IDEMIA

eSIM IoT à grande échelle : enseignements des premières implémentations de la spécification SGP.31/32

Surmonter les défis et assurer une intégration fluide.

CONNECTIVITÉ

POSTÉ LE 11.25.24

L'introduction de la spécification SGP.31/32 marque un tournant et ouvre de nouvelles perspectives sur le marché de la connectivité eSIM pour l'Internet des Objets (IoT).

Plus flexibles et ouvrant davantage de possibilités, les normes SGP.31/32 offrent plus de liberté pour adapter les implémentations à des besoins spécifiques. Les premiers tests d'implémentation ont révélé **la nécessité d'établir des lignes directrices et de mettre en place des bonnes pratiques en complément des spécifications** pour garantir le succès des déploiements. Cet article a pour objectif de partager des observations et des solutions pour faciliter l'intégration, assurer l'interopérabilité et optimiser les performances pour différents types d'appareils et sur différents types de réseaux.

La genèse de la spécification eSIM IoT SGP.31/32

Si la spécification M2M existante, SGP.01/02, est adaptée pour des appareils alimentés en permanence et connectés à des réseaux non limités en termes de puissance ou de bande passante, comme des voitures connectées, elle ne convient pas pour des appareils aux ressources limitées, comme des compteurs à gaz, des compteurs d'eau ou d'autres équipements alimentés par batterie.

La GSMA a proposé une nouvelle spécification eSIM IoT (SGP.31/32) pour répondre aux besoins en matière de connectivité IoT de masse et permettre la gestion à distance de flottes d'appareils IoT. De multiples acteurs y ont collaboré pour qu'elle réponde aux nouveaux cas d'usage et verticaux de l'eSIM IoT.

Les composants de la spécification eSIM IoT

La norme eSIM IoT est dérivée de la norme eSIM grand public (SGP.21/22) avec quelques adaptations pour tenir compte des spécificités des applications IoT.

Le Subscription Manager – Data Preparation+ (SM-DP+) conserve le rôle qu'il avait dans la norme eSIM grand public, à savoir gérer l'hébergement, la préparation et le téléchargement des profils eSIM.

Deux nouveaux composants sont introduits : l'eIM et l'IPA.

- **L'eSIM IoT Remote Manager (eIM)** permet de contrôler à distance une flotte d'appareils IoT. Il gère les opérations relatives à l'état des profils sur l'eSIM (c'est-à dire dans l'eUICC, ouembedded Universal Integrated Circuit Card) : activation, désactivation, suppression et téléchargement des profils à distance.
- **L'IoT Profile Assistant (IPA)** joue le rôle de médiateur entre l'eSIM et l'eIM. Il permet le téléchargement et l'installation des profils eSIM par l'intermédiaire du SM-DP+.

Des expérimentations pour tester les solutions SGP.31/32 de A à Z

Au cours des deux dernières années, la nouvelle spécification SGP.31/32 a fait l'objet de nombreux tests d'implémentation en prévision des déploiements commerciaux prévus à grande échelle fin 2025. Les principaux fabricants d'appareils et les opérateurs mobiles ont collaboré avec les fournisseurs de services pour identifier les solutions les plus efficaces et performantes en pratique et identifier les compléments à apporter de façon à réaliser les déploiements de la manière la plus simple et la plus efficace possible.

Principaux défis de la spécification SGP.31/32

Défi n°1 : Pas de migration prévue entre les implémentations M2M et IoT

Les déploiements M2M existants resteront opérationnels selon leurs modalités actuelles jusqu'à la fin de leur cycle de vie. Cela imposera de **gérer simultanément les systèmes M2M existants et les nouveaux déploiements IoT**, par exemple pour les constructeurs automobiles qui ont déjà mis en œuvre la spécification M2M mais qui passeront à la spécification eSIM IoT pour bénéficier de son architecture de déploiement plus simple et moins contraignante.

Un système de gestion centralisé apparait comme une nécessité pour gérer tous les appareils, qu'ils soient IoT ou M2M. Ce système doit fournir un point d'accès unique et permettre de définir des règles pour gérer la connectivité selon les besoins métier. Par exemple, il pourrait permettre de configurer à distance et automatiquement le changement de fournisseurs de connectivité pour une flotte traversant une frontière, sans avoir à se soucier de la spécification eSIM (M2M ou IoT) utilisée pour connecter chaque voiture ou appareil de cette flotte.

Défi n°2 : La grande diversité des appareils IoT

Pour faire face à la diversité des appareils IoT, amenée à croître de manière exponentielle, la spécification eSIM IoT offre une plus grande souplesse quant à l'emplacement de l'IoT Profile Assistant (IPA). Un IPAe est situé dans l'eUICC, tandis qu'un'IPAd est intégré directement dans l'appareil.

