eSIM Compliance

Report 2025

Contents

Contents (continued)

1. Executive Summary

Combining functional and security certification of the hardware, software, platform and site elements, with relevant activities undertaken by trusted organisations, the GSMA eSIM Compliance Process verifies the correct and secure operation of the eSIM products. Following this Compliance Process the issuance of digital certificates are authorised, ensuring that GSMA-certified eSIM products on the market can securely interact.

Each year, the GSMA certifies a high volume of eSIM products including eUICC, SM platforms and eSIM capable devices. This report is an analysis of the GSMA's eSIM product certifications listing, which provides insight into current trends in the eSIM Consumer, M2M and IoT markets as well as some conclusions and brief information on the likely trends into 2026 and beyond.

Abbreviations

Abbreviation	Description
CI	Certificate Issuer
eIM	eUICC Remote IoT Manager
eSA	eUICC Security Assurance
eSIM	Embedded SIM
eUICC	Embedded Universal Integrated Circuit Card
IoT	Internet of Things
M2M	Machine to Machine
PKI	Public Key Infrastructure
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SM-DP+	Subscription Manager Data Preparation+
SM-DS	Subscription Manager Discovery Server
SM-SR	Subscription Manager Secure Routing

2. What is the eSIM Compliance Process?

Recognising the need to demonstrate eSIM product compliance to technical specifications in a common accessible way, in 2017 the GSMA developed a compliance framework for eSIM capable Devices, eUICCs and Subscription Management servers.

The GSMA Industry Specifications SGP.24, for eSIM Consumer and IoT Products, and SGP.16, for eSIM M2M Products, detail the compliance requirements, and expected means to demonstrate compliance, for products designed to the eSIM Consumer, M2M and IoT specifications.

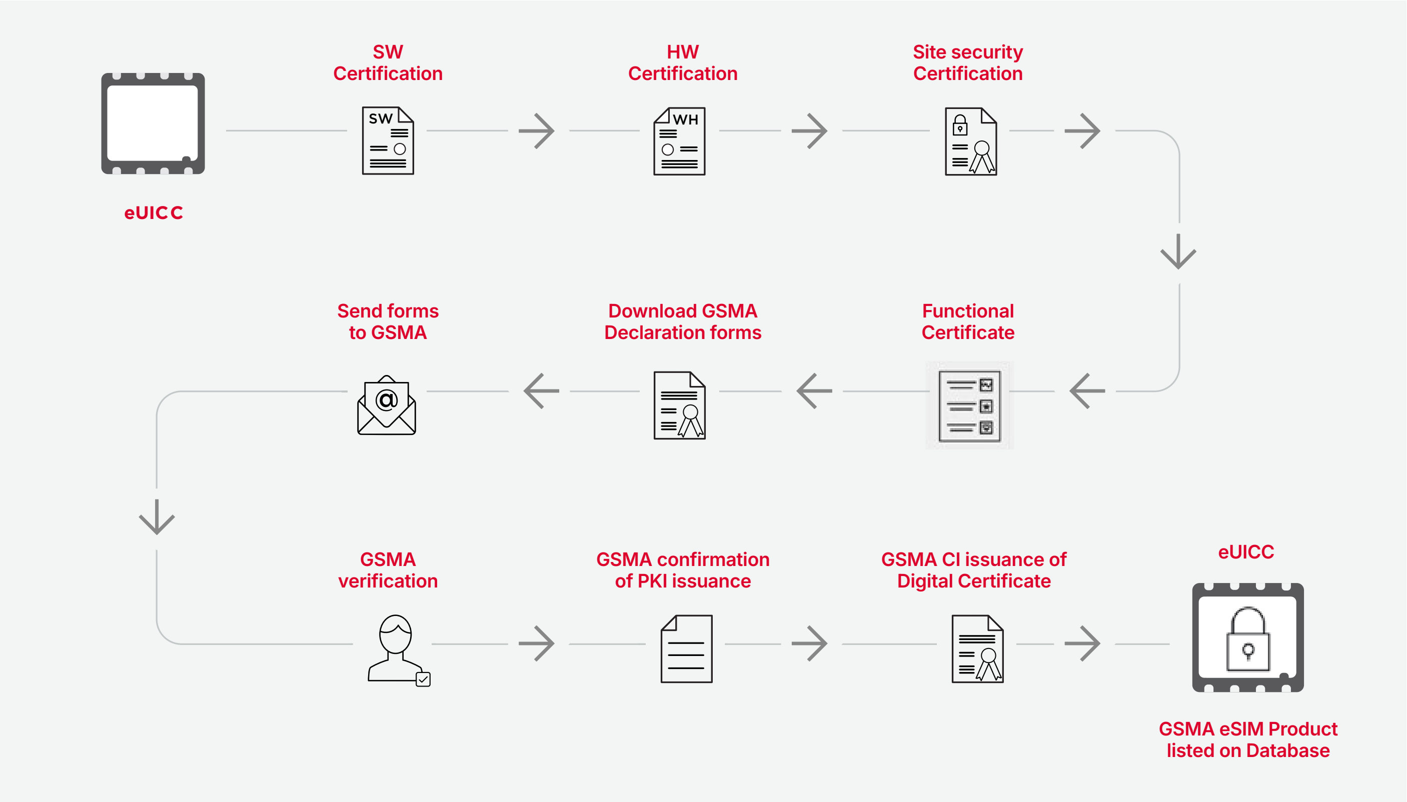
These industry specifications provide declaration templates to be completed and submitted by product manufacturers to GSMA once an eSIM product has proven its functionality, security and robustness via the indicated functional and security certification programs, software and hardware certification, interoperability, and other required elements.

3. eSIM Compliance Process Overview

The compliance requirements focus on security assurance, functionality, and interoperability. The result of a successful SGP.24 (Consumer and IoT Products) and SGP.16 (M2M products) declaration of compliance is a recognised achievement plus eligibility to use an eSIM digital certificate (PKI).

This is used for authentication between eUICCs and eSIM Subscription Management servers (SM-DP+ and SM-DS) once in the field.

The eSIM Compliance Process overview is as follows (example for eUICC product):


eUICC
SW Certification
SW
HW Certification
WH
Site security Certification
Functional Certificate
Download GSMA Declaration forms
Send forms to GSMA
@
GSMA verification
GSMA confirmation of PKI issuance
GSMA CI issuance of Digital Certificate
eUICC
GSMA eSIM Product listed on Database

The above example illustrates the Compliance Process for Discrete or Integrated eUICC products. More information on how this process works for other entities within the eSIM Ecosystem can be found HERE.

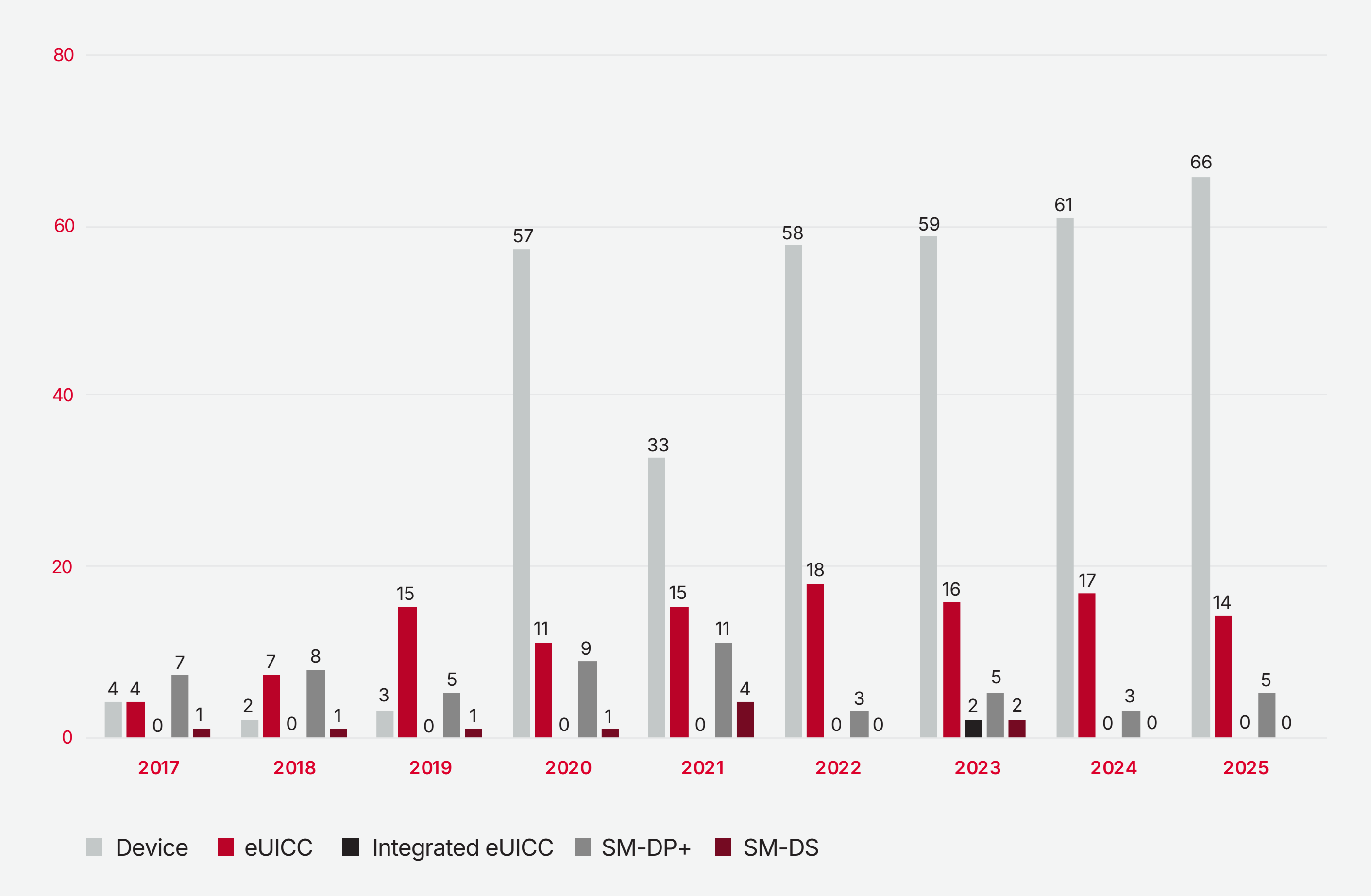
4. eSIM Compliance Products

GSMA certified eSIM Products are listed on the eSIM Compliance database accessible to GSMA members on the GSMA Member Gateway Platform.

The statistics presented in this report represents the number of eSIM Consumer Products (Devices, eUICCs, eIM, SM Servers), eSIM M2M Products and eSIM IoT Products that have declared compliance against the GSMA Compliance Process using SGP.24 (Consumer and IoT) or SGP.16 (M2M) between 2017 and 2025.

5. Consumer eSIM Products

5.1 Consumer eSIM Certified Products per Year



This graph illustrates the annual distribution of Devices, Discrete eUICCs, Integrated eUICCs, SM-DP+s, and SM-DSs over the period from 2017 to 2025.

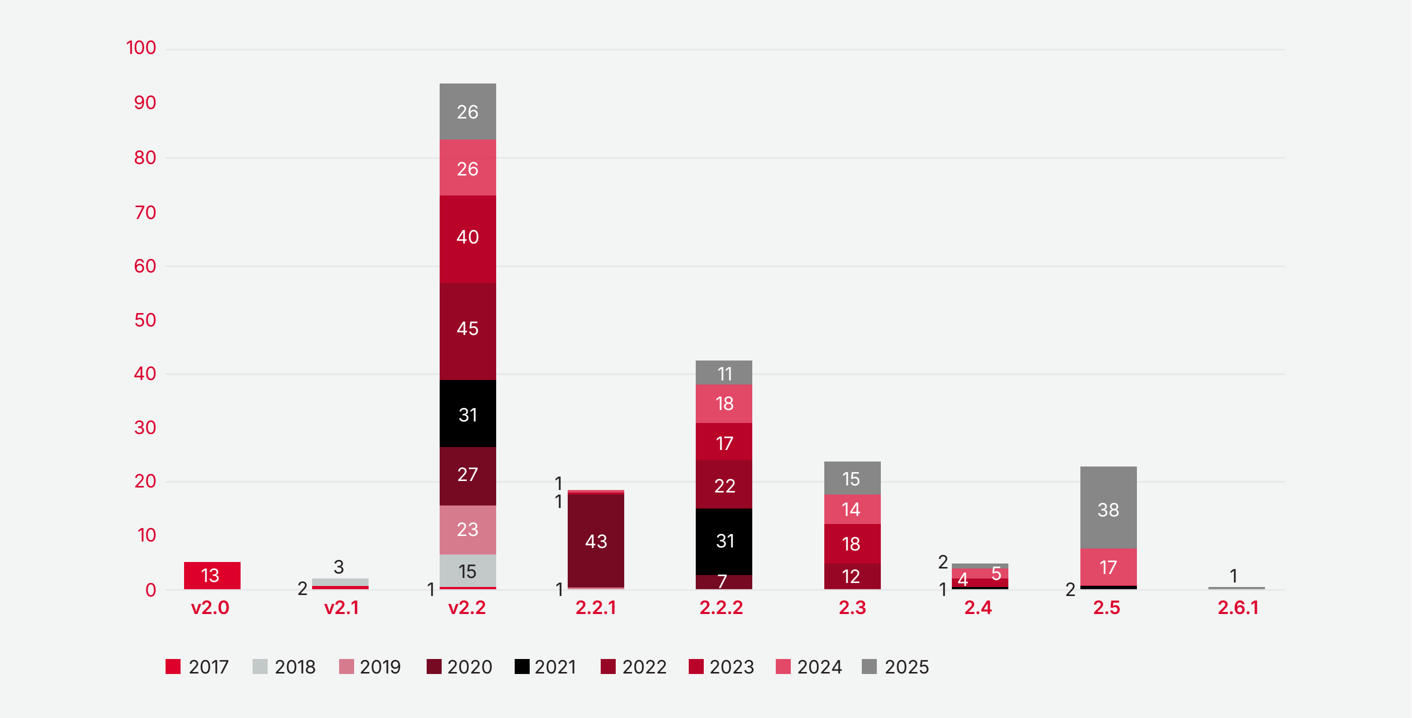
Key observations:

- **Device** products show a marked increase, rising from 4 in 2017 to 66 in 2025, with a significant surge in 2020 (57) and continued growth thereafter.
- **eUICC** products fluctuate, starting at 4 in 2017, peaking at 18 in 2022, and then declining to 14 by 2025.
- **Integrated eUICC** products are introduced in 2023, reaching a maximum of 2, but are absent in the last two years (2024 and 2025).
- **SM-DP+** products show as slow but steady growth with a peak of 11 in 2021.
- **SM-DS** products are only present in select years, with the highest count being 4 in 2021.

Overall, the graph demonstrates a strong upward trend in eSIM Device products, moderate growth in eUICC and Integrated eUICC, and steady rise of SM-DP+ with low adoption of SM-DSs.

