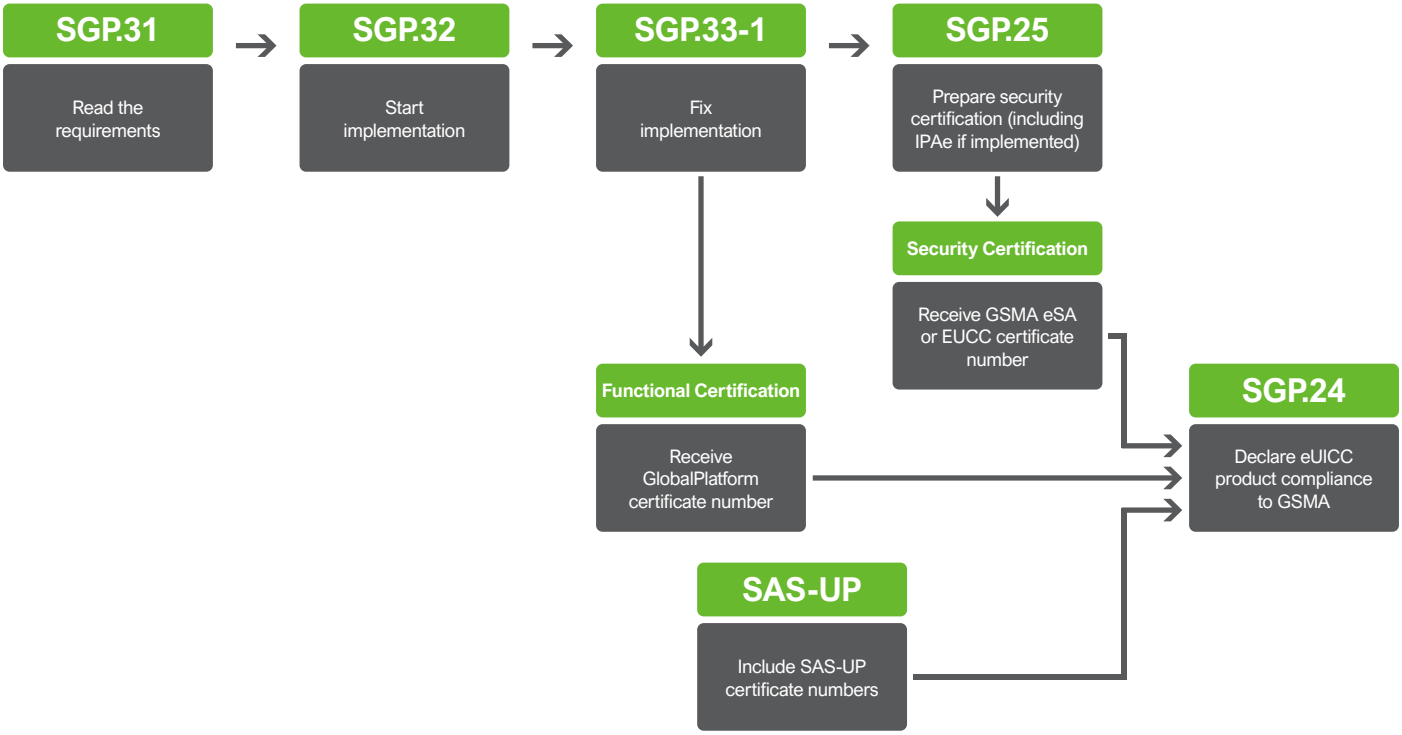


Figure 3 IoT eUICC Certification Process

The IoT eUICC certification process follows the existing certification process for any eUICC. The implementer shall read both SGP.31 and SGP.32. The functional certification process is based on the test specification SGP.33-1 and is run by GlobalPlatform on behalf of the GSMA. The security certification of the eUICC is based on the Protection Profile (SGP.25). SGP.25v2.1 is associated with Common Criteria Protection Profile BSI-CC-PP-0100-V2 and is suitable for both consumer and IoT eUICCs. Two methodologies are accepted today for the security evaluation: the GSMA eUICC Security Assurance (eSA) scheme and the EU Cybersecurity Certification Scheme on Common Criteria (EUCC).