- **L'IPAd (IoT Profile Assistant dans l'appareil)** est la solution adaptée pour les appareils dotés de systèmes d'exploitation robustes et d'une puissance de calcul suffisante. C'est au fabricant de l'appareil que revient la responsabilité de développer le logiciel et de respecter les protocoles nécessaires.
- **L'IPAe (IoT Profile Assistant dans l'eUICC)** est idéal pour les appareils qui ne peuvent pas supporter l'IPAd comme les appareils à faible puissance, ou lorsque le fabricant préfère ne pas se charger lui-même du développement. C'est alors le fournisseur de l'eUICC qui s'en occupe. Cette option plus simple pour le fabricant ne nécessite pas de développement supplémentaire de sa part.

Bien que l'IPAe et l'IPAd offrent les mêmes fonctionnalités, **l'intégration de l'IoT Profile Assistant à l'eUICC (IPAe) présente des avantages considérables** pour les fabricants d'appareils et rend plus facile la gestion à distance de la carte eSIM.

Pour gérer efficacement des appareils IoT aux caractéristiques diverses, les fabricants d'appareils devraient également privilégier une solution capable de **générer les profils eSIM en temps réel** et de les adapter au dernier moment, juste

avant le téléchargement.

Défi n°3 : L'interopérabilité entre l'eIM et l'IPA

Pour plus de flexibilité la spécification SGP.31/32 laisse aux fabricants la liberté de choisir les **protocoles de communication** entre l'eIM et l'IPA. Une architecture modulaire du composant eIM, capable de communiquer avec divers IPA (IPAe ou IPAd) fournis par différents vendeurs, sera à même de garantir l'interopérabilité, quel que soit l'appareil.

Défi n°4 : L'évolutivité des besoins

Les entreprises doivent être capables d'assurer la connectivité d'un nombre très important d'appareils et de gérer les fluctuations d'activité, à l'instar d'un opérateur logistique qui déplace à travers les frontières toute une flotte de biens de valeur équipés de traceurs. La disponibilité de ces systèmes critiques doit être assurée à l'échelle mondiale. **Le déploiement de solutions eSIM dans un cloud public** permet de gérer ces fluctuations et de supporter efficacement les augmentations de charge.

Défi n°5 : La sécurité

Les déploiements dans des clouds publics offrent également une sécurité accrue, avec des mises à jour et des correctifs réguliers, une protection robuste contre les attaques par déni de service distribué (DDoS), une redondance des systèmes facilitant la reprise des services en cas de sinistre, un contrôle d'accès rigoureux et le chiffrement des données.

L'eIM introduit par la spécification SGP.31/32 impose des protocoles de sécurité de communication spécifique avec l'eUICC, celle-ci ne pouvant accepter que les demandes provenant d'un eIM autorisé et authentifié. **La certification SAS (*Security Accreditation Scheme*) pour les eIM**, bien que non obligatoire, est un gage de sécurité supplémentaire.

Étant donné que de nombreux appareils IoT resteront en service pendant des décennies, il est également essentiel d'anticiper l'éventualité des menaces quantiques en choisissant un fournisseur de solutions eSIM qui prend en charge la **cryptographie post-quantique**. Les solutions cryptographiques existantes doivent être évaluées et des mesures préventives doivent être prises pour assurer la sécurité de la connectivité des appareils de façon pérenne, avec la possibilité de faire des mises à jour une fois les appareils en service.

Défi n°6 : Les petits appareils à la puissance limitée

Intégrée à la carte mère, l'iSIM (*integrated SIM*) répondra aux besoins des appareils IoT particulièrement limités en termes de taille et d'énergie, ainsi qu'à ceux des appareils t déployés dans des environnements difficiles. **Une iSIM certifiée SGP.31/32** s'intégrera parfaitement à une solution de gestion complète de l'eSIM IoT.

Assurer une implémentation efficace et fluide de l'eSIM IoT

Les premières solutions eSIM IoT mises en œuvre conformément à la spécification SGP.31/32 ont confirmé la flexibilité et les possibilités offertes par la nouvelle spécification GSMA, ainsi que son potentiel pour transformer la connectivité IoT et stimuler l'adoption de l'eSIM. Ces premiers tests d'implémentation ont également permis d'identifier plusieurs défis majeurs.

En adoptant quelques bonnes pratiques et grâce aux enseignements des premières implémentations, l'écosystème IoT peut tirer pleinement parti des promesses de la technologie eSIM IoT.