

Proposal

Consultation ARCEP Préparer le future des réseaux mobiles

September 23th, 2022 R.1.0

Introduction

Major trends are impacting our world: the explosion in demand for security in the consumer space as well as in the government spaces, the rise of physical to digital and the need for convenience and frictionless experiences.

In the face of its challenges, IDEMIA conceives security in a global way, upstream of technological developments, by factoring in the customer's environment and how they specifically use technology. In a world of ever-increasing exchanges, security primarily means protecting identities. This is why IDEMIA places Augmented Identity at the heart of its actions.

IDEMIA places the client, consumer or citizen at the heart of everything it does, combining security, convenience, the human factor and continuity within a single proposition. This capability for integration is what we call the «magic combination».

It is the result of our talents, of the women and men who anticipate, think, design, develop, protect and market our security solutions of today and tomorrow: 13,000 employees working for a safer world. Identify and protect, contribute to progress in our society, provide every individual with a recognizable and secure identity. Create trust at every level: a country, a firm, an IT system or just a smartphone. These are our commitments at IDEMIA.

Table of content

| | |
|---|----------|
| 1 / About IDEMIA | 4 |
| 1.1 > Company overview | 4 |
| 1.2 > Enter the world of Augmented Identity | 4 |
| 2 / Our strengths | 7 |
| 2.1 > Leading trusted identities for an increasingly digital world | 7 |
| 2.2 > Delivering future-proofed innovation | 8 |
| 2.3 > Serving clients in 180 countries | 8 |
| 3 / Réponses à la consultation ARCEP | 9 |
| 3.1 > La 5G : une innovation de rupture qui continue d'évoluer vers la 6G | 9 |
| 3.2 > Les évolutions d'architecture des réseaux mobiles | 9 |
| 3.3 > Les usages et les besoins en fonctionnalités attendus | 10 |
| 3.4 > Innovation et développement économique | 10 |
| 3.5 > Différentes réponses techniques possibles | 11 |
| 3.6 > Évolution de l'écosystème pour répondre aux besoins des verticaux | 11 |
| 3.7 > Couverture et qualité de service des réseaux ouvert au public | 12 |
| 3.8 > Questions spécifiques à la couverture à l'intérieur des bâtiments | 12 |
| 3.9 > Numérique soutenable | 12 |
| 3.10 > Mutualisation | 13 |
| 3.11 > Questions spécifiques par bande de fréquences | 13 |
| 3.12 > Les fréquences harmonisées au niveau européen qui pourrait faire l'objet d'une attribution à court terme | 13 |
| 3.13 > Les fréquences identifiées à l'UIT en cours d'harmonisation européenne | 13 |
| 3.14 > Des bandes prospectives, en cours de discussion mondialement | 13 |
| 3.15 > Autres sujets éventuels | 14 |

1 / About IDEMIA

1.1 > Company overview

En tant que leader des technologies d'identité, IDEMIA se donne pour mission d'ouvrir le monde et de le rendre plus sûr. En s'appuyant sur sa R&D à la pointe de l'innovation, IDEMIA développe des technologies uniques au monde grâce à son savoir-faire historique en matière de biométrie, de cryptographie, d'analyse de données, de systèmes et d'appareils intelligents.

IDEMIA propose à l'ensemble de ses clients publics et privés des solutions de paiement, de connectivité, de contrôle d'accès, de voyage, d'identité et de sécurité publique. Chaque jour, IDEMIA sécurise ainsi des milliards d'interactions physiques et digitales partout dans le monde.

Avec près de 15 000 collaborateurs, IDEMIA compte parmi ses clients plus de 600 organisations gouvernementales, plus de 2 300 entreprises, répartis sur 180 pays dans le monde, en ayant à cœur d'avoir une démarche à impact, éthique et responsable.

Pour plus d'informations, rendez-vous sur www.idemia.com et suivez-nous @IDEMIAGroup sur Twitter.

IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters. We provide Augmented Identity for international clients from Financial, Telecom, Identity, Public Security and IoT sectors.

With 13,000 employees around the world, IDEMIA serves clients in 180 countries.

1.2 > Enter the world of Augmented Identity

We provide customized solutions in a world that evolves and advances faster than ever before. Today, information travels rapidly around the digitized space, defying boundaries and breaking the traditional codes of security. But our industry expertise, our knack for foresight and our keen ability to adapt has brought us to the forefront of our industry and continues to push us even further every day.

