GSMA

eSIM Starter Guide – Top Tips

GSMA's starter guide is aimed at those who wish to launch eSIM offerings for their customer base but who are not entirely sure of best practice and the operational topics they need to consider.

At a high level here are some key pointers to keep in mind.

Understand the Technology: Familiarize yourself with eSIM technology and its benefits. eSIMs eliminate the need for physical SIM cards, allowing for remote provisioning and greater flexibility in device management.

Make yourself aware of industry standards and updates: Key is being aware of solutions that work for all rather than bespoke solutions that cost more to implement and maintain. Interoperable solutions for new technologies are key. Stay updated with the latest eSIM standards, industry developments, and regulatory requirements. And once you are up and running, regularly assess and upgrade your eSIM infrastructure to ensure compatibility and compliance.

Security and Authentication: Implement robust security measures to protect customer data and ensure secure authentication during eSIM activation and profile changes.

Identify Target Segments: Determine the target market segments where eSIMs can provide the most value. This could include consumer wearables, travellers, IoT devices, connected cars, or other specific industries.

Define Use Cases: Determine the specific use cases for eSIM provisioning. Whether it's for IoT devices, consumer devices, or enterprise solutions, having a clear understanding of your target market and application will help tailor your provisioning strategy.

Choose the right eSIM Provider: Select a reliable eSIM provider that suits your needs. Consider factors like coverage, network compatibility, pricing, and available services. Ensure they have a robust infrastructure and support system.

Partner with Device Manufacturers: Collaborate with device manufacturers to ensure their devices support eSIM functionality. This collaboration is crucial for seamless integration and compatibility.

Offer a Range of Plans: Provide a variety of flexible data plans to cater to different customer needs. This could include options for data-only, voice and data, or specialized plans for IoT applications.

Implement Security Measures: Prioritise security when provisioning eSIMs. Utilize encryption protocols, secure channels, and other industry best practices to protect sensitive customer information during the provisioning process.

Simplify Onboarding Process: Streamline the onboarding process for customers by developing user-friendly interfaces and tools. Focus on sustainable out of the box / it just works solutions to guide them through the eSIM activation and setup steps. Minimize any potential complications or barriers.

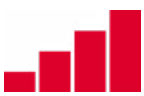
Test Provisioning Workflows: Thoroughly test your eSIM provisioning workflows before launching them. This includes verifying activation, profile download, network connectivity, and any additional services or features associated with your eSIM offering.

Offer Support Channels: Establish multiple support channels to assist customers during the provisioning process. This can include online resources, FAQs, chatbots, and customer support representatives who can address any issues or inquiries promptly.

Roaming Agreements: Establish roaming agreements with other operators to offer global connectivity for eSIM-enabled devices. Seamless connectivity across different regions is a key benefit of eSIM technology.

Customer Support: Provide dedicated customer support for eSIM-related inquiries and issues. As eSIM technology may still be new to some users, offering assistance and troubleshooting services can enhance the customer experience.

Analytics and Insights: Leverage data analytics to gain insights into customer behaviour, usage patterns, and preferences. This information can help refine your eSIM offerings and identify new business opportunities.



GSMA

GSMA eSIM Services

There is a number of services outlined briefly below which the GSMA run to support the industry in the deployment of eSIM. Most have been specified to demonstrate trust and security.

eUICC Security Accreditation Scheme (SAS) – this scheme includes eUICC manufacturing sites so mobile operators, regardless of their resources or experience, can assess the security of their eUICC suppliers through SAS-UP. It also includes SAS-SM whose focus is security auditing and accreditation for the providers of the eUICC subscription management services.

