

Unlocking seamless eSIM integration in the automotive sector and beyond

The incredible potential of the embedded IoT Profile Assistant (IPAe) to simplify IoT device connectivity management.

CONNECTIVITY

POSTED ON 08.20.24

The introduction of eSIM M2M technology has revolutionized vehicle communication, streamlining logistical processes and providing OEMs with the flexibility to seamlessly switch connectivity providers even after their products have reached end-customers.

From eSIM M2M to eSIM IoT: the pivotal role of the IoT Profile Assistant (IPA)

It comes as no surprise that, beyond the automotive industry, other sectors such as utilities, healthcare, manufacturing or logistics – to name only a few – have swiftly recognized the potential benefits of eSIM technology. However, the intricate nature of the eSIM M2M architecture has resulted in only a few successful deployments outside of the automotive sector. This has paved the way for the **emergence of eSIM IoT (Internet of Things) specification**.

The eSIM IoT specification was intended to **maximize the reuse of existing architectures** employed in another variant of eSIM – eSIM Consumer – currently used to connect millions of smartphones, smartwatches, and tablets every day. Since eSIM IoT targets different types of devices, it inherited some functionalities from eSIM M2M while also introducing a few new ones that were absent in both previous specifications. For consumer applications, such as smartphones and smartwatches, eSIM management seamlessly relies on Local Profile Assistant (LPA) functionality. **The concept of the IoT Profile Assistant (IPA) has emerged to mirror this functionality in the realm of IoT. A specific variant, known as IPAe (IPA embedded), is gaining prominence** for its potential to simplify IoT device management within the automotive industry and beyond.

Understanding the foundations of IPA

In consumer settings, eSIM technology uses familiar applications without any technical intricacies. In contrast, the eSIM IoT introduces a different framework where Original Equipment Manufacturers (OEMs) or service providers are the device owners and need to be able to control these remotely. Within this framework, **interaction takes place between the IoT Profile Assistant (IPA) and the eSIM IoT Remote Manager (eIM)**, with the eIM assuming a controlling role.

Authentication is a crucial aspect in IoT. For the eIM to effectively manage profile states on IoT devices, a secure mechanism is employed. **Each request sent to IoT devices is stamped with a secret key held by the eIM, ensuring**

proper authorization. This holds particular importance in the automotive industry, where security and authorization are paramount for vehicle communication and control systems. **The IPA facilitates this process by forwarding requests to the eSIM,** which, configured with a corresponding public key, verifies the authorization of the requesting entity.

IPAE vs. IPAd

OEMs, grappling with the challenge of mastering eSIM technology, are confronted with decisions regarding the deployment of IPA, particularly given the millions of existing devices with firmware constraints. **A pivotal distinction emerges between implementing IPA as an application component or integrating it into the device's operating system (IPAd), as opposed to making it an inherent part of the eSIM (IPAE).**

As OEMs expand their focus beyond the automotive sector, they are embracing diverse strategies. Despite the backend simplifications introduced by the eSIM IoT specification, complexities arise for device manufacturers. OEMs, operating in various industries, may encounter **challenges in implementing, integrating, testing, and certifying IPAd.** Comparatively, IPAE emerges as a prominent choice due to its potential applicability beyond automotive domains.

Addressing automotive industry challenges

In the automotive sector, where Tier-1 companies oversee TCU development, integrating IPAd presents a formidable challenge. Limited familiarity with eSIM technology poses a significant hurdle, and switching Tier-1 suppliers could result in substantial development costs. Conversely, **IPAE emerges as a game-changer, facilitating a seamless transition to eSIM IoT without necessitating firmware changes.** This advantage is beneficial for both OEMs and Tier-1 suppliers.

The promise of IPAE

The introduction of IPAE represents a significant change in approach to eSIM integration within the automotive industry. OEMs currently utilizing IDEMIA's eSIM IoT solution with integrated IPAE can **seamlessly transition to the new eSIM standard,** enjoying the benefits of a broader selection of available Mobile Network Operators (MNOs) and simplified back-end integration, all **without the need to update the TCU firmware.** With IPAE seamlessly integrated, concerns regarding validation, security, and maintenance are alleviated, placing the responsibility squarely on the device maker and ensuring a smooth lifecycle.

The broader implications of IPAE adoption

The emergence of IPAE in the realm of eSIM integration represents a significant advancement, including for applications beyond automotive use. This approach not only enhances device communication but also tackles the challenges encountered by OEMs and their suppliers, facilitating a smoother and more cost-effective transition to the new eSIM standard. As technology progresses, **the integration of IPAE is poised to play a pivotal role in shaping the landscape of IoT connectivity.**