Finally, the eUICC manufacturing environment shall be certified according to GSMA's Security Accreditation Scheme for UICC and eUICC Production (SAS-UP). Once all these steps are satisfied, the EUM can declare the eUICC to GSMA through forms provided in SGP.24, and have it accepted by the ecosystem.

7.2. eIM Certification

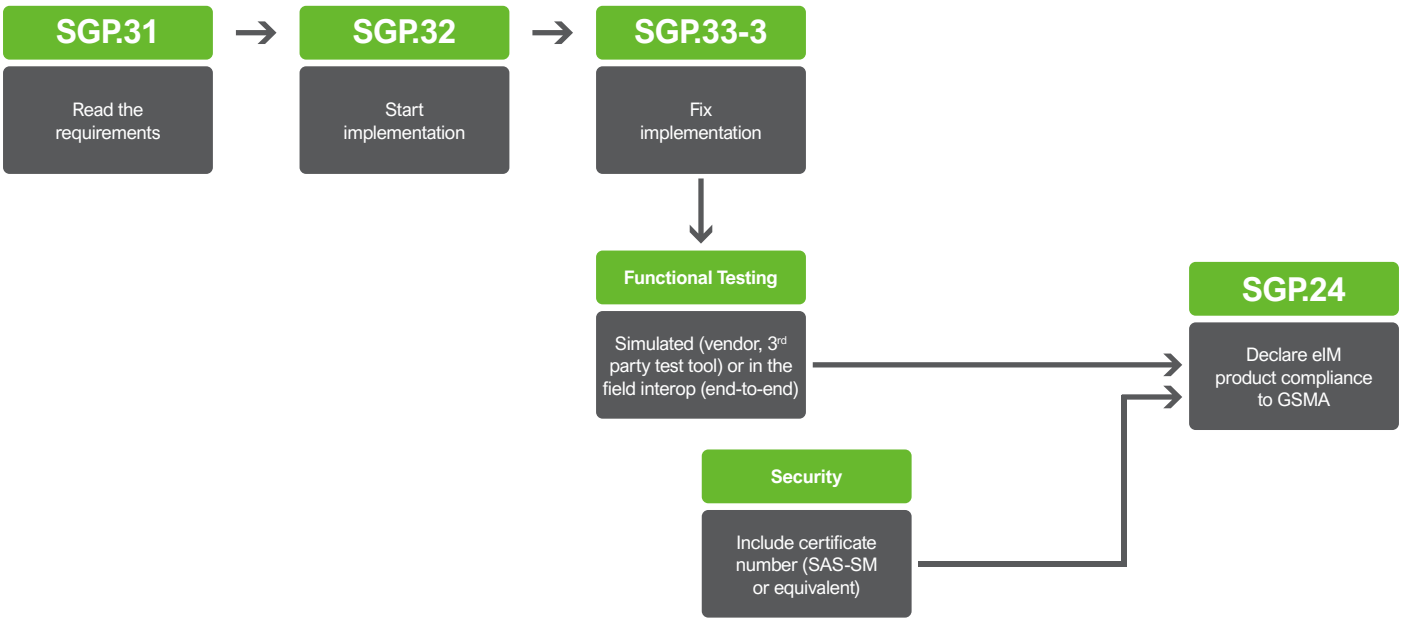


Figure 4 eIM Certification Process

The eIM certification is similar to the SM-DP+ certification. The eIM vendor shall declare functional compliance against the test specification SGP.33-3 and shall have SAS-SM certification or equivalent for security.