5.2 eSIM Consumer Specifications Versions

Since 2017, GSMA has been evolving its specifications to incorporate new features, resolve issues or introduce improvements. The following graph shows how the technical versions of Consumer Specifications have been used in eSIM Consumer Products over the years.



These graphs illustrate how the version of SGP.22 used changed with time where the following can be noted:

Top Used Versions

- **V2.2** and **V2.2.2**, released in 2017 and 2020 respectively, stand out as the most widely adopted versions, with peak usage reaching 200 products for **V2.2** and 100 products for **V2.2.2** certified across multiple years. This consistent use shows these have been stable and active versions for a long period.
- **V2.3** and **V2.5**, released in 2021 and 2023 respectively, also show notable adoption, especially considering their more recent release timing. The increasing adoption of these more recently released versions show that the updated features and enhancements in the releases are increasingly becoming available in commercial products.

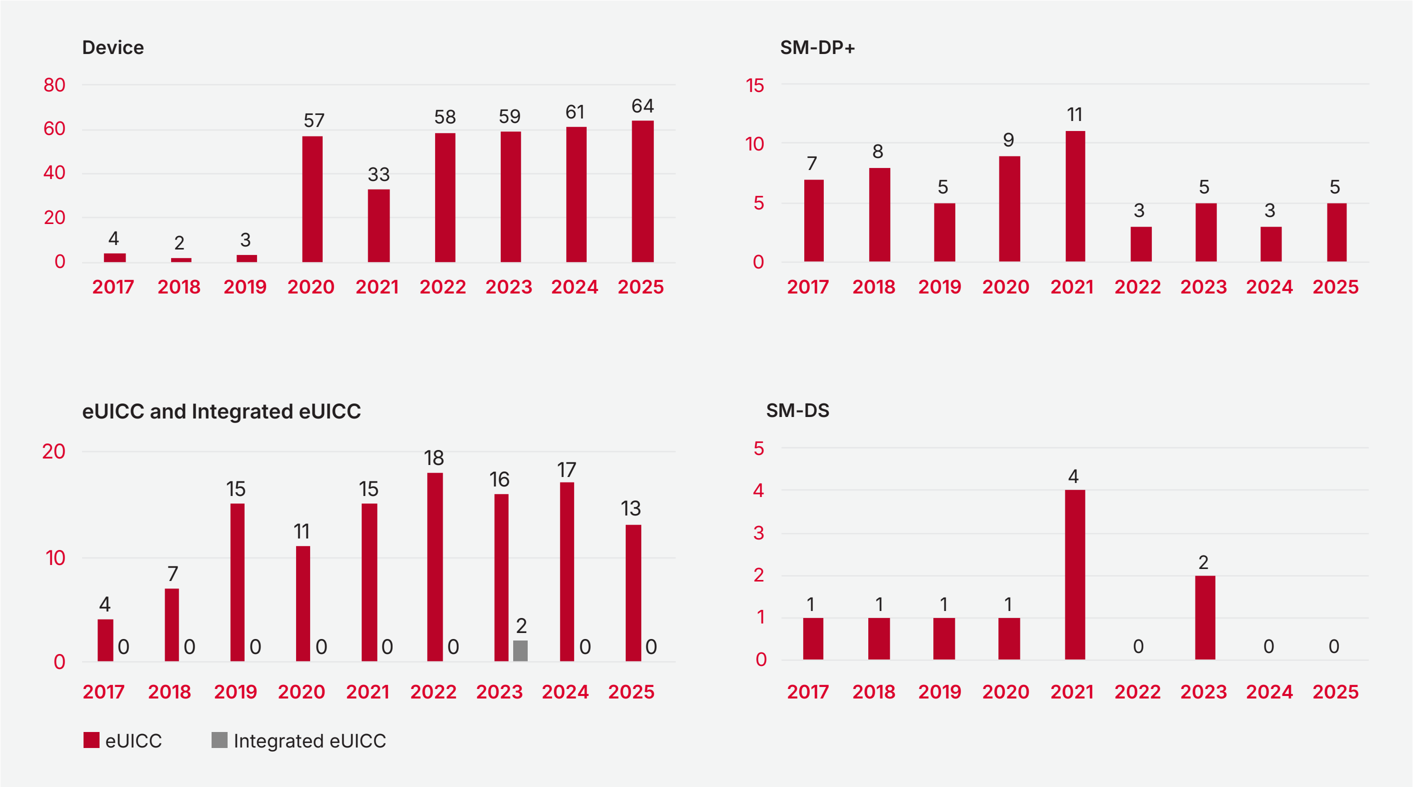
Recent Versions

- **V2.6** and **V2.6.1** show minimal usage, which aligns with their recent publication in 2025.
- **V3.0** and **V3.1** show minimal usage despite their release in 2022 and 2023 respectively.

Despite its minimal usage, the adoption of these versions is likely to grow in the coming months or years depending on stability, compatibility, and feature uptake.

In 2025 the most used versions were v2.5(32), v2.2 (26), v2.3 (15) and V2.2.2 (11).

5.3 Consumer eSIM Certified Products per Type



Market Needs Perspective

eUICC Products Enable Device Diversity

- The data shows that the number of eUICC and Integrated eUICC products does not directly correlate with the number of devices. This is because a single eUICC solution can be integrated into multiple device types (e.g., smartphones, wearables, IoT modules). The market demand is therefore driven by the flexibility and interoperability of eUICC technology, which enables manufacturers to address a wide range of device categories and use cases with fewer, but more versatile, eUICC solutions.

SM-DP+ as a Multi-Tenant Enabler

- The relatively stable number of SM-DP+ platforms, compared to the growing device ecosystem, highlights their role as scalable infrastructure. A single SM-DP+ instance can serve multiple mobile network operators and enterprises, supporting a broad array of commercial and industrial deployments. This reflects a market need for robust, centralised platforms that can efficiently manage large and diverse eUICC populations across different customers.

Device Growth Reflects Expanding Use Cases

- The strong upward trend in device numbers indicates expanding adoption of eSIM technology across industries. However, this growth is enabled by the underlying eUICC and SM-DP+ infrastructure, which allows manufacturers and service providers to scale.

SM-DS Remains Niche

- The consistently low numbers for SM-DS suggest that, while the technology is available, market demand is limited to specific scenarios. This reflects a focus on specialised applications where SM-DS functionality is required.

5.3.1 eUICC Products

An eUICC product, is a secure component embedded in either a discrete or integrated form factor, designed to be removable or non-removable within devices. It enables Remote SIM Provisioning (RSP), allowing mobile network profiles to be securely downloaded and managed over-the-air.

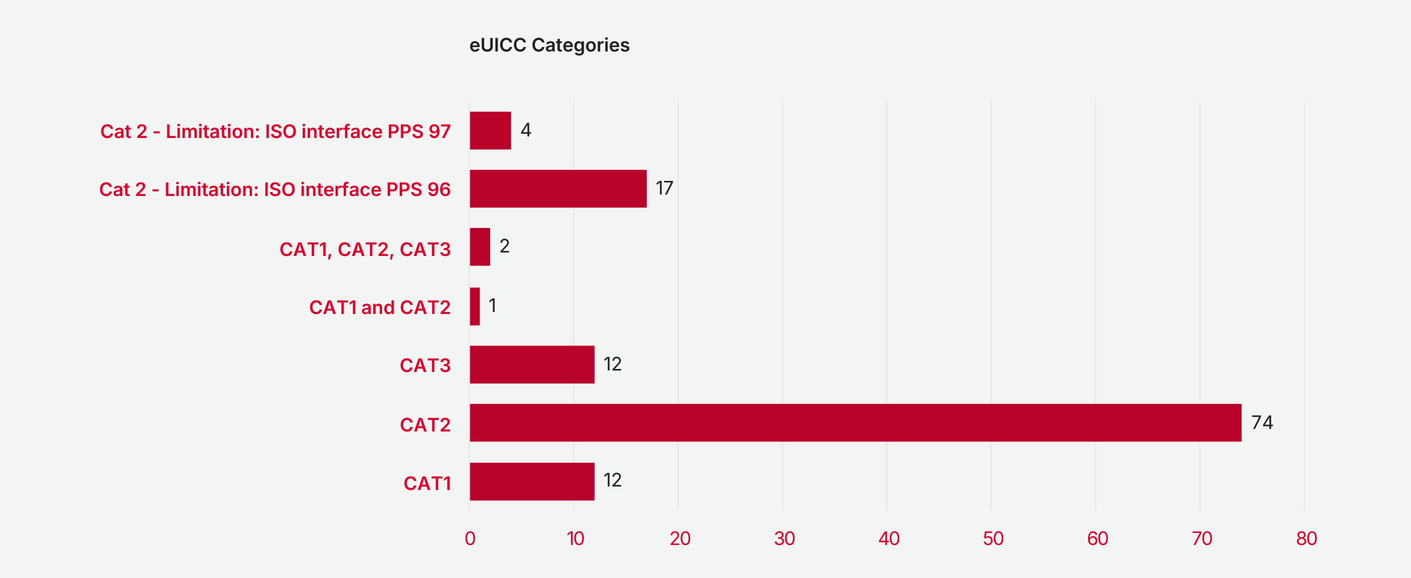
The following sections present a comprehensive overview of eUICC Consumer products declared to GSMA, categorised by product type, software and hardware security compliance, optional feature support, and other relevant attributes.

5.3.2 eUICC Categories

eUICC categories are defined within the SGP.22 as follows:

Feature	Basic eUICC (CAT1)	Medium eUICC (CAT2)	Contactless eUICC (CAT3)
Memory Size	64 Kb	384 kB	1024 kB
ISO interface PPS	PPS 96	PPS 97	PPS 97
BIP over HTTPS	Yes	Yes	Yes
Processor Speed	Not Required	≥ 25 MHz	≥ 25 MHz
Crypto Processor Speed	Not Required	≥ 100 MHz	≥ 100 MHz
Memory Protection Unit	Not Required	Required	Required
NFC Compliance	Not Applicable	Not Applicable	Required

The eUICC Consumer Products belong to the following categories:



Conclusions

Most eUICCs Are in the Medium Category

The majority of eUICCs are classified as CAT2, or CAT2 with PPS 96 and PPS 97 limitations. This means most products are designed to meet medium-level requirements, depending on their specific features and market segmentation.

Basic and Contactless Categories Are Less Common

The categories with the lowest volumes are CAT3 and CAT1. This suggests that products with basic or contactless features are less common, possibly reflecting more specialised use cases or simpler device types.

Multi-Category eUICCs Show Versatility

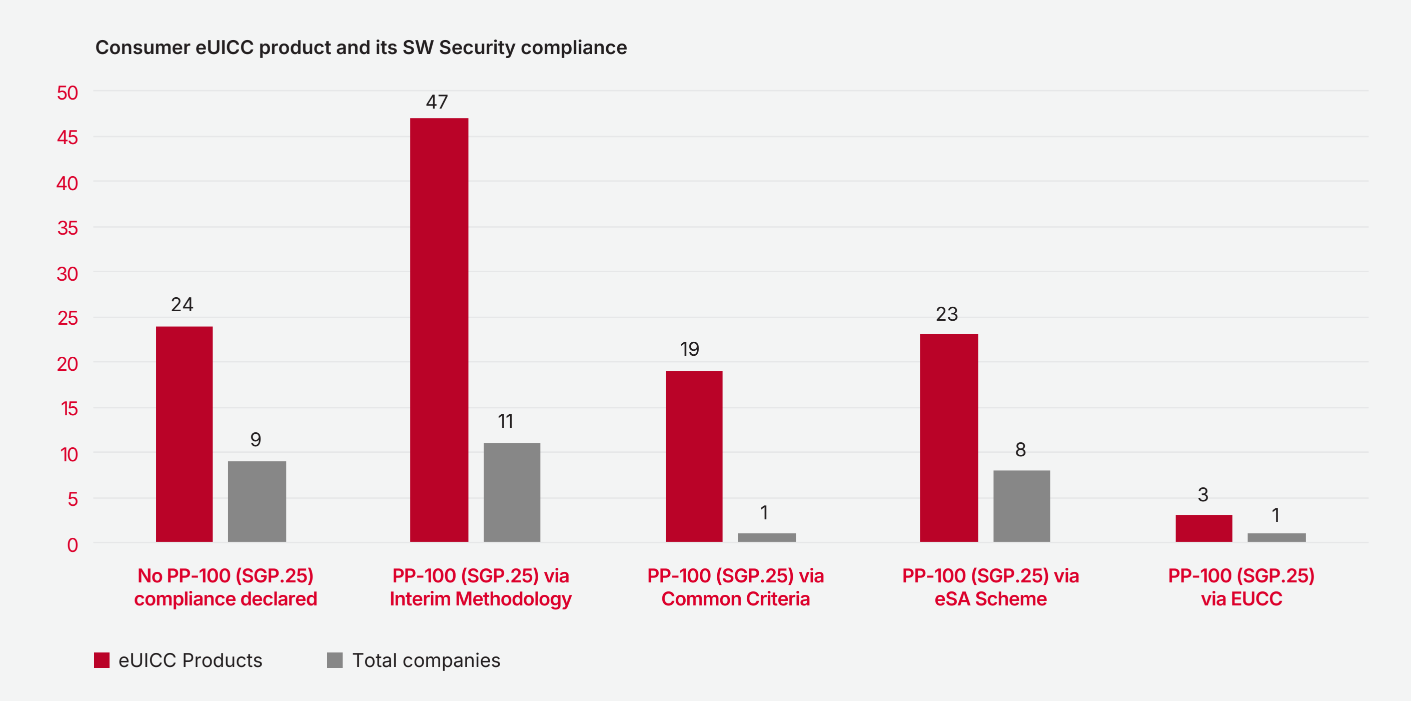
The presence of multi-category eUICCs indicates a trend towards multi-purpose products that can meet the needs of multiple market segments and requirements.

5.3.3 Software Security

The software security requirement within the eSIM Compliance Process mandates that the GSMA Consumer and IoT Protection Profile (Common Criteria PP-0100/SGP.25) needs to be fulfilled. Over the years, GSMA allowed 5 methodologies to demonstrate this software security requirement:

1. No compliance declared (early adopters)
2. eUICC Statement of Security Evaluation Completion (interim methodology solution)
3. Common Criteria Certification
4. eSA scheme certification
5. EUCC

Only options 3, 4 and 5 are now possible but the following statistics indicates the number of Consumer eUICC products certified with each of these methodologies over the years:



Conclusions

No Declared Compliance:

24 products from 9 companies did not declare PP-100 (SGP.25) compliance. These were early adopters, and it's important to note that declaring products without software certification has not been permitted since 2019.

Interim Methodology:

Used in 47 products from 11 companies, this was the most common compliance route. However, it was officially deprecated in 2023 and is no longer available.

eSA Scheme:

With 23 products from 8 companies, this is the second most used method. Its strong uptake is notable, especially since it was only introduced in 2022 and is one of the three currently valid certification options.