Leading us into the future

Being a leader means staying on top of the disruptive innovations that impact our security landscape. We understand the need to secure people in both their physical and digital worlds, especially as connectivity growth will keep fostering more and more digital services. We know that in our globalized society, the number of peer-to-peer exchanges, travel and border crossings are exploding. We are aware that the digitalization of the economy brings about a wave of new business models and opportunities to reinvent the customer journey where data, security and privacy have an essential role to play. We are also mindful of the consumerization of technology and how it impacts our identity and private life.

Empowering people to enjoy life through Augmented Identity

At IDEMIA, we embrace this new reality and we understand the security concerns that accompany advancement. We analyzed the world around us and reinvented the concept of identity. We call it Augmented Identity – an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions. An identity that is so enhanced, adaptable, strengthened and self-sovereign that it allows us to truly enjoy life – because securing our identity is key to making our world a safer place

A safer, more streamlined identification

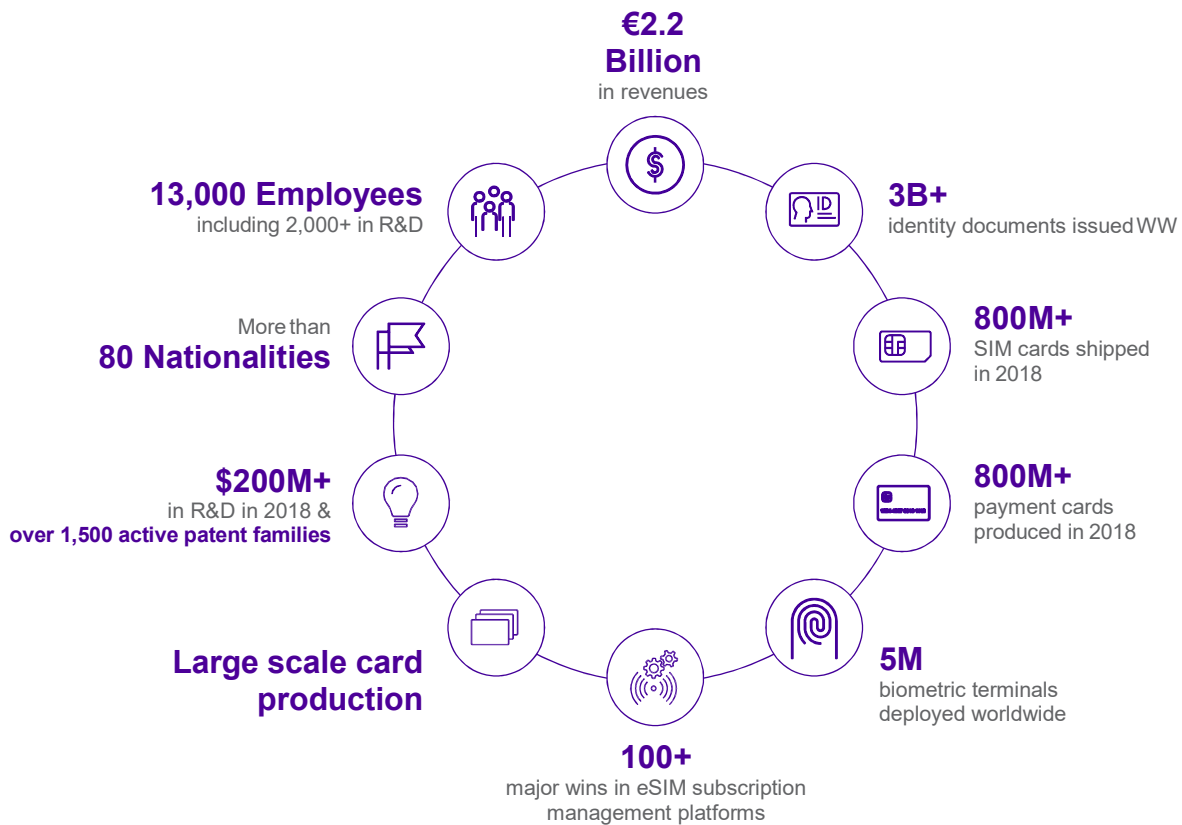
We now use our identity to pay, travel, cross borders, commute every day, have fun, open a bank account, seek medical care and use our connected devices – and this list will only continue to expand in the coming years. Given the vast range of environments and usages, securing our identity has become mission critical in the world we live in today. However, we recognize that even the strictest security measures are useless if they complicate usage. They must then be convenient and user-friendly – rooted in what is intrinsic to us, in who we are through biometrics. We also observed that our lifestyles demand a level of continuity never seen before. Indeed, we need our identity to travel with us seamlessly – whether in the physical or digital world or for government or commercial usages.