7.3. IPAd Certification

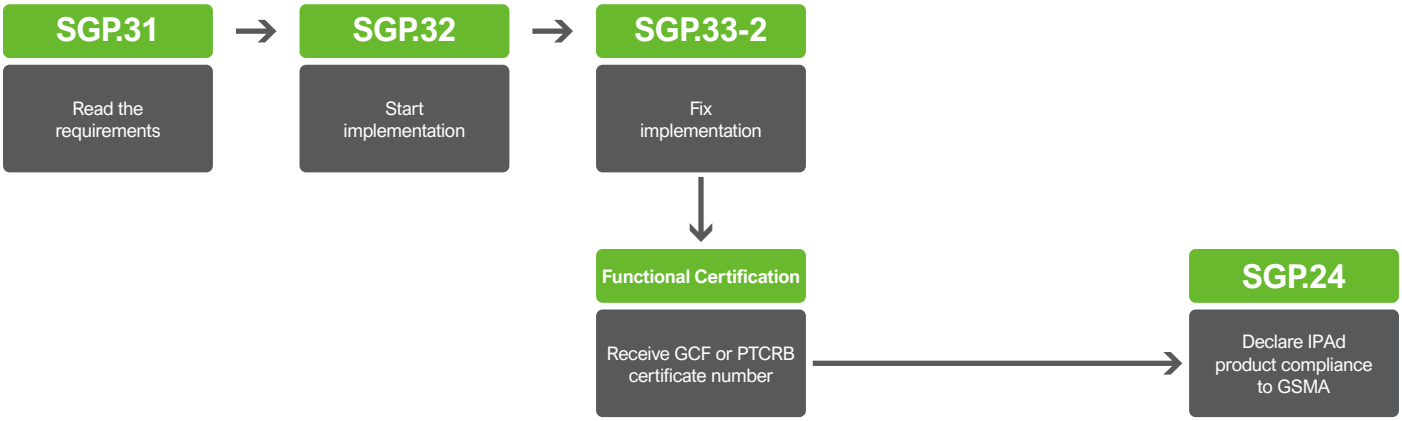


Figure 5 IPAd Certification Process

An IPA implemented in an eSIM IoT device can demonstrate functional compliance to the eSIM IoT requirements. The functional certification process is based on the test specification SGP.33-2 and is run by either the Global Certification Forum (GCF) or PTCRB[4] on behalf of the GSMA. Once the functional certification is achieved, the device manufacturer can declare the eSIM IoT device to GSMA through forms provided in SGP.24.

7.4. Opportunities to Increase Interoperability

As SGP.32 adoption builds and more industry feedback is received, TCA is exploring opportunities to bridge gaps in the existing GSMA testing infrastructure to promote safe, reliable and consistent IoT deployments in the field. Further information will be communicated on these potential initiatives as and when work progresses.

[4] Note that the acronym 'PTCRB' originally stood for PCS Type Certification Review Board, but since its origins in 1997 it has evolved way beyond Personal Communications Services and now covers the much more complex 4G and 5G technologies.

8. Conclusion and Next Steps

So that the potential of the IoT can be fully realised, TCA is committed to ensuring that SGP.32 deployments are underpinned by a strong foundation of security and interoperability.

In response to common industry questions and challenges flagged by industry participants following early adoption, this paper has aimed to further this commitment by analysing key ecosystem developments, offering technical guidance to address key operations and deployment scenarios, and examining the scope of the supporting testing and compliance infrastructure.

As the SGP.32 ecosystem matures and adoption builds – coupled with ongoing enhancements and updates to the specifications and supporting testing infrastructure – new considerations will undoubtedly be raised.

In response, TCA's RSP Working Group stands ready to develop and share further guidance with the industry to address these emerging challenges. To directly support this work, organisations across the SGP.32 ecosystem are strongly encouraged to consider engaging with TCA and becoming a member. This enables participation across TCA's various Working Groups, which are collectively working to shape the ongoing development of the SGP.32 ecosystem to promote increased security and interoperability.

9. 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.