Common Criteria and EUCC:

These methods are less adopted, with 19 and 3 products respectively, each supported by just one company. Alongside the eSA Scheme, they are the only certification paths currently available to the industry.

Summary

This diagram shows a clear shift in software security compliance for consumer eUICC products. While many early products lacked declared certification, this practice has been discontinued since 2019. The now-deprecated Interim Methodology was widely used, but the industry is transitioning towards newer security standards.

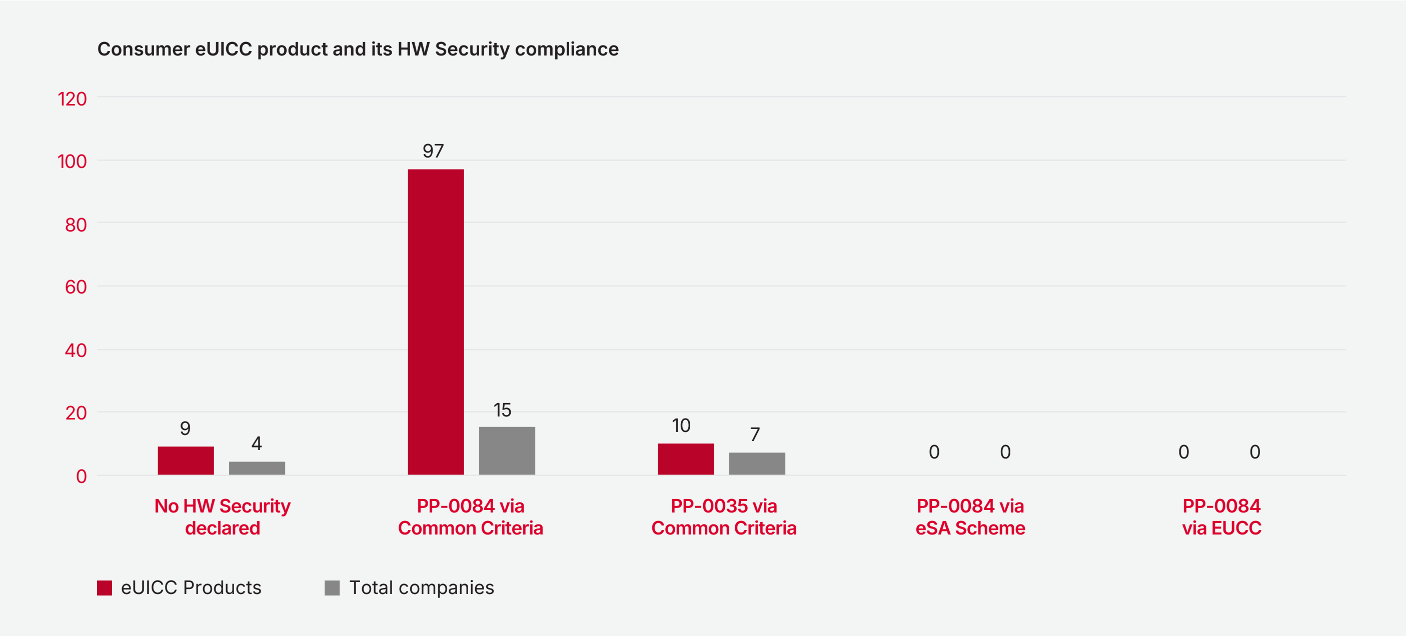
The eSA Scheme, despite being recently introduced, has gained strong traction. Meanwhile, Common Criteria and EUCC remain niche but still with potential to growth as part of the three recognised certification options currently available.

5.3.4 Hardware Security

The hardware security requirement within the eSIM Compliance Process mandates that the GSMA Consumer and IoT Protection Profile (Common Criteria PP-0084 or PP-0035) needs to be fulfilled. Over the years, GSMA allowed 5 methodologies to demonstrate this hardware security requirement:

1. No compliance declared (early adopters)
2. PP-0035 via Common Criteria Certification
3. PP-0084 via Common Criteria Certification
4. PP-0084 via eSA scheme certification (recently added, not adopted yet)
5. PP-0084 via EUCC (recently added, not adopted yet)

Only options 2 to 5 are now possible but the following statistics indicates the number of Consumer eUICC products certified with each of these allowed processes:



Conclusions

PP-0084 via Common Criteria

This is the most widely adopted hardware security certification, with 97 products from 15 companies. Its popularity reflects strong industry trust and alignment, especially since PP-0084 has been part of the hardware requirements from the beginning.

PP-0035 via Common Criteria

Used in 10 products from 7 companies, PP-0035 has seen lower adoption compared to PP-0084. Although both were introduced as alternative certification options from the start, PP-0084 has clearly become the preferred choice.

No Hardware Security Declared

There are 9 products from 4 companies that did not declare compliance with either PP-0084 or PP-0035. These are early market eUICC declared between 2017 and 2019. It's important to note that since 2019, declaring products without hardware certification has no longer been permitted.

PP-0084 via eSA Scheme and EUCC

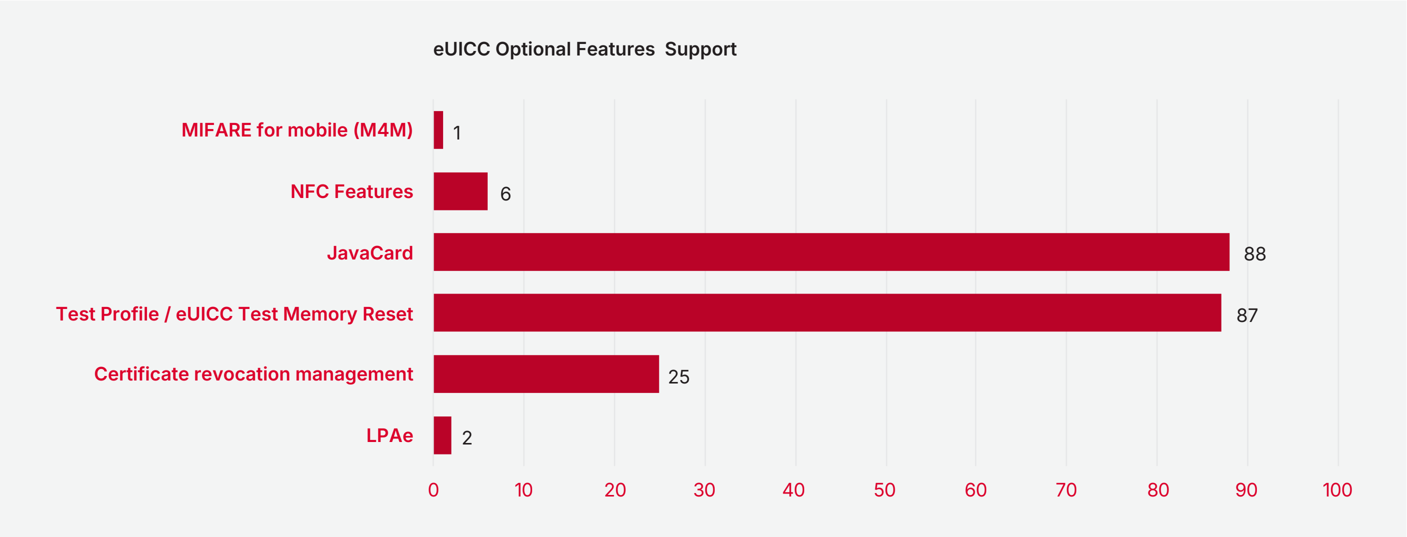
These certification options show zero adoption so far. This is expected, as they were only introduced in early 2025 and may still be in the early stages of industry evaluation and implementation.

Summary

The data shows a clear preference for PP-0084 via Common Criteria as the industry standard for hardware security in consumer eUICC products. While PP-0035 was introduced as an alternative, its adoption remains limited. Early products without declared compliance are no longer permitted under current certification rules. Newer options like eSA Scheme and EUCC have yet to gain traction, likely due to their recent introduction.

5.3.5 Optional Features Supported

From SGP.24 V2.3, release in October 2020, eUICC manufactures can indicate the optional features support by their eUICC compliance product. As such, the below table indicate the supported optional features in eUICC from 2020 onwards:



Conclusions

JavaCard and **Test Profile / eUICC Test Memory Reset** are the most widely supported features, each present in nearly 90 products. This high level of adoption highlights their central role in enabling key functionalities across eUICC implementations.

Certificate Revocation Management shows moderate support, with 25 products including it. This suggests that while not universally adopted, it holds value for certain use cases or deployment models.

In contrast, **NFC Features**, **LPAe**, and **MIFARE for Mobile (M4M)** are supported in only 6, 2, and 1 product respectively. Their limited presence indicates that these features are either niche, emerging, or relevant only to specific device types or market segments.

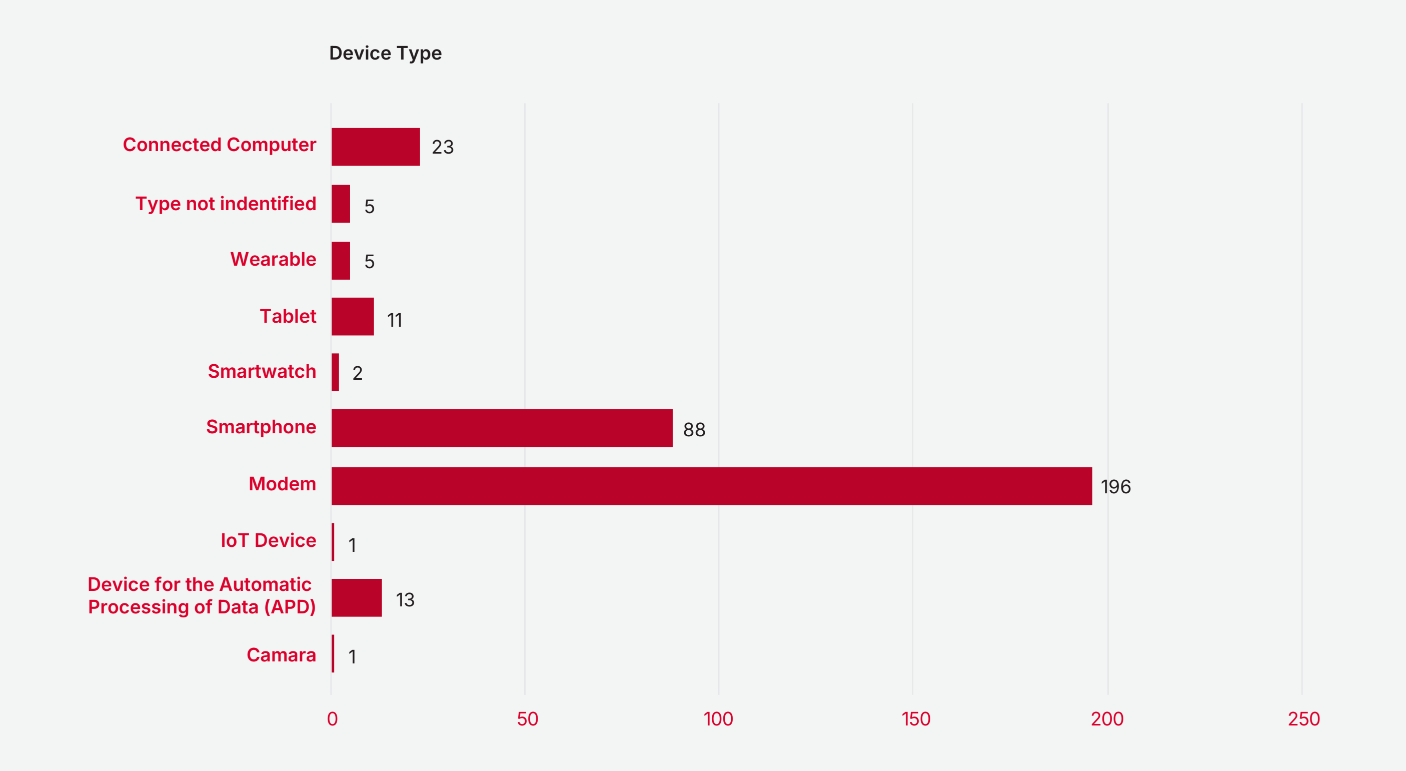
5.4 eSIM Device Products

An eSIM Device, is a device equipped with an embedded Universal Integrated Circuit Card (eUICC) that supports Remote SIM Provisioning (RSP).

These devices can securely download, manage, and switch mobile network profiles over-the-air.

The following sections provide insights into the types of eSIM-enabled devices declared to GSMA, highlighting trends in Device type, eUICC slots, capabilities, and market adoption.

5.4.1 eSIM Device Type



Conclusions

Modems and Smartphones Dominate the Landscape

The largest share of devices are modems (196 units) and smartphones (88 units). This confirms that connectivity and mobile communication remain the primary drivers in the device ecosystem. These categories likely represent core infrastructure and user endpoints in both consumer and enterprise environments.

Specialised Devices Show Niche Adoption

- **Devices for the Automatic Processing of Data (APD)** account for **13 units**, indicating a focused but important role in enterprise automation and data handling.
- **Connected Computers (23 units)** show moderate use, possibly for desktop or fixed-location operations.
- **Tablets (11 units), wearables (5 units), and smartwatches (2 units)** are present in smaller numbers, suggesting targeted or emerging use cases.
- The presence of only **1 IoT device** and **1 camera** suggests either early-stage deployment or that these devices are being integrated into other categories or classified differently.

Unclassified Devices

The **"Type not identified"** (5 units) category reflect classification gaps in early adopters where it was not needed to identify the device type.

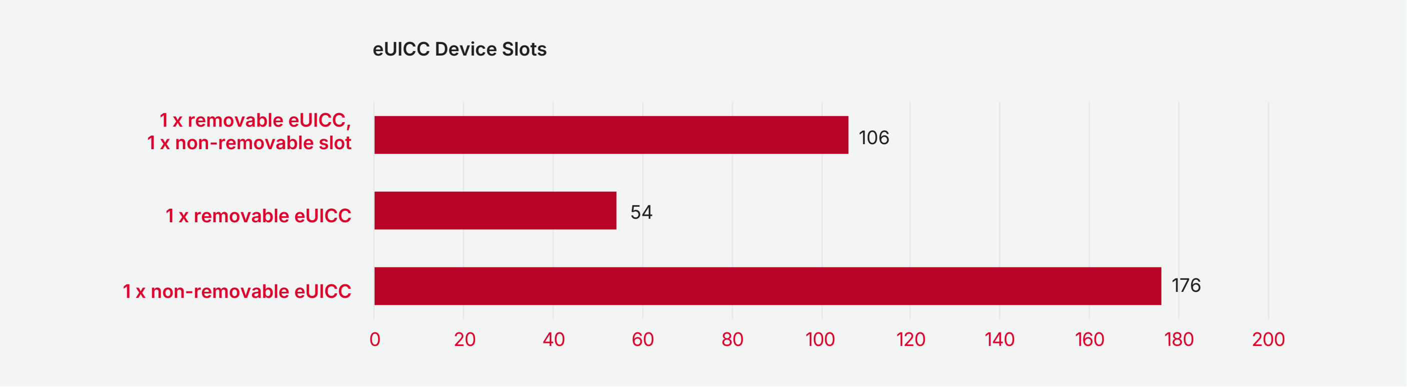
Summary

Modems and smartphones continue to be the most prevalent devices, underscoring the importance of network connectivity and mobile access. However, the presence of APD units, tablets, wearables, and other specialised devices reflects a diversifying ecosystem. This variety points to evolving needs in both consumer and business contexts, especially in areas like automation, mobility, and data processing.