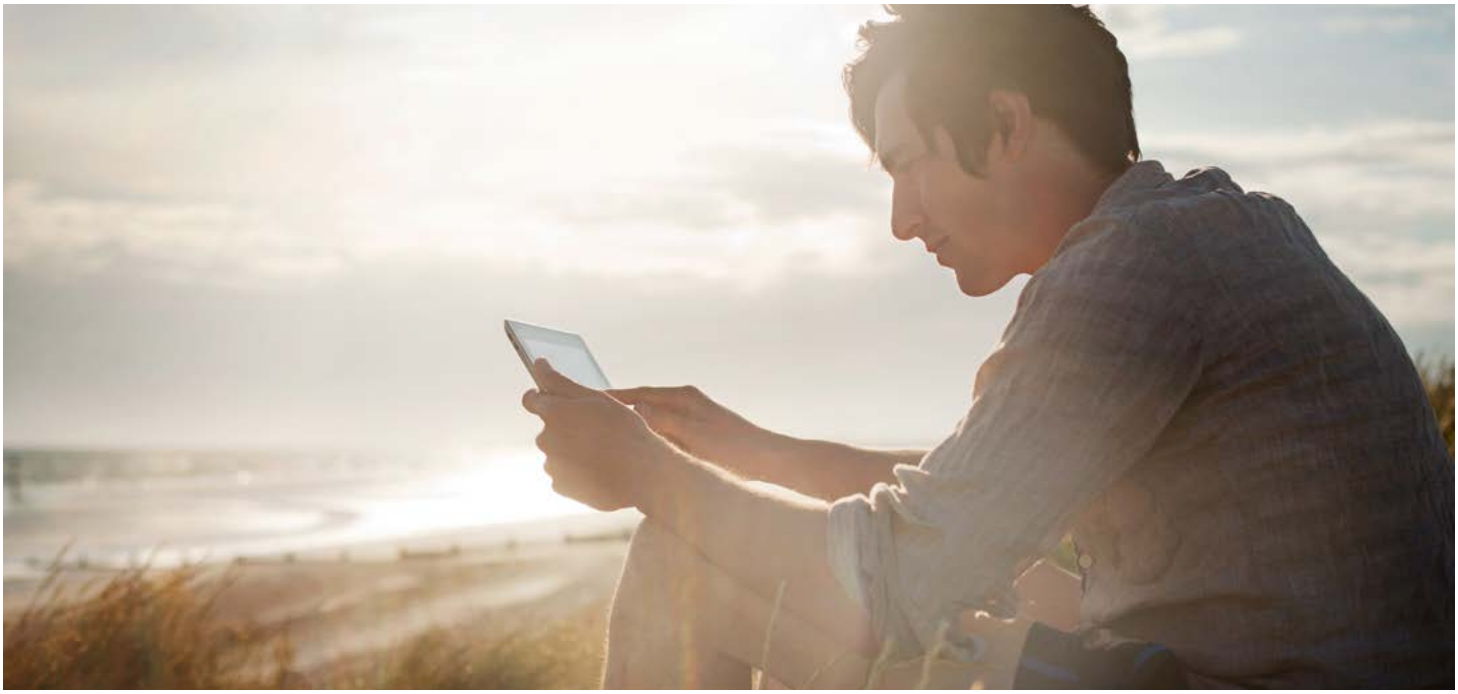
eUICC Identity Scheme (eIS) – in a similar vein to the unique IMEI number that is associated with all connected devices at a unique individual level, eUICCs require an eUICC Identification Number (EID) which is unique and persistent. eUICC manufacturers are now able to create their own unique EIDs, starting with the acquisition of their own eUICC Identification Number (EIN) at a company level. The GSMA is the industry appointed First Level EID assignment authority, as per the industry eSIM specification document, SGP.29.

eUICC Security Assurance (eSA)– this scheme focusses on the security evaluation and certification of the eUICC. All eUICC products should demonstrate robust security of their hardware and software eUICC components with either Common Criteria or GSMA eSA Scheme, don't procure any products that have not been independently endorsed through CC or eSA.

eSIM Provisioning

How are eUICC remotely switched on for activation? Known technically as remote SIM provisioning (RSP). Before we come on to talk about the GSMA's industry standard remote provisioning solution called Discovery, we need to introduce the role and need for digital Public Key Certificates (PKIs)

GSMA Public Key Infrastructure (PKIs) - are required for eSIM Consumer, IoT and M2M remote provisioning to enable eUICC and subscription management entities to identify and authenticate each other within the GSMA remote provisioning ecosystems, facilitating security and interoperability. PKI certificates are managed by GSMA Certificate Issuers (CI); organisations accredited by GSMA as GSMA Certificate Issuer. GSMA CIs meet defined criteria, GSMA PRD SGP.28 and operate GSMA accredited Certificate Issuer for certificate issuance and Maintenance, in line with the GSMA eUICC PKI Certificate Policy, GSMA PRD SGP.14.