Only you can be you

Our promise is simple: with our technology and innovations in hand, *only you can be you*. In designing our market-leading solutions, we rely on the most physical, natural and authentic verification: the body's own biometric data. Your identity can be verified with a simple glance or the tap of a finger – which means that your identity cannot be stolen, imitated, jeopardized or corrupted. You are in direct control of your personal information. We have brought together complementary know-how and technologies that have never been combined before for both the physical and digital era: secured connectivity, secured payments and secured identity management. Not only does our technology help consumers and citizens alike travel with passports and pay with smartphones – it helps them identify themselves securely and effortlessly. And with every technological disruption, we adapt to meet the new and evolving security demands of today and tomorrow.

2 / Our strengths

2.1 > Leading trusted identities for an increasingly digital world



Well positioned in our markets

- #1** in police biometric systems
- Trusted by **1,800** financial institutions
- #1** in civil identity solutions
- Trusted by **500+** mobile operators
- #1** in biometric security systems for access and authentication
- Trusted by **leading** premium car makers
- #1** in US driver's license issuance

2.2 > Delivering future-proofed innovation

At IDEMIA innovation is « future-proofed », which means:

CUSTOMER-CENTRIC

We believe that innovation should support clients and partners to serenely apprehend the future.

MEANINGFUL

We aim at having a positive impact on peoples' everyday lives in a concrete, ethical and useful way.

SCALABLE

We address the needs of billions of people from providing a whole nation with identities to enabling its citizens to get in touch.

COLLABORATIVE

We believe that technology and skills are fed by external exchanges.

ALL ALONG THE VALUE CHAIN

We deliver vertical answers in the physical and digital worlds: from chip to Cloud.

2.3 > Serving clients in 180 countries

We transform society for a better tomorrow and we enable billions of people to...

Exist in the eye of society

We sit at the helm of Aadhaar, the largest and most ambitious identity program in the world.

Travel seamlessly

We streamline the passenger journey through airports with automated departure processes.

Live in a safer world

We support police forces with efficient tools to protect public places and solve cases faster.

Digitalize their critical activities

We allow people to open a bank account, sign up for a mobile data plan and access governmental services all from the comfort of their home.

Transact in a fast and secure way

We provide bank customers with hassle-free and highly secure payment means.

Connect securely

We secure connectivity for people and objects on cellular and low power networks.

3 / Réponses à la consultation ARCEP

3.1 > La 5G : une innovation de rupture qui continue d'évoluer vers la 6G

Question 1 à 3 :

Au-delà de l'amélioration de la vie privée apportée par la Release 15 et à laquelle IDEMIA répond avec son offre eXtra One dédiée, les évolutions qui nous semblent les plus pertinentes de la Release 16 sont Network slicing, le support des réseaux privés, Multiples Devices and Identités Multiples et Vehicule to everything in 5G network (V2x5G). Concernant la Release 17, il s'agit de l'amélioration sécuritaire de la procédure de resynchronisation lors de l'authentification, la Protection de l'identité et de la confidentialité lors du trafic offload 5G vers WLAN, Réseaux non-terrestres/ Satellites et les Terminaux 5G avec Capacité Réduite (RedCap)

Concernant la Release 18, les évolutions clés sont la Protection des identifiants transmis sur l'interface air, le Réseau IoT personnel, les Réseaux automatisés et la Connectivité pour Drones et Robots.

Concernant la 6G il sera clé pour la sécurité d'embarquer les algorithmes supportant la cryptographie Quantum/Post Quantum, d'intégrer de l'Artificial Intelligence et du Edge Computing / Cloud.