As more specialised and hybrid devices emerge, it becomes increasingly important to implement flexible and scalable solutions that support a wide range of device types and connectivity requirements.

5.4.2 Device eUICC Slots

Devices can be designed to support non-removable eUICCs, removable eUICC or dual-slot configurations (removable and non-removable eUICCs). This chart presents the distribution of device slot configurations for eUICCs.



Conclusions

- **1 x non-removable eUICC:** 176 devices
  This is the most prevalent configuration, indicating a strong industry preference for embedded (non-removable) eUICCs. This aligns with trends favouring security, compact design, and reduced physical servicing, especially in consumer electronics and IoT deployments.
- **1 x removable eUICC**: 54 devices
  This configuration reflects continued demand for flexibility, allowing users to replace or upgrade the eUICC as needed. It is less common than embedded solutions but remains relevant for certain device types and use cases.
- **1 x removable eUICC, 1 x non-removable slot:** 106 devices
  Devices supporting both removable and non-removable eUICCs offer maximum versatility, enabling seamless migration, redundancy, or support for multiple operational scenarios.

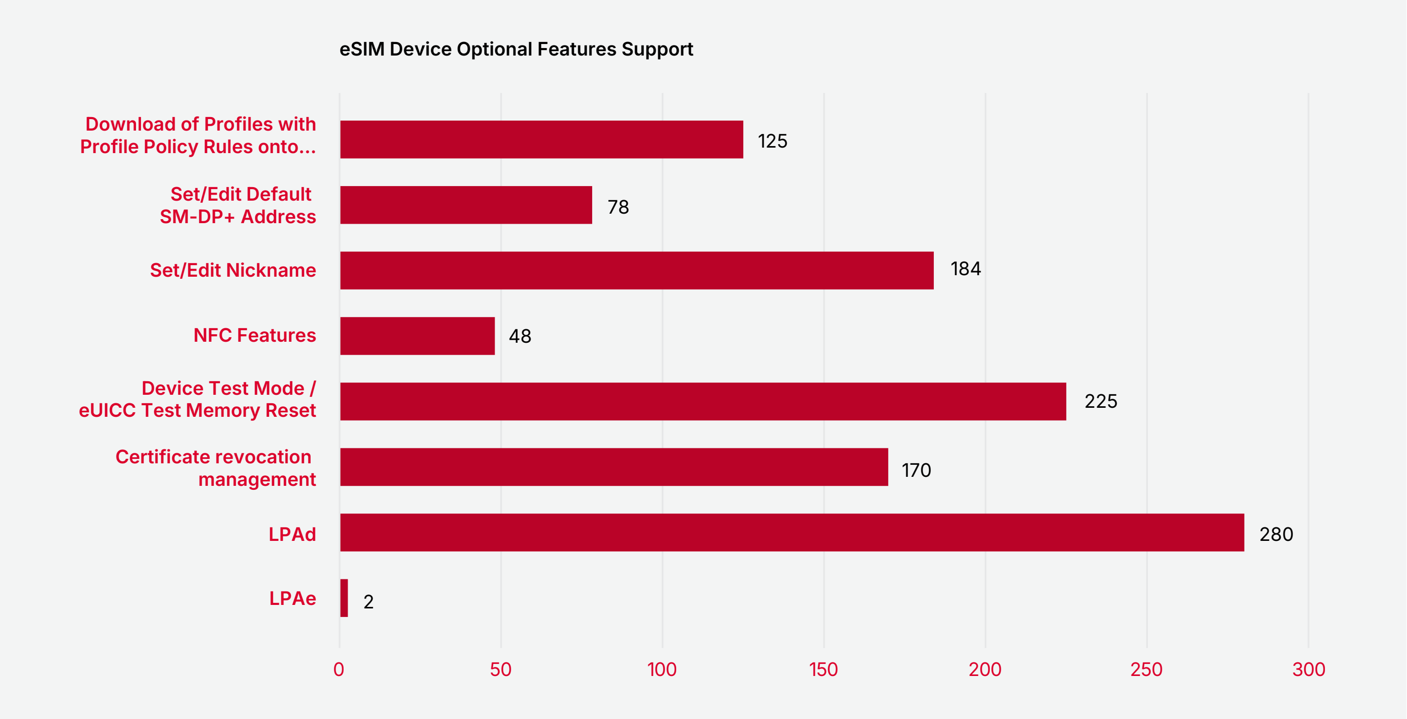
Summary

The data shows a clear preference for embedded (non-removable) eUICCs only devices but also highlights the ongoing importance of flexibility and redundancy provided by devices with removable and dual-slot configurations.

This diversity in device slot design reflects the varied and evolving needs of the market.

5.4.3 Optional Features Supported

From SGP.24 V2.3, release in October 2020, Device manufactures can indicate the optional features support by their Device compliance product. As such, the below table indicate the supported optional features in eUICC from 2020 onwards:



Conclusions

LPAd is the most widely supported feature, present in **280 devices**, indicating its strong relevance and integration across the eSIM ecosystem.

Device Test Mode / eUICC Test Memory Reset also shows high adoption, supported by **225 devices**, suggesting its importance for testing and maintenance workflows.

Features like **Set/Edit Nickname** and **Certificate Revocation Management** are moderately supported, with **184** and **170 devices** respectively, reflecting their practical utility.

Download of Profiles with Policy Rules and **Set/Edit Default SM-DP+ Address** have lower but notable support, indicating selective implementation based on device type or use case.

NFC Features and especially **LPAe** show **limited support**, with only **48** and **2 devices** respectively. This suggests these features are either niche, emerging, or not widely prioritised by manufacturers.

5.5 SM-DP+ and SM-DS Products

The SM-DP+ is a key component in the GSMA Remote SIM Provisioning architecture for Consumer Devices. It is responsible for securely preparing, storing, and delivering operator profiles to eUICCs in consumer eSIM devices. SM-DP+ enables encrypted profile downloads and manages profile lifecycle operations.

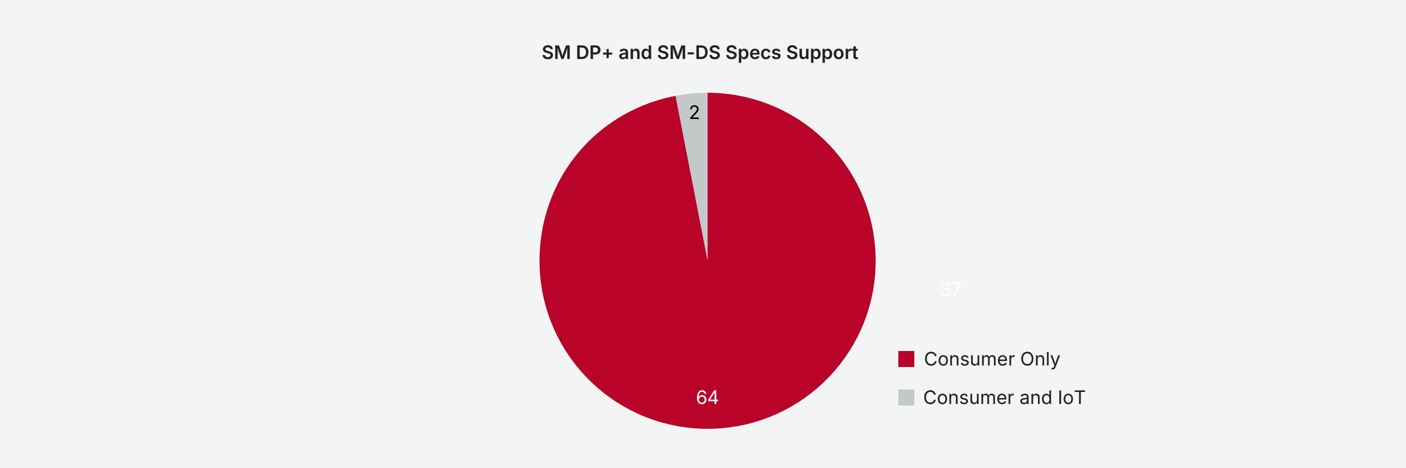
The SM-DS acts as a central discovery point in the GSMA RSP framework, enabling eSIM devices to locate available SM-DP+ servers for profile download. It facilitates seamless connectivity by allowing devices to retrieve profile availability information without prior configuration.

The following sections explore the distribution and adoption of SM-DP+ and SM-DS platforms declared to GSMA, offering a view into how operators and service providers support remote provisioning.

5.5.1 SM-DP+ and SM-DS Specification Support

SM-DP+ and SM-DS components were initially designed for the **eSIM Consumer Architecture** and later extended to support the **IoT Architecture**. With the release of the complete eSIM IoT framework allowing product declarations in early 2025, these entities can now operate across both domains.

The following graph provides insight into how SM-DP+ and SM-DS platforms are currently supporting **Consumer-only** use cases or offer **dual support** for both **Consumer and IoT** architectures.



The pie chart highlights that the distribution of SM-DP+ and SM-DS platforms based on their architectural support is:

- **Consumer Only:** 64 platforms
- **Consumer and IoT:** 2 platforms

This means that 97% of the platforms support Consumer-only use cases, while just 3% support both Consumer and IoT.

Conclusions

Consumer-only support dominates the current landscape, with the vast majority of platforms (64 out of 66) dedicated solely to this architecture.

Dual support for Consumer and IoT is still rare, with only 2 platforms offering this capability which may be due to the recent release of specifications enabling it.

Summary

The graph reveals that most of the eSIM Platforms are design for **Consumer-only support**, with dual architecture support remaining minimal.

As the industry continue to adopt the capabilities introduced in **SGP.31/32 for eSIM IoT**, we may see a gradual shift toward more platforms supporting both Consumer and IoT use cases.

6. IoT eSIM Products

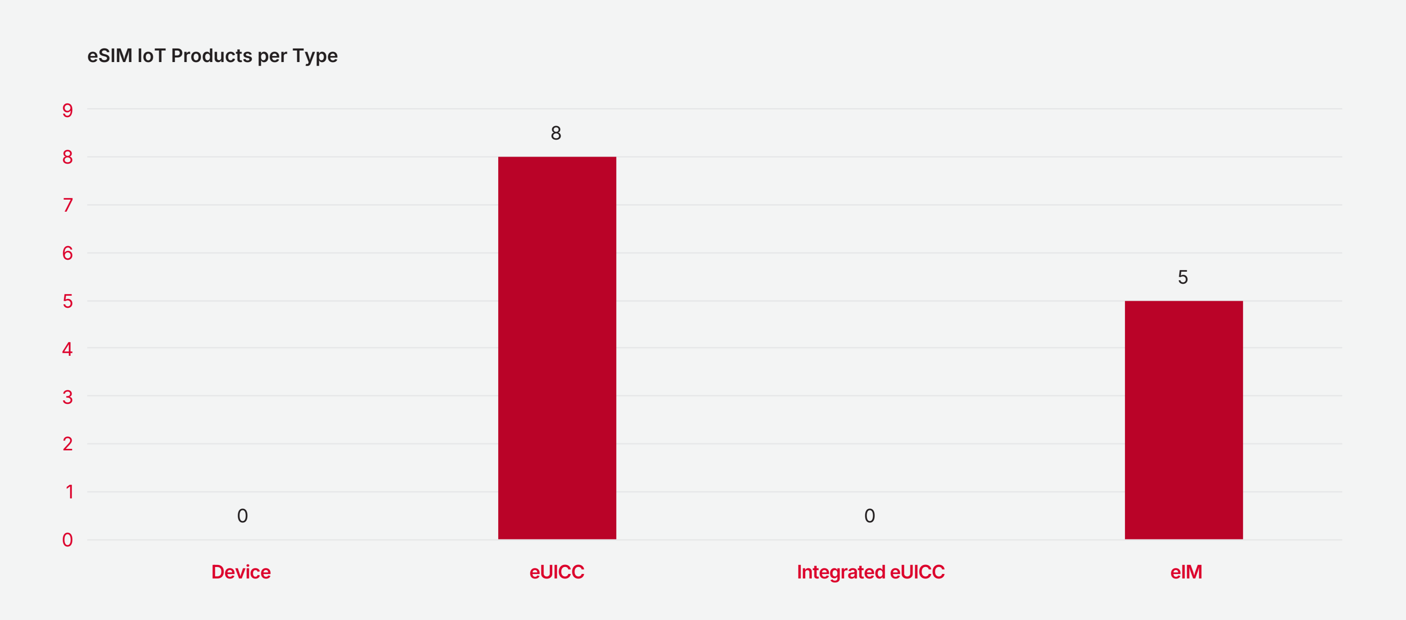
6.1 eSIM IoT Specifications Versions

Since 2022, GSMA has been evolving its IoT specifications to incorporate features, resolve issues or introduce improvements. Nevertheless, the only versions able to demonstrate compliance are SGP.31/32 V1.2 using the test documents SGP.33-1, SGP.33-2, SGP.33-3 v1.2 published in early 2025. The only products that have been declared as compliant are based on the SGP.31 / .32 v1.2 specifications.

Note that the IoT specifications are built on top of the Consumer specifications, so all SGP.21 and .22 properties can be inherited unless specifically excluded.

6.2 IoT eSIM Certified Products per Type

Given eSIM IoT specifications have only been completed in early 2025, the figures below are lower than those for eSIM Consumer and eSIM M2M.



The presence of **8 eUICC** and **5 eIM** products so soon after the publication of eSIM IoT specifications suggests that these two categories were **prioritised by manufacturers** - likely due to factors such as Market demand and readiness and maturity in development pipelines.

