Les clés du succès pour les déploiements de l'eSIM IoT

Les facteurs qui feront toute la différence pour les opérateurs alors qu'ils se préparent au déploiement commercial de la spécification SGP.32.

CONNECTIVITÉ

POSTÉ LE 04.02.26

Une étude récente sur le marché de l'eSIM IoT menée par Kaleido Intelligence pour IDEMIA Secure Transactions (IST) confirme que les opérateurs ont unanimement décidé d'adopter la spécification GSMA SGP.32 pour accélérer leurs feuilles de route dans l'Internet des Objets (IoT) : 100 % sont déjà engagés dans son déploiement. Si certains mènent déjà des preuves de concept ou préparent un lancement commercial, la plupart en sont encore aux premières phases de développement, avec des lancements prévus, au plus tôt, pour 2027.

Cette étude met en évidence :

- Les principaux moteurs d'adoption de l'eSIM IoT par les opérateurs et les fabricants d'objets connectés
- Les défis les plus importants qu'anticipent les opérateurs alors qu'ils se préparent à déployer la spécification SGP.32
- Leurs stratégies de commercialisation et les opportunités de monétisation qui émergent

Télécharger le rapport

Si vous êtes encore en train d'affiner votre stratégie et de comparer les différentes solutions eSIM IoT du marché, voici nos recommandations pour ne pas passer à côté de ce moment décisif.

1/ Fluidifiez votre intégration SGP.32 et concentrez-vous sur votre cœur de métier

Bien que la spécification SGP.32 ait été conçue pour simplifier l'architecture et réduire la complexité d'intégration technique par rapport au précédent standard M2M (SGP.02), **80 % des opérateurs voient encore les coûts et la complexité à long terme comme le principal défi de déploiement.** Cette prudence reflète la pression sur les marges sur le marché de la connectivité IoT, ainsi que le manque de recul sur le déploiement de la spécification SGP.32 à ce stade. Cependant, ces préoccupations sont largement compensées par une forte demande des clients IoT, qui y voient l'opportunité d'étendre l'usage de l'eSIM à un éventail plus large d'appareils, dont ceux à faible consommation d'énergie.

Voici quelques pistes si vous souhaitez tirer pleinement parti de la nouvelle spécification et en faire un moteur de croissance pour votre activité IoT :

- **Réduire au minimum les frictions d'intégration** avec les fabricants d'appareils (OEMs) et les entreprises clientes
- **Confier la charge de la certification** à votre fournisseur de solutions eSIM
- **Simplifier l'intégration** des flux de travail digitaux liés à l'eSIM avec vos systèmes existants
- **Mener des tests d'interopérabilité**, afin de pouvoir déployer à grande échelle en toute confiance

Éviter les coûts supplémentaires et les imprévus liés à l'intégration logicielle commence par l'adoption d'une solution eSIM clé en main qui permet d'exposer directement les services de gestion eSIM à vos partenaires de l'écosystème IoT et à vos clients via **une API unique et des interfaces utilisateur intuitives**. Une plateforme agnostique, qui prend en charge tous les types d'appareils, plusieurs formats de carte (SIM, eSIM, iSIM) ainsi que des références uniques pour les eUICC et les profils, simplifiera vos opérations et vous permettra de vous concentrer sur votre cœur de métier : fournir la connectivité.

Choisir un fournisseur eSIM qui propose **des solutions complètes, certifiées par la GSMA,** comme IDEMIA Secure Transactions[2], fluidifiera votre déploiement et limitera l'impact que pourrait avoir l'évolution des exigences de conformité et de sécurité. En réduisant vos efforts d'intégration et de certification, vous pouvez vous concentrer sur **la modernisation de vos systèmes BSS**[3], afin de mettre en place des flux de travail eSIM entièrement digitalisés et très efficaces, ce qui constitue le 2e principal défi selon 71 % des répondants à notre étude. Cela permettra également de libérer des ressources pour **résoudre les éventuels problèmes d'interopérabilité** encore présents, une étape essentielle avant l'adoption à grande échelle de l'eSIM pour l'IoT.