- Voici quelques autres évolutions potentielles:
- Vidéo et Biométrie analytics (ex. pour les services de mission critiques)
- Vidéo haute résolution 8K (ex. télémédecine, plateforme TV/streaming)
- Réalité augmentée (ex. éducation, industries)
- Intelligence artificielle & machine learning (ex. améliorer la détection des fraudes, se protéger des cyberattaques)
- UWB ou une technologie assimilée pour avoir une détection précise de la localisation. Un faisceau (spatialement réduit e.g. en 5.5GHz) pourrait être attribué à un élément communiquant

Ces services pourraient être rendus disponibles au plus près des usagers mobiles grâce à la 5G. La faible latence permettra de renforcer la réaction au plus vite de service de sécurité par exemple dans un cas d'usage de surveillance vidéo (dans le respect des règles GDPR)

3.2 > Les évolutions d'architecture des réseaux mobiles

Question 4 à 7 :

En tant que fournisseur d'un élément au plus près de l'utilisateur, nous étudions comment l'edge computing pourrait permettre de déporter les services de traitement de données dans la carte SIM.

La carte offre une solution standard fiable et sécurisé, mais caché dans l'équipement mobile. Les services à offrir seront donc directement lié à l'opérateur ou en lien fort avec lui. L'évolution eSIM pourrait permettre d'offrir des services à l'OEM, en particulier en termes de capacités cryptographiques et d'élément de confiance, sans dépendance vis à vis de l'opérateur

La cybersécurité reste un challenge primordial pour ces nouvelles architectures en manque de maturité. La surface d'attaque est plus large.

La sécurisation des échanges au niveau applicatif ou mieux au niveau transports est une nécessité dans un monde ouvert. L'utilisation des systèmes de sécurité existants, en particulier de la SIM comme 'root of trust' pour protéger l'identité et les données des utilisateurs est une nécessité.

La construction de réseaux "privés" (ou personnel) pourrait amener a une attribution locale de fréquences. Une non interoperabilité entre acteurs pourrait poser problèmes (e.g. pour le V2X un véhicule d'un autre pays qui n'arrive pas à se connecter aux réseaux nationaux/Européens)

3.3 > Les usages et les besoins en fonctionnalités attendus

Question 8 à 12 :

Parmi les usages que l'on peut attendre pour les nouveaux réseaux, on peut citer :

- Convergence virtuelle/Digitale (Métaverse, Communication multimodales)
- Industrie 5.0 (Digital twins, interactions humains / Robots)
- Sous Réseaux (réseaux In-Car, Réseaux In-Body) et réseaux de réseaux, réseaux hétérogènes
- Robotique
- "Localisation spatiale précise d'un acteur du reseau (e.g. UWB), pour par exemple l'indoor ou en cas de désastre de localisation (e.g. tremblement de terre personnes ensevelies)
- Communication maillé pour éviter les SPOF"

Les marchés industriels et le marché grand public seront les grands bénéficiaires car la 5G et les évolutions des standards permettront l'émergence de nouveaux services, améliorant la sécurité des réseaux, des objets et des personnes tout en étant interconnectés. Les scénarios d'utilisation des réseaux hétérogènes et de la robotique seront autant dans un scénario de mobilité que dans un environnement fixe.

Les réseaux seront autant des utilisateurs de nouvelles technologies (Intelligence Artificielle) que des facilitateurs pour d'autres technologies (la robotique).

L'intelligence Artificielle et en particulier l'intelligence distribuée seront clés pour couvrir l'ensemble des cas d'utilisations.

Des mécanismes d'authentification renforcées (Biométrie) et des mécanismes de confiance (Root of Trust) et de confiance distribuée (par exemple Blockchain) seront nécessaires pour couvrir la grande hétérogénéité des cas et des éléments du réseau.

Enfin le développement des technologies quantiques et conjointement de la cryptographie post-quantique sera nécessaire pour assurer la sécurité de l'ensemble du système.

3.4 > Innovation et développement économique

Question 13 à 15 :

Les nouveaux cas d'usage (Télémédecine, Téléservice, multiverse, communication critique) permettront une meilleure répartition du tissu industriel, mais aussi la digitalisation des PME. Cela permet à la plupart des PME de dépasser leur implantation locale pour accéder au marché mondial mais aussi d'accéder à une main d'œuvre beaucoup plus vaste.

Les fonctionnalités M2M/IoT peuvent permettre une meilleure utilisation des ressources dans un environnement citadin (-> Réverbères (voir panneaux publicitaires) qui s'allument que quand il y a quelqu'un dans la rue, -> Régulation des feux "automatique" en fonction du trafic véhicule (V2x))

La convergence monde réel/monde virtuel est aussi une opportunité pour la création de nouveaux marchés. La coupe du monde de Rugby et Les Jeux Olympiques de 2024 sont des exemples d'événements qui nécessiteront un déploiement exceptionnel de ressource.