6.3 eUICC Products

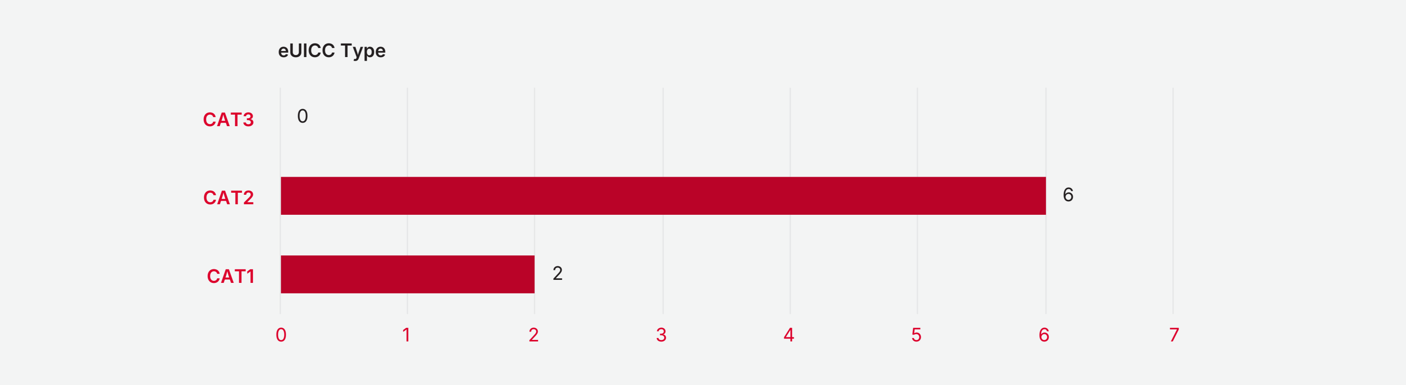
The following sections present a comprehensive overview of eUICC IoT products declared to GSMA, categorised by product type, software and hardware security compliance, optional feature support, and other relevant attributes.

6.3.1 IoT eUICC Categories

eUICC categories are defined within the PRD SGP.22 as follows:

Feature	Basic eUICC (CAT1)	Medium eUICC (CAT2)	Contactless eUICC (CAT3)
Memory Size	64 Kb	384 kB	1024 kB
ISO interface PPS	PPS 96	PPS 97	PPS 97
BIP over HTTPS	Yes	Yes	Yes
Processor Speed	Not Required	≥ 25 MHz	≥ 25 MHz
Crypto Processor Speed	Not Required	≥ 100 MHz	≥ 100 MHz
Memory Protection Unit	Not Required	Required	Required
NFC Compliance	Not Applicable	Not Applicable	Required

The eUICC IoT Products belong to the following categories:



Conclusions

Most eUICCs Are in the Medium Category

The market is currently favouring Medium eUICCs (CAT2) perhaps due to their balance of performance and compliance.

Basic and Contactless Categories Are Less Common

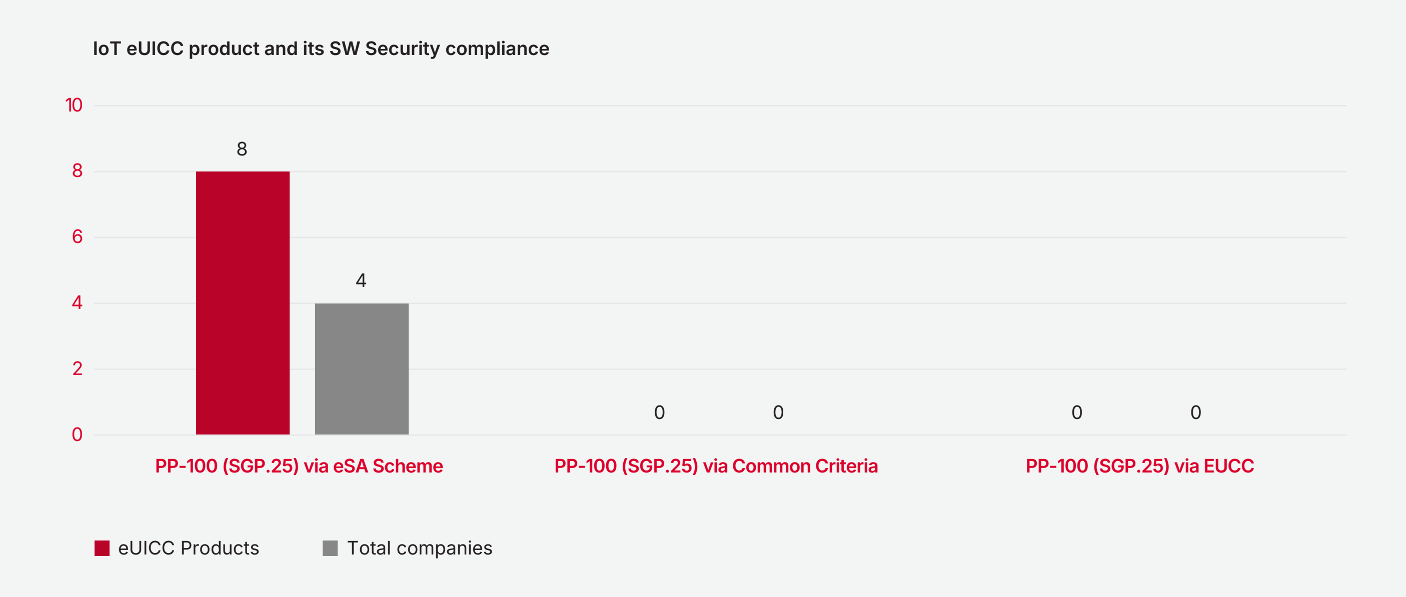
Basic eUICCs (CAT1) are present but less common and Contactless eUICCs (CAT3) have yet to see adoption, likely due to the extra requirements to satisfy this category.

6.3.2 Software Security

The software security requirement within the eSIM Compliance Process mandates that the GSMA IoT Protection Profile (Common Criteria PP-0100/SGP.25) needs to be fulfilled. GSMA allow 3 methodologies to demonstrate this software security requirement:

2. 1. Common Criteria Certification
3. 2. eSA scheme certification
4. 3. EUCC

The following graph indicates the number of IoT eUICC products certified with each of these methodologies:



Conclusions

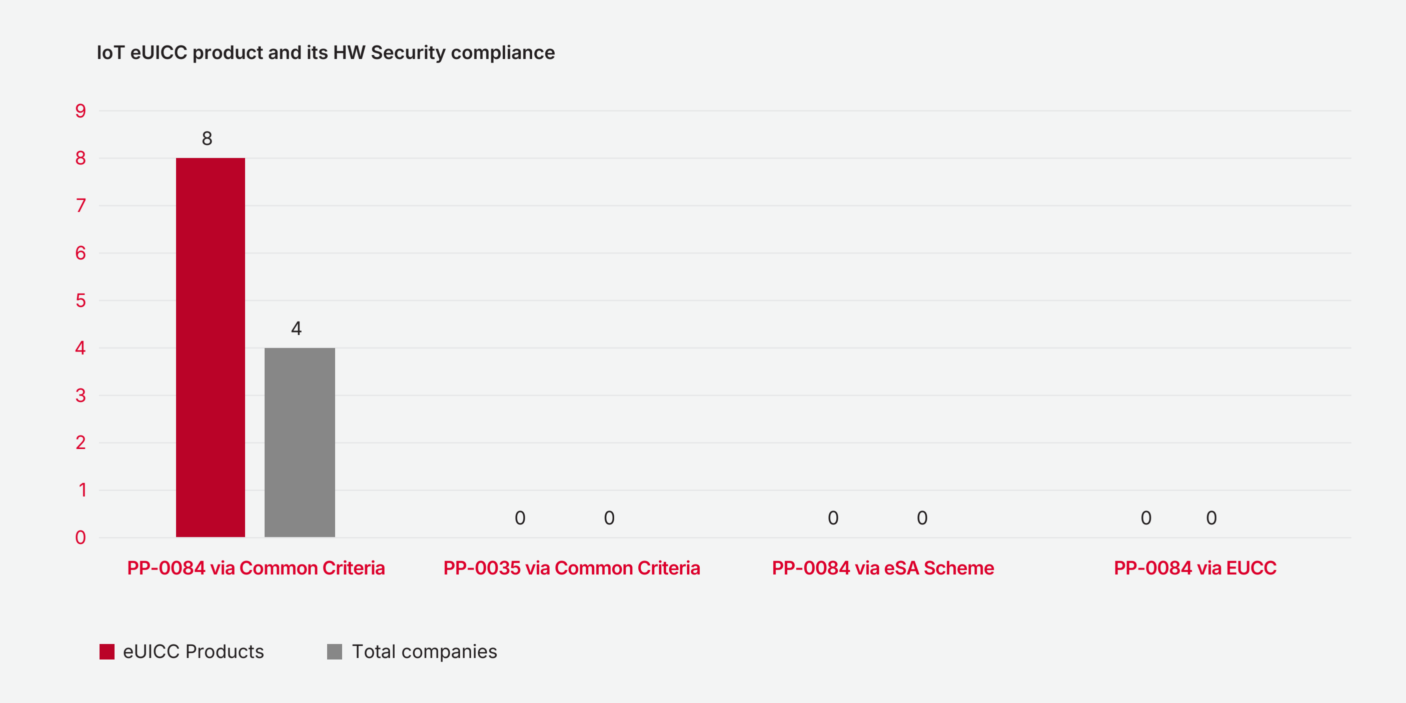
The eSA Scheme has emerged as the primary and, so far, the only method used to declare software compliance for IoT eUICCs. With participation of all 8 products from 4 different companies, its strong adoption highlights its relevance and adaptability. This success may be attributed to the scheme's optimisation for the dynamic nature of the eUICC market, effectively addressing the needs of both IoT and consumer segments. Its early traction suggests a solid foundation for broader industry alignment and future scalability.

6.3.3 Hardware Security

The hardware security requirement within the eSIM Compliance Process mandates that the GSMA IoT Protection Profile (Common Criteria PP-0084 or PP-0035) needs to be fulfilled. GSMA allowed 4 methodologies to demonstrate this hardware security requirement:

1. PP-0035 via Common Criteria Certification
2. PP-0084 via Common Criteria Certification
3. PP-0084 via eSA scheme certification (recently added, not adopted yet)
4. PP-0084 via EUCC (recently added, not adopted yet)

The following graph indicates the number of IoT eUICC products certified with each of these methodologies:



Conclusions

PP-0084 via Common Criteria

Among the four evaluated security compliance pathways, PP-0084 via Common Criteria stands out as the only one currently adopted. All 8 declared IoT eUICC products, representing 4 different companies, have used this methodology to achieve compliance—highlighting its strong industry acceptance.

PP-0035 via Common Criteria

This pathway has not been used in any of the declared IoT eUICC products. Given its historically lower adoption rate even in the consumer eUICC segment, it is evident that PP-0084 has become the preferred choice for hardware security certification.

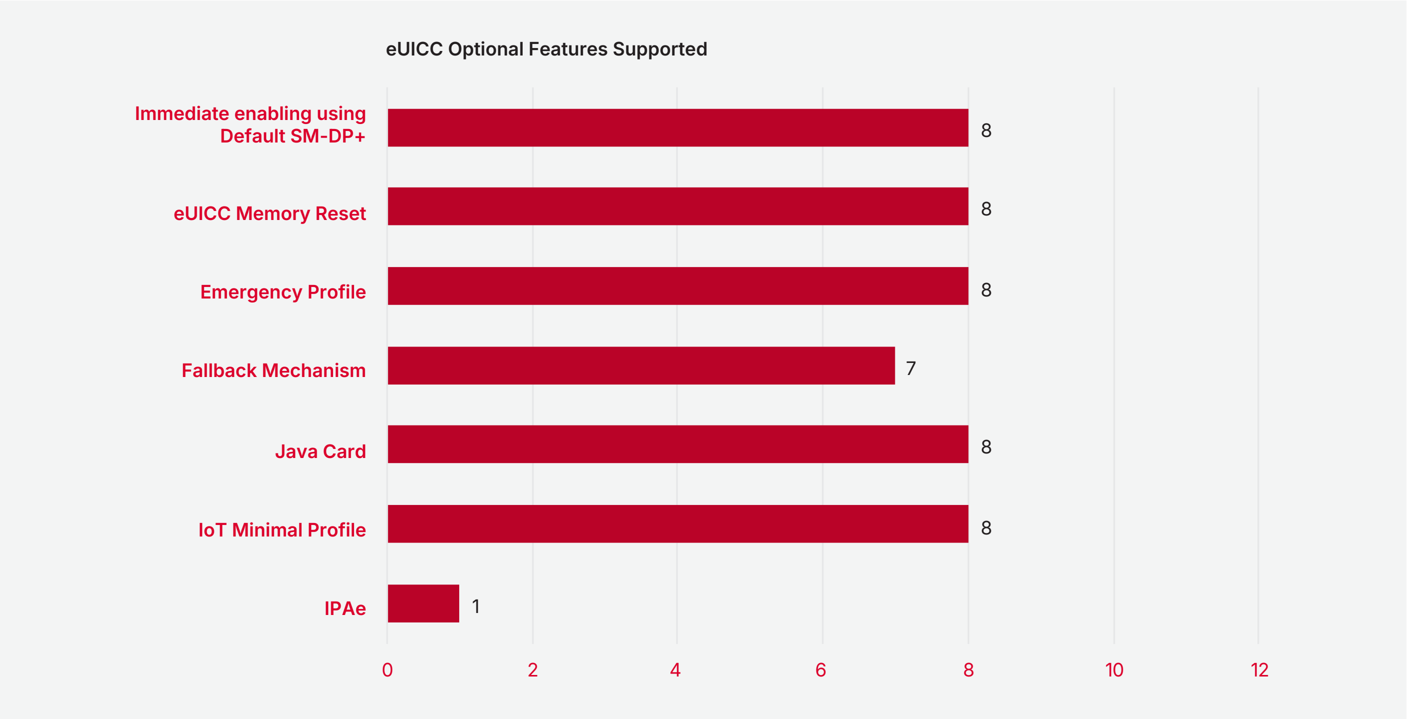
PP-0084 via eSA Scheme and via EUCC

These certification options have seen no adoption to date, which is expected as both were only introduced in early 2025.

Their uptake may still be in the early stages of industry evaluation and implementation.

6.3.4 Optional Features Supported

Since the first eSIM IoT Specification release, eUICC manufactures have the ability to indicate the optional features support by their eUICC compliance product. As such, the below table indicate the supported optional features in all IoT eUICC products since its inception:



Conclusions

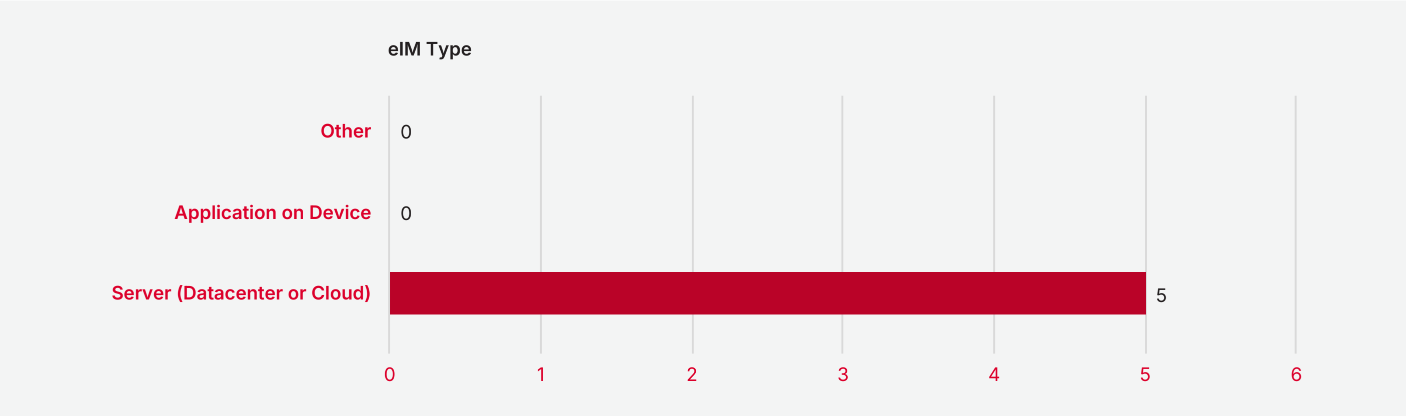
A cluster of features including **Immediate enabling using Default SM-DP+, eUICC Memory Reset, Emergency Profile, Java Card, and IoT Minimal Profile** are each supported by **8 products and Fallback Mechanism** supported by **7 products**. This suggests these features are considered foundational or highly beneficial for enabling flexible, secure, and efficient IoT operations.

In contrast, **IPAe** is supported by only **1 product**, indicating minimal adoption. This could be due to technical limitations, lack of standardisation, or insufficient support in compliance testing frameworks, such as GlobalPlatform Functional Compliance Testing.

6.4 eIM Products

6.4.1 eIM Types

The eIM products can be declared as Applications on Devices, Server (Database or Cloud and others). The following graph illustrates the eIM Types those 5 products declared so far belong to:

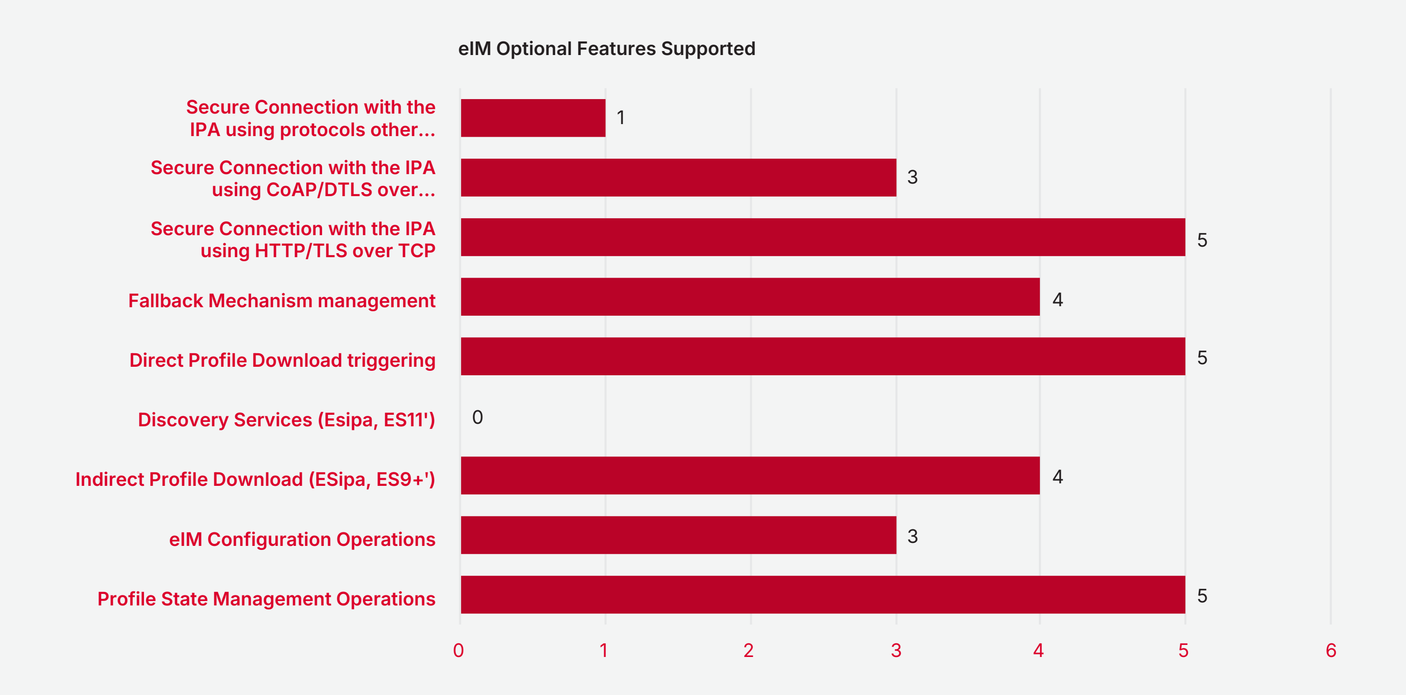


From the 5 eIM products declared to GSMA, all 5 belong to the type of Server (Database or Cloud and others) and None of these products belong to the type On-device applications. Given that specifications for declaring compliance were only published at the beginning of 2025, this early trend suggests:

- Vendors are prioritising Server solutions either Datacentre or cloud-based eIM solutions, likely due to scalability, manageability, and alignment with existing infrastructure.
- Device-based or alternative models may still be under development or awaiting further market demand.

6.4.2 Optional Features Supported

Since the first eUICC IoT specifications release, eIM Providers have the ability to indicate the optional features support by their eIM compliance product. As such, the below table indicate the supported optional features in all eIM products since its inception:



Conclusions

The most widely adopted optional features - each supported by **all 5 eIM products** - are **Secure Connection with the IPA using HTTP/TLS over TCP, Direct Profile Download triggering**, and **Profile State Management Operations.** Their relatively high uptake suggests these capabilities are considered essential for enabling secure and efficient remote profile management in IoT deployments.

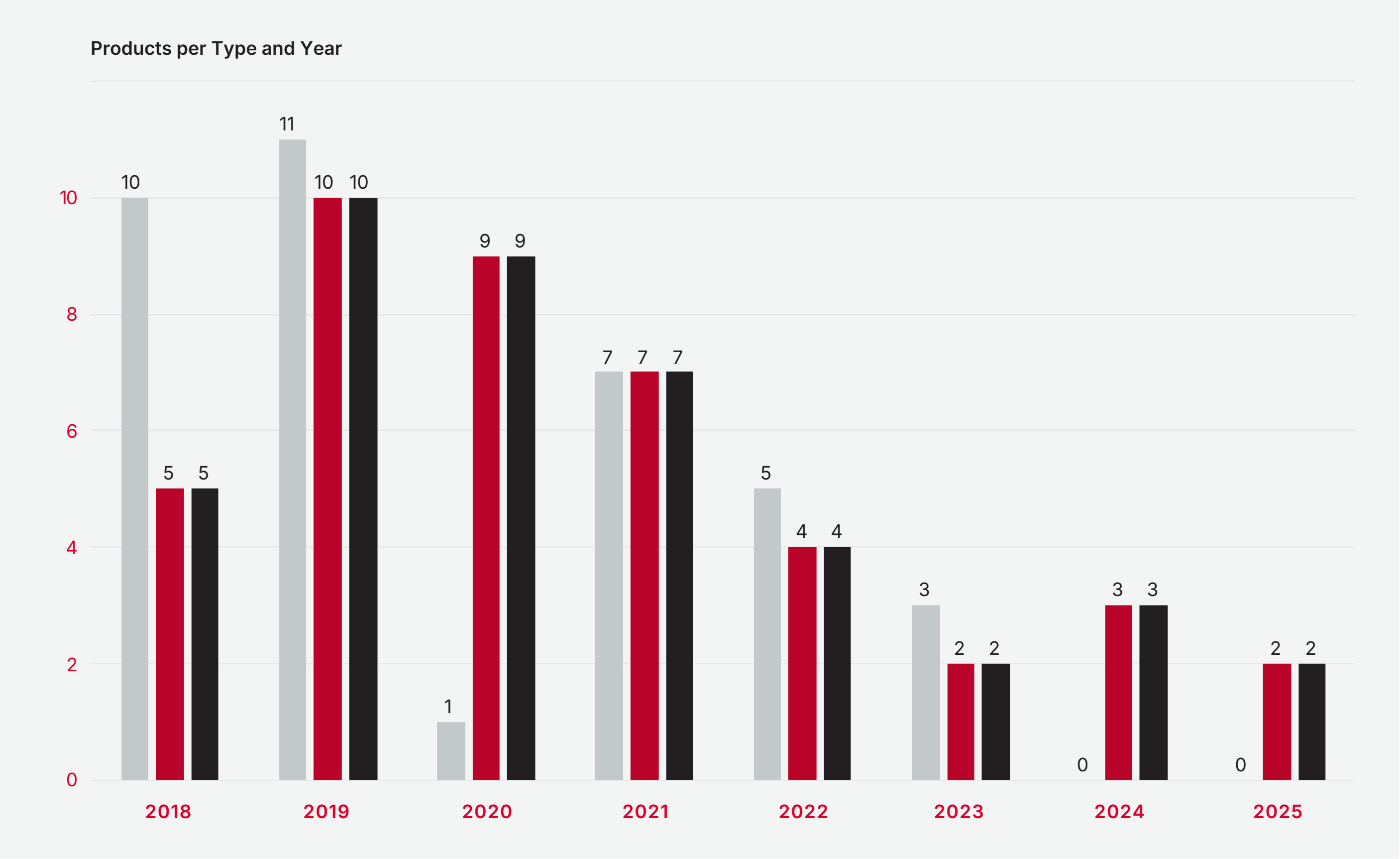
Features such as **Fallback Mechanism management and Indirect Profile Download** (ESipa, ES9+') show moderate adoption, with support from **4 products** each.

Secure Connection with the IPA using CoAP/DTLS over UDP and **eIM Configuration Operations** are each supported by **3 products**, reflecting a more selective implementation.

At the lower end, **Secure Connection with the IPA using protocols other than the specified ones** is supported by only **1 product**, suggesting minimal industry interest or readiness. Meanwhile, **Discovery Services (ESipa, ES11')** shows **no adoption at all**, indicating it is either not prioritised by vendors or still under evaluation for future relevance.

7. M2M eSIM Products

7.1 M2M eSIM Certified Products per Year



This graph illustrates the annual distribution of eUICCs, SM-DPs, and SM-SRs over the period from 2018 to 2025.

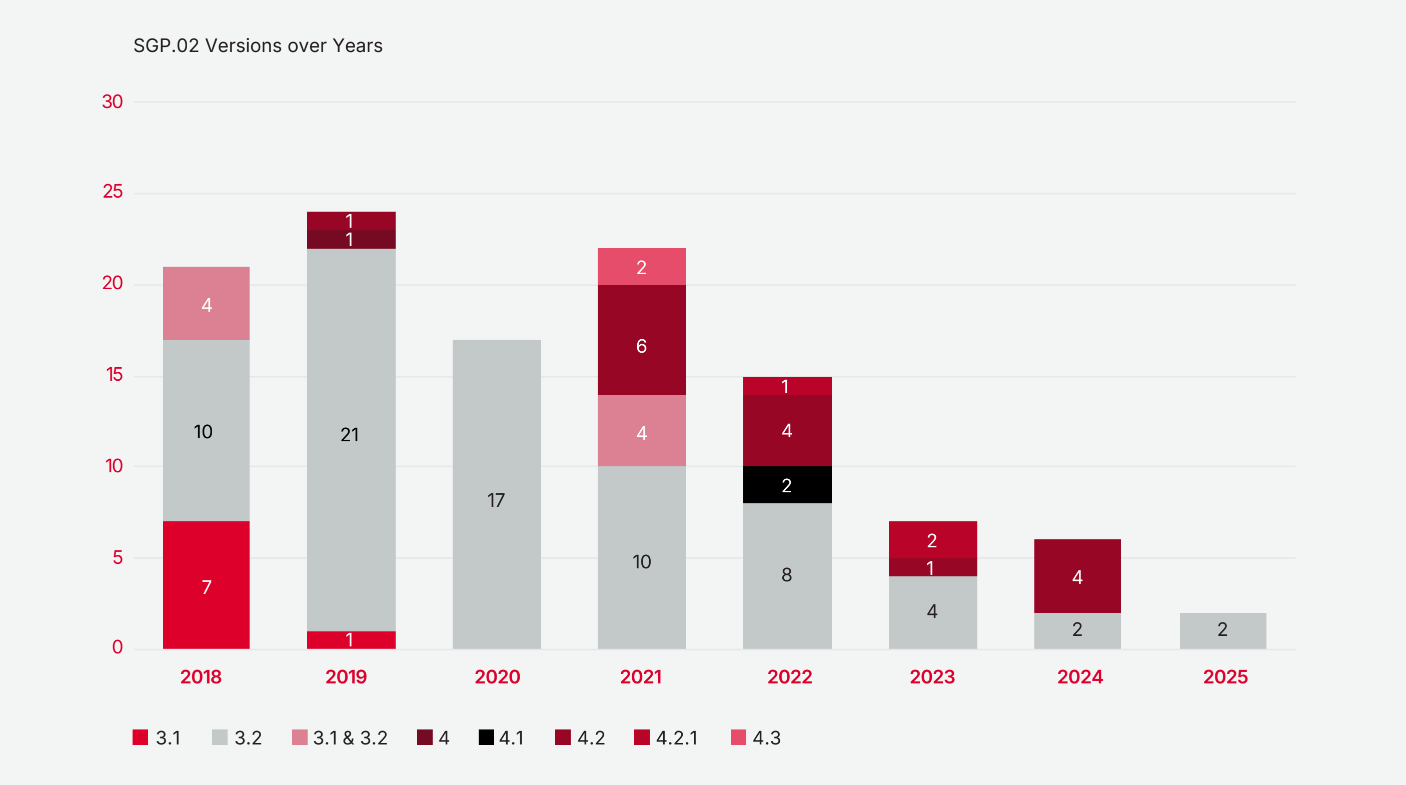
Key observations:

- **eUICC** products peaked early, with **10 products in 2018** and **11 in 2019**, leading all categories.
- **SM-DP** products also saw strong adoption, rising from **5 products in 2018** to **10 in 2019**.
- **SM-SR** products remained stable at **5 products** in both years.

Overall, the graph illustrates that from 2022 onwards, all categories experienced a decline with eUICC dropping to 5 products in 2022, then to 3 in 2023, and was absent in 2024 and 2025. Equally SM-DP and SM-SR both declined to 4 and 2 products respectively by 2023 but stabilised with 2–3 products each in 2024 and 2025.

7.2 eSIM M2M Specifications Versions

Since 2018 until now GSMA has been evolving its M2M specifications to incorporate features, correct mistakes or introduce improvements. The following graph shows how the technical versions of M2M Specifications have been used in eSIM M2M Products over the years.