2/ Protégez vos activités IoT contre la fraude, les cyberattaques et les menaces quantiques

Les risques liés à la sécurité et à la fraude sont le troisième défi mis en évidence par les répondants à notre étude (par 52% d'entre-eux), et à juste titre. À mesure que la connectivité IoT se développe, la surface d'attaque s'élargit. La cybersécurité en général, et tout particulièrement la robustesse des **mécanismes cryptographiques** mis en place, ainsi que des **capacités de détection avancées**, seront essentiels pour protéger vos systèmes IoT et ceux de vos clients. Des téléchargements ou des opérations de provisionnement de profils eSIM non autorisés pourraient compromettre la sécurité de votre réseau, son intégrité et la continuité de vos services. Des implémentations cryptographiques inadaptées ou obsolètes, au niveau de la plateforme de gestion eSIM ou des appareils, pourraient également entraîner des perturbations majeures de service à moyen terme. Pour assurer la pérennité de vos opérations face à ces risques, il est important :

- **D'appliquer les principes de** zero-trust, c'est-à-dire vérifier l'identité des appareils, authentifier chaque utilisateur et chaque requête, appliquer le principe du moindre privilège et assurer une surveillance continue
- **De détecter les schémas inhabituels de téléchargement de profils eSIM,** grâce à l'analyse de données par l'IA
- **D'anticiper les menaces de cybersécurité émergentes**, grâce à la crypto-agilité

Alors que les *Security Accreditation Schemes* de la GSMA (*SAS-SM* et *SAS-UP*) définissent le socle général de sécurité pour la gestion eSIM et la production d'eUICC, le cycle de vie très long des appareils IoT, qui peut dépasser 20 ans, fait des **capacités de sécurité continue** un enjeu stratégique. Certains collectent déjà les données chiffrées pour les déchiffrer plus tard, et d'ici 15 à 20 ans, les ordinateurs quantiques devraient être capables de casser les protocoles cryptographiques asymétriques actuellement utilisés. Pour anticiper les risques de sécurité qui émergent et protéger vos déploiements eSIM IoT, la préparation face au quantique est essentielle à tous les niveaux (eUICC, plateformes eIM et SM-DP+). Cela commence par des puces prêtes pour l'ère quantique, c'est-à-dire conçues pour **supporter la transition vers des protocoles cryptographiques hybrides** qui combinent cryptographie classique et post-quantique. Il faudra également être en mesure de **mettre à jour à distance le système d'exploitation des eSIMs** afin d'assurer la

crypto-agilité des appareils à long terme, en permettant aux systèmes cryptographiques de s'adapter sur le terrain en fonction de l'évolution des menaces de cybersécurité.

3/ Apportez de la valeur à vos clients entreprises et OEMs, au-delà de la connectivité

Comme le souligne Matthew Iji, *Director of Forecasting & Modelling* chez GSMA Intelligence dans son billet de blog d'août 2025 intitulé *IoT: Big Growth, Bigger Questions* : « Le succès ne sera pas simplement une question d'échelle, il viendra de ceux qui savent simplifier la complexité, créer une valeur tangible et faire de l'IoT un élément incontournable pour les secteurs qu'ils accompagnent. » [4] Ce point de vue est partagé par 97 % des répondants à notre étude, qui confirment que la baisse de l'ARPU *(Average Revenue per Device)* influence leur stratégie et les incite à **explorer de nouveaux leviers de monétisation** au-delà de la connectivité. Cela passe par des services professionnels (comme le conseil, l'intégration et le support), des services à valeur ajoutée (du type business intelligence, cybersécurité ou gestion des appareils), ou par la combinaison de l'ensemble de ces services au sein de solutions IoT complètes et clé en main.

Chez IDEMIA Secure Transactions nous allons au-delà de la simple mise en œuvre de la spécification eSIM IoT. Nous mobilisons notre expertise en cryptographie post-quantique, en intelligence artificielle, en analyse de données et en matière de services OTA avancés, et nous tirons parti de nos relations étroites avec les OEMs pour vous aider à développer **des services IoT qui feront la différence.**

---

[1] Enquête en ligne sur le marché eSIM IoT menée par Kaleido Intelligence pour IDEMIA Secure Transactions à l'été 2025 auprès de 154 MNOs, MVNOs et MVNEs.
[2] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/sas-accredited-sites/
[3] Business Support System
[4] https://www.gsmaintelligence.com/blogs/iot-big-growth-bigger-questions

---