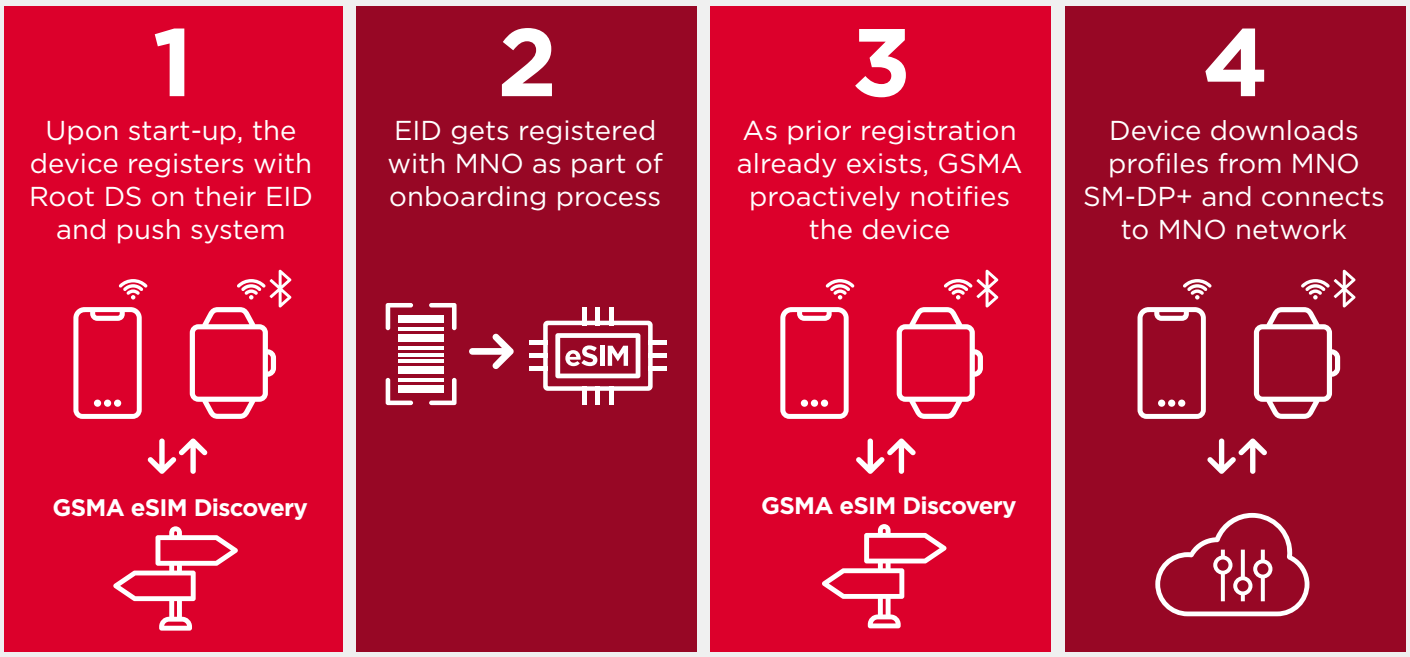


GSMA

Industry Specified RSP Solution

GSMA eSIM Discovery

GSMA eSIM Discovery is an integral part of GSMA Remote SIM Technical Specification and Architecture, SGP.21/31 eSIM Consumer/IoT Architecture Specification, and SGP.22/32 eSIM Consumer/IoT Technical Specification. Also known as Root DS, GSMA eSIM Discovery provides a universal, independent lookup service to connect MNOs and devices for streamlined eSIM downloads.



GSMA eSIM Discovery is applicable for consumer and IoT devices, and has benefits for all 3 markets.

A Better Customer Experience

- **Remote eSIM profile activation is so much easier**
- **Customers no longer have to request their profile**
- **No searching menus, scanning QR codes or switching on and off**

Greater Efficiencies for Enterprise

- **eSIM devices are activated remotely, saving time and money on employee onboarding**
- **Subsequent updates also require minimal user interaction - keeping costs down in the long-term**
- **New IoT specifications mean businesses can deploy eSIM profiles on a smaller scale**

Unlocks Opportunities for IoT

- **No need for operators to host a dedicated infrastructure for IoT projects, as they can reuse the consumer eSIM infrastructure, including GSMA eSIM Discovery**
- **Enables IoT trials in new areas without much investment**

The GSMA industry solution provides a central repository for the eSIM Device. By using the eSIM Identifier (EID), a unique identifier for each eSIM, the MNO can submit the service address and event ID to the GSMA as a pending action.

When the device starts for the first time or the customer clicks the “Add eSIM” on their devices, it automatically checks with the GSMA SM-DS if there are any pending actions/events, and, once retrieved, it prompts the customers for a confirmation and starts the download process.

GSMA

eSIM Provisioning Candidate Solutions

QR Codes

Initially, this was one of the more common ways of providing the technical information for a device to provision as it did not require MNOs to change their existing processes. The server address and event id are programmed in a QR code. Once the QR code is scanned by the device, the information is extracted and the download process kicks in.

While QR codes do not require extra integration or customization on the device side, they face longer term challenges.

- **Some devices do not have cameras, or have blocked camera access**
- **Deploying a fleet of devices will require complicated QR code matching and no automation**
- **This is not seen as a long term sustainable option due to cost**
- **The eSIM ecosystem uses modern tech**

Operator Mobile Apps

Operators might also choose to develop and deploy mobile applications to authenticate their customers, the mobile application provides the necessary information to the device directly.

While providing a more comprehensive user experience, customers may not want to install an application due to

- **Limited uses for consumers, they will need to download the mobile application for one-off use**
- **Occupying precious space on the mobile device**
- **Privacy and security concerns**
- **For corporate or centrally managed devices, operator apps can be complicated**

Next Steps

Whether an MNO, MVNO or Connectivity Service Provider it's time to start exploring the benefit of eSIMs for your customers. Start by reviewing the eSIM platform providers landscape.

You can view a list of GSMA eSIM Discovery Service Providers here.