This graph illustrates the versions used, the most and the least popular over the years where the following can be noted:

Most Popular Versions

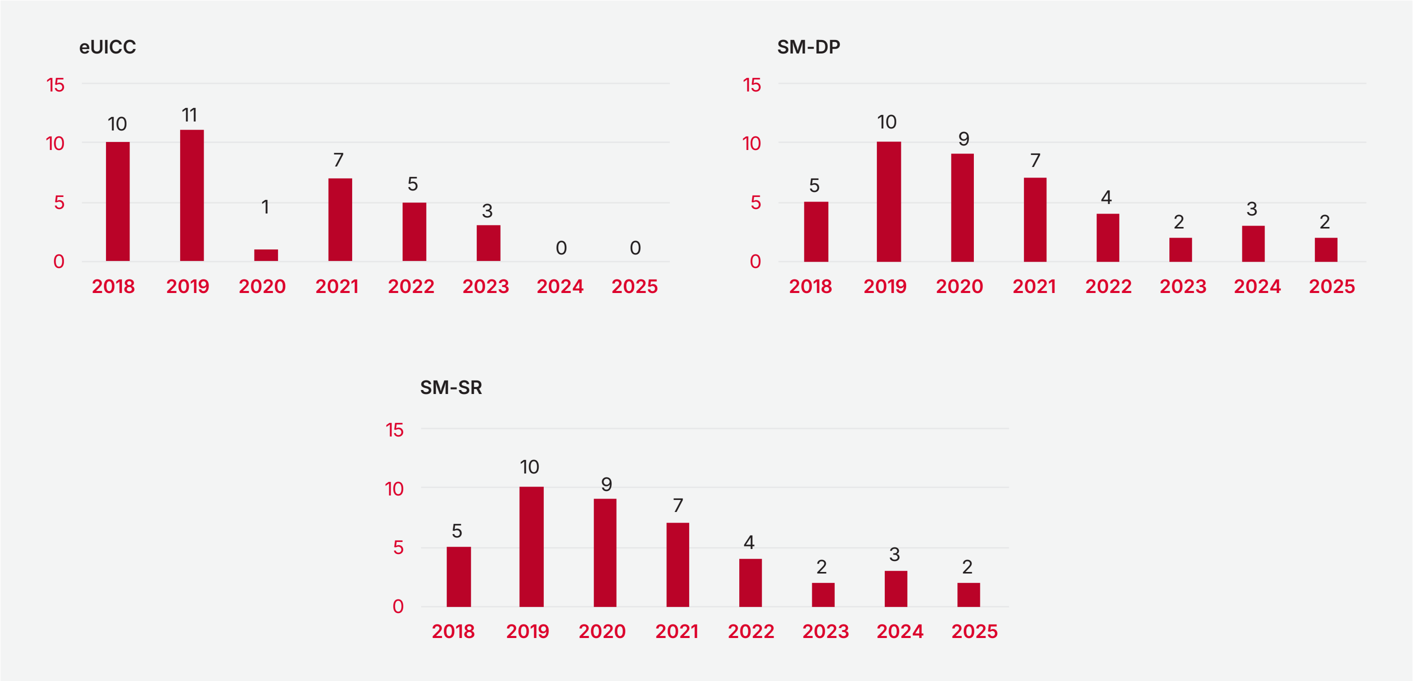
- **V3.2**, released prior to 2019, stands out as the most widely adopted version. It reached peak usage of approximately 25 products in 2019, with consistent presence through 2024, though gradually declining. This sustained use indicates that V3.2 has been a stable and trusted version over a long period.
- **V3.1**, also visible from 2018 to 2021, shows moderate adoption, especially in the early years. While not as dominant as V3.2, its early uptake suggests it was a reliable predecessor during the initial adoption phase

Recent Versions

- The **4.x series** (including **V4.1, V4.2, V4.2.1,** and **V4.3**) has emerged gradually from 2022 onwards, reflecting a transition phase in the ecosystem:
  - **V4.1** shows the earliest and most consistent adoption among the 4.x versions, with usage increasing steadily through 2025.
  - **V4.2** and **V4.2.1** appear in 2023–2024, with V4.2.1 continuing into 2025, indicating growing interest.
  - **V4.3**, introduced in 2025, is the most recent and shows initial uptake, suggesting early-stage adoption.

This trend highlights a progressive shift toward newer specifications, with the 4.x versions gaining momentum but not yet surpassing the historical dominance of the 3.x series. Their future adoption will likely depend on feature maturity, ecosystem readiness, and backward compatibility.

7.3 M2M eSIM Certified Products per Type



Market Needs Perspective

SM-SR and SM-DP Reflect Shared Lifecycle

- The SM-SR and SM-DP graphs show identical trends in deployment over time, peaking at 10 instances in 2019 and gradually declining to 2 by 2025. This parallel trajectory suggests that these components are typically deployed together, likely as part of integrated solutions.
- Their early growth followed by a steady decline may reflect a mature infrastructure that is no longer expanding, possibly due to a shift toward newer architectures.

eUICC Deployment Shows Early Momentum, Then Decline

- The eUICC graph shows a strong start, peaking at 11 in 2019, but then dropping sharply to 1 in 2020, and eventually reaching zero by 2024.
- This pattern suggests that while eUICC adoption initially surged, it may have been superseded by alternative solutions, or its deployment has stabilised in existing devices without further expansion.

Infrastructure Stability vs. Device Evolution

- The continued presence of SM-SR and SM-DP, albeit at lower levels, indicates that core infrastructure remains in place to support existing deployments.
- In contrast, the disappearance of eUICC deployments in recent years may reflect a shift in M2M device design or architectures.

7.4 eUICC Products

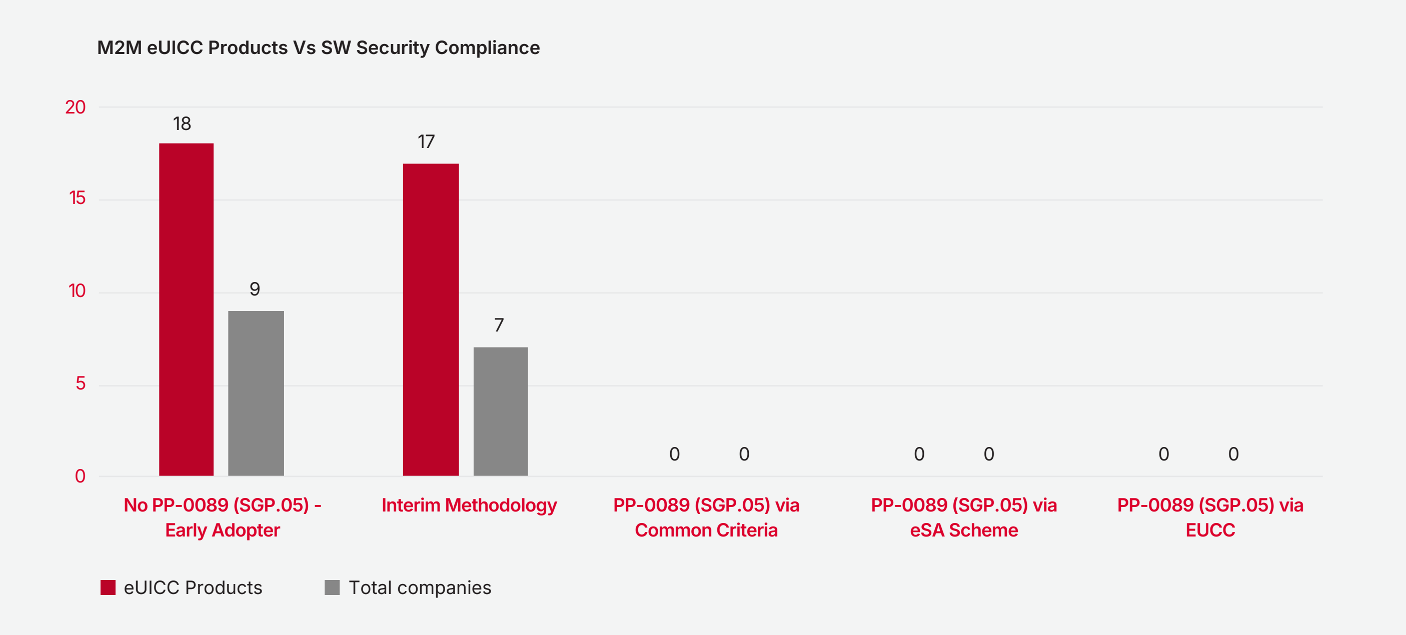
The following sections present a comprehensive overview of eUICC products declared to GSMA, categorised by product software and hardware security compliance.

7.4.1 Software Security

The software security requirement within the eSIM Compliance Process mandates that the GSMA M2M Protection Profile (Common Criteria PP-0089/SGP.05) needs to be fulfilled. Over the years, GSMA allowed 5 methodologies to demonstrate this software security requirement:

1. No compliance declared (early adopters)
2. eUICC Statement of Security Evaluation Completion (interim methodology)
3. PP-0089 Common Criteria Certification
4. PP-0089 eSA scheme Certification
5. PP-0089 EUCC Certification

Only options 3 ,4 and 5 are now possible but the following statistics indicates the number of M2M eUICC products certified with each of these methodologies:



Conclusions

No Declared Compliance – Early Adopters:

18 products from 9 companies did not declare PP-0089 (SGP.05) compliance. These represent early products, and while such declarations were once accepted, they reflect a period before stricter certification norms were enforced.

Interim Methodology:

Used in 17 products from 7 companies, this transitional compliance route was widely adopted. Though it offered a practical path during evolving standards, its use has diminished and is longer possible to use it since 2023 as more formal schemes have emerged.

PP-0089 via Common Criteria, eSA Scheme & EUCC:

No products or companies have yet adopted PP-0089 (SGP.05) through either Common Criteria, eSA Scheme or EUCC. This absence suggests that these certification paths have yet to gain traction in the M2M eUICC segment, possibly due to complexity, cost, limited industry readiness or simply lack of volumes in recent years.

Summary

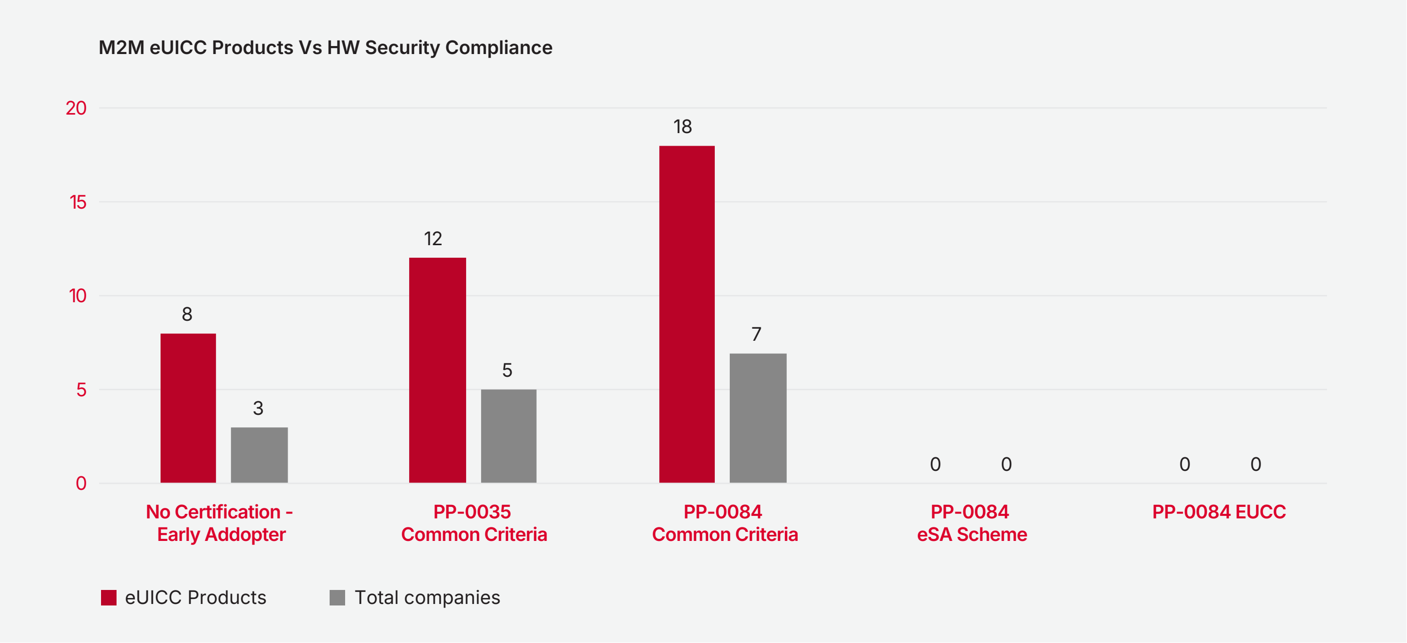
This graph illustrates a clear reliance on legacy or transitional compliance approaches for M2M eUICC products. The dominance of early adopters and interim methodology highlights the industry's initial push to market without formal certification. However, the complete lack of adoption for PP-0089 via Common Criteria, eSA Scheme or EUCC signals a gap in uptake of robust security standards probably due to an absence of new product designs in the most recent years. As expectations evolve, the industry may need to shift towards these recognised certification paths to ensure long-term security and interoperability.

7.4.2 Hardware Security

The hardware security requirement within the eSIM Compliance Process mandates that the GSMA M2M Protection Profile (Common Criteria PP-0084 or PP-0035) needs to be fulfilled. Over the years, GSMA allowed 5 methodologies to demonstrate this software security requirement:

1. No compliance declared (early adopters)
2. PP-0035 via Common Criteria Certification
3. PP-0084 via Common Criteria Certification
4. PP-0084 via eSA scheme certification (recently added, not adopted yet)
5. PP-0084 via EUCC

Only options 2 to 5 are now possible but the following statistics indicates the number of Consumer eUICC products certified with each of these allowed processes:



Conclusions

No Certification – Early Adopters:

8 products from 3 companies were launched without hardware security certification. These represent the earliest adopters products and reflect a time when formal certification was not yet standardised or enforced.

PP-0035 Common Criteria:

12 products from 5 companies comply with PP-0035, indicating moderate adoption. This certification has served as robust security standard, offering a recognised route for hardware security compliance.

PP-0084 Common Criteria:

With 18 products from 7 companies, PP-0084 is the most widely adopted certification method. Its strong uptake suggests growing industry alignment with this robust hardware security standards.

PP-0084 eSA Scheme and PP-0084 EUCC

No products or companies have adopted these method yet. This absence suggests that the PP-0084 eSA Scheme and EUCC has not yet gained traction in the M2M eUICC hardware security space, possibly due to its recent introduction in 2025 of eUICC Scheme and the recent activation of EUCC.

Summary

This graph illustrates the evolution of hardware security compliance in M2M eUICC products.

The shift from uncertified early adopters to formal certification - particularly PP-0084 - demonstrates the industry's growing commitment to robust security standards.

The complete lack of uptake for the PP-0084 eSA Scheme and EUCC highlights an opportunity for future growth, provided industry awareness and readiness improve.