Des exemples existent aux Etats-Unis de déploiements locaux et temporaire dans le cadre d'événements sportifs / culturels:

<https://www.t-mobile.com/news/network/t-mobile-5g-swings-into-yankee-stadium>

<https://www.pymnts.com/technology/2022/5g-powers-immersive-events-at-baseballs-all-star-week/>

On peut ajouter aussi la mise en place de réseaux spécifiques pour les unités de secours en cas de désastres (par exemple un tremblement de terre, inondations)

3.5 > Différentes réponses techniques possibles

Question 16 à 18 :

On peut s'attendre à la segmentation suivante:

- Les réseaux opérés pour les TPEs
- Les réseaux opérés et mixtes pour les PME
- Tous les types de réseaux pour les industriels et les grandes entreprises.
- Réseaux privés isolés peuvent apporter une sécurité supplémentaire dans les zones sensibles (e.g. Centrales nucléaires)
- Les Compétences, le coût et la maîtrise seront les critères de sélections du modèle pour les entreprises.

Le principal intérêt des réseaux hybrides est de permettre une gestion unifiée d'un réseau multi-bearer (Cellulaire + WIFI +...) sans avoir le coût du déploiement et de la maintenance d'un réseau. L'hybridation peut permettre une meilleure couverture dans les zones "blanches" (e.g. une partie du trafic d'un réseau privé alloué au public)

Les opérateurs (pour l'infrastructure) en partenariat avec des OEM (pour l'intégration et le déploiement, par exemple Ericsson, ATOS) éventuellement en complément avec des fournisseurs de services Cloud (AWS, Microsoft Azure)

3.6 > Évolution de l'écosystème pour répondre aux besoins des verticaux

Question 19 à 20 :

Oui, même si l'investissement initial (compétences/argent) limite l'accès aux nouveaux acteurs. A terme, le marché devrait faire baisser les prix de chaque parties, créer potentiellement de nouveaux marchés. En revanche, le marché va se complexifier, et les risques de défaillances d'un acteur seront plus élevés (mais moins impactant)

Les opérateurs télécoms restent les plus capables (en termes de compétences et de moyens). L'ouverture à d'autres personnes morales (entreprises, associations) est bénéfique, mais nécessitera un contrôle (sous la forme par exemple soit d'une certification, soit d'un déploiement par une entreprise certifiée)

3.7 > Couverture et qualité de service des réseaux ouvert au public

Question 21 à 23 :

Tous les services cités auquel il faut ajouter le jeu. Le streaming et le gaming, sont encore très imparfait en mobilité (TGV), dans des endroits difficiles d'accès (certaines gares de métros), et pour la combinaisons des deux (trajets RER/métros)

Le débit la congestion, et les interruptions de connexions sont les indicateurs clés de performance, dans un cadre individuel autant que professionnel. Dans l'ensemble la couverture reste stable, mais j'ai noté une dégradation en province cette année.

3.8 > Questions spécifiques à la couverture à l'intérieur des bâtiments

Question 24 à 28 :

La localisation spatiale (e.g. "indoor GPS") et/ou la détection de présence peuvent permettre une meilleure gestion. La problématique de la confidentialité pour les utilisateurs est néanmoins un point de vigilance.

Le WIFI reste la solution numéro 1 en intérieur, malgré différentes limitations (portées, traversées des murs, configuration). Un des principaux avantages du WIFI est le grand nombre d'équipements le supportant, nettement supérieur aux équipements supportant le réseau cellulaire. L'absence de provisionning rend l'intégration du WIFI beaucoup simple pour les fabricants. Néanmoins le WIFI n'est pas très approprié pour l'IoT (consommation/fiabilité), et sa robustesse (facilement brouillable/engorgé).

3.9 > Numérique soutenable

Question 29 à 31 :

Il est important que les dynamiques et méthodologies mises en œuvre par les différents acteurs et consortiums de l'industrie soient alignées afin de pouvoir s'assurer qu'elles sont cohérentes. Un exemple concret concerne les analyses de cycles de vie, qui doivent inclure une partie liée à l'impact environnemental lors de l'utilisation d'un produit. A date, il n'existe pas de méthodologie standardisée qui définit le volume d'échange de données entre l'utilisateur et le réseau .

Le numérique soutenable implique également une nécessité de transparence de résultats et une position