8. eSA Scheme Certifications

eSA, short for **eUICC Security Assurance**, is GSMA's streamlined certification framework designed to validate the security of eUICC software. Built upon the principles of the **Common Criteria methodology**, the eSA scheme offers a globally accepted security benchmark for software developers. Its compact structure ensures a quicker, more agile certification process—perfectly suited to the evolving nature of eUICC technology.

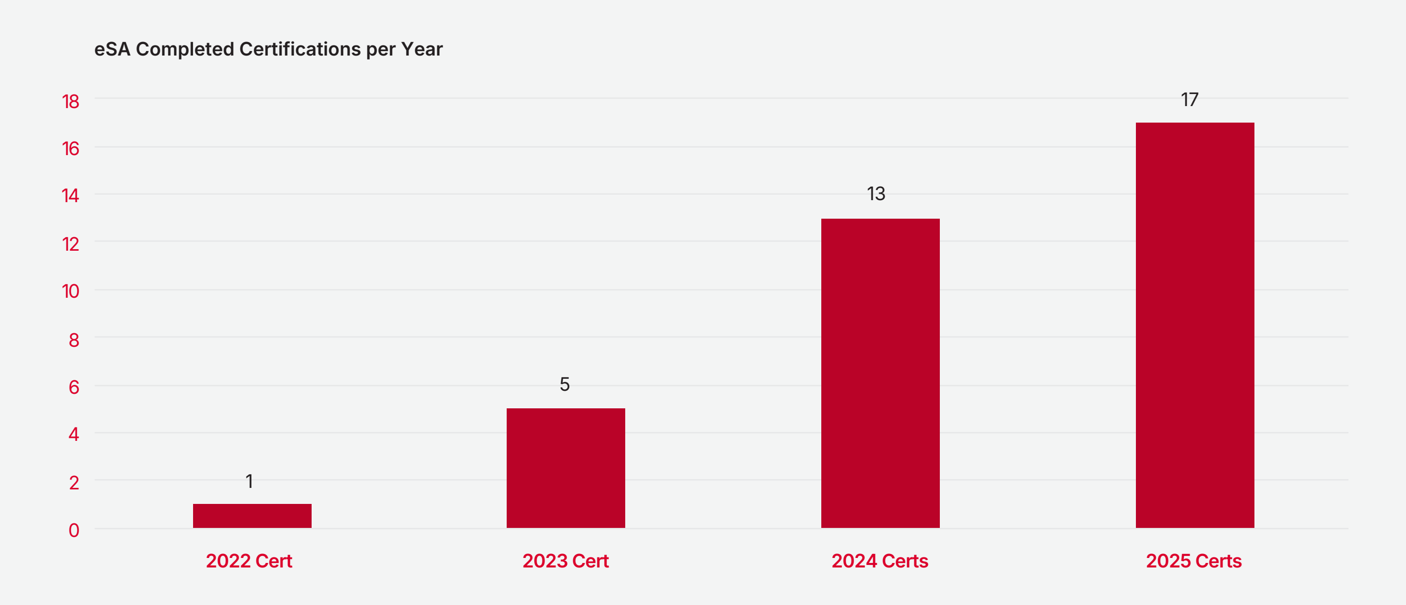
This certification model is distinguished by:

- **Global recognition across the industry**
- **Strong security resilience**
- **Rapid and efficient evaluation**
- **Continuous enhancement of security standards**
- **Independent assessment and validation**
- **Alignment with sector-wide security expectations**

The **eSA scheme** stands as one of the three approved pathways for demonstrating eUICC software security compliance to GSMA, applicable across all three eSIM architecture types: **M2M**, **Consumer**, and **IoT**.

8.1 eSA Certifications per Year

Since its launch in 2022 several eUICCs have been certified each year, as illustrated in the graph:



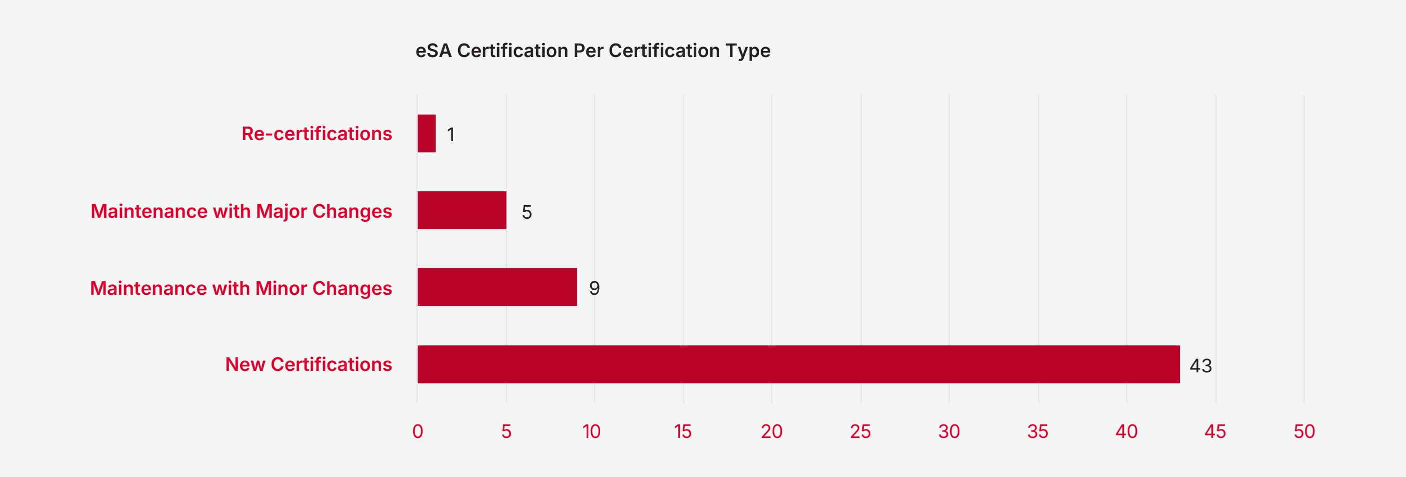
The graph illustrates a clear and steady upward trend in certification completions from 2022 to 2025. Starting with just **1 certification in 2022**, the number rose to **5 in 2023**, then surged to **13 in 2024**, and reached **17 in 2025**. This progression reflects a strong and consistent growth in certification activity year on year, suggesting increased engagement or prioritisation of this certification type.

8.2 eSA Certifications per Certification Type

The type of eSA certification are defined as follows:

Certification Type	Definition
New Certification	Applied to entirely new product evaluations.
Maintenance with Minor Changes	Used when changes to the Target of Evaluation (TOE) have no security impact.
Maintenance with Major Changes	Applied when security-relevant changes are made to the TOE.
Full Re-Certification	Used to extend the validity of an existing certificate, with or without changes to the TOE.

The number of eUICC products certified by the eSA scheme in all four categories is as follows:

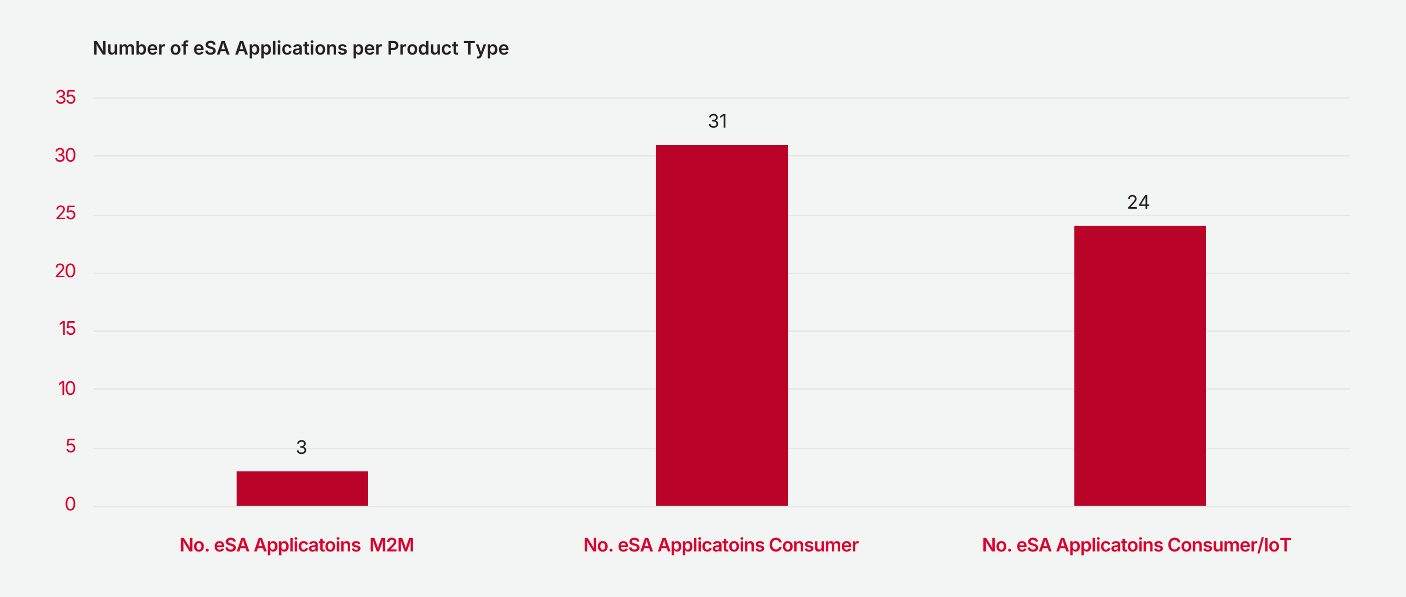


The diagram highlights a strong emphasis on **New Certifications**, which represent **43 out of the total certifications** - a trend likely driven by the recent launch of the eSA scheme in **2022**, prompting a wave of initial product evaluations. In contrast, the presence of **Recertifications with Minor Changes (9)** and **Major Changes (5)** suggests that the scheme is maturing, with existing products undergoing targeted updates and security reassessments based on the nature of the changes.

The notably low count of **Full Recertifications (1)** aligns with the scheme's recent introduction, indicating that few products have yet reached the end of their certification lifecycle. Overall, the distribution reflects a dynamic and expanding certification landscape, with a clear focus on onboarding new products while gradually building a base of maintained and evolving certified solutions.

8.3 eSA Certifications per Architecture Type

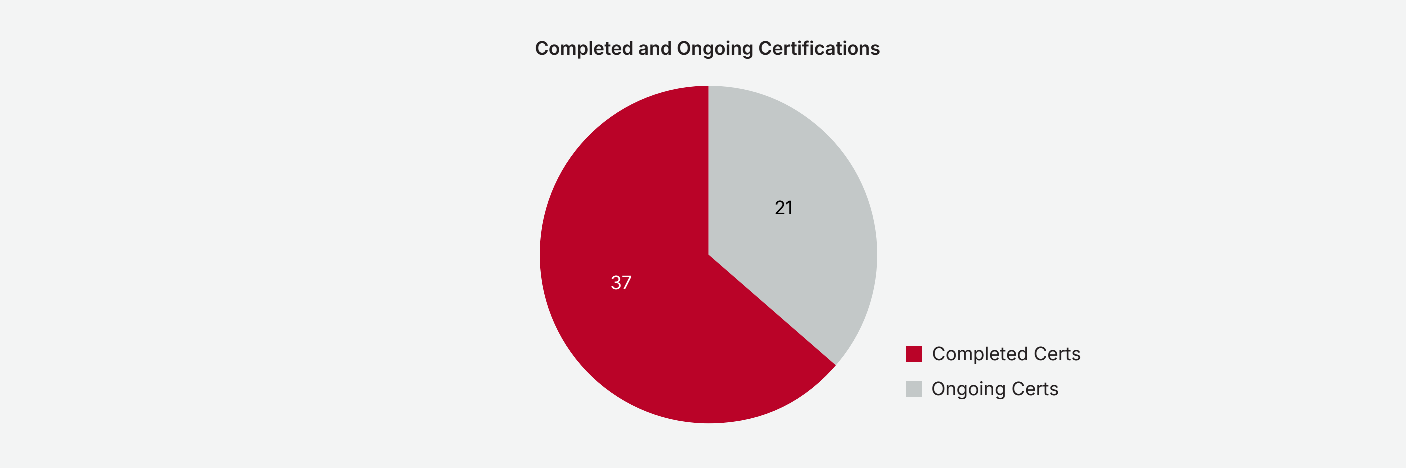
The eSA scheme applies to eUICC products developed for M2M, Consumer, and Consumer/IoT architectures. The chart below presents the number of products that have initiated the eSA application process - not necessarily completed it- for each category, offering insight into the adoption levels across different market segments.



The diagram illustrates the distribution of eSA applications across three product categories: M2M, Consumer, and Consumer/IoT. It shows a clear dominance of the Consumer segment, with 31 applications, followed by Consumer/IoT at 24, and a significantly lower count of 3 applications for M2M. This suggests that the eSA scheme is being most actively adopted in consumer-oriented products, likely due to higher market demand and faster product cycles in that segment. The limited uptake in M2M may reflect longer development timelines or more stable deployments that require fewer certifications. Overall, the chart highlights the scheme's strong traction in consumer and hybrid IoT domains.

8.4 eSA Certifications Completed Vs Ongoing

The number of completed and ongoing eUICC certifications is illustrated in the pie chart below:



The pie chart presents a clear comparison between the number of certifications that have been finalised versus those still in progress. Out of a total of 58 certifications, 37 have been completed, while 21 remain ongoing. This indicates that approximately 64% of certifications have successfully passed through the eSA process, reflecting strong momentum and operational efficiency. The remaining 36% represent active evaluations, suggesting a healthy pipeline and continued engagement with the certification scheme.

For more information on the eUICC certified products using the eSA Scheme you can check the available list HERE.

9. Conclusions

In the dynamic landscape of mobile connectivity, the adoption of eSIM technology continues to revolutionize the industry.

The GSMA eSIM Compliance Process remains a cornerstone in ensuring that eSIM products meet the stringent requirements for security and reliability, as established by industry-recognized certifications. This process guarantees that eSIM products will seamlessly integrate with various networks and devices, thereby meeting the high standards of quality expected by both the mobile industry and end users. As we move forward, the commitment to compliance and interoperability will be crucial in maintaining the trust and satisfaction of all stakeholders in the mobile ecosystem.

GSMA will continue to improve its range of processes and services to help the mobile industry achieve its goals and expectations for security and compliance of its products. Follow GSMA Industry Services for more information.

Related Information

eUICC Security Assurance (eSA) Scheme

Security Accreditation Scheme (SAS)

eSIM Consumer and IoT Compliance Process

eSIM M2M Compliance Process

eSIM Compliance Report 2024

A Guide to eSIM Architectures

eSIM Page

GSMA

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.
For more information, please visit the GSMA corporate website at www.gsma.com.

Document Editor

GSMA Staff

For further information, please visit:
https://www.gsma.com

GSMA Head Office
1 Angel Lane
London, EC4R 3AB
U.K.
Tel: +44 (0)207 356 0600
Email: info@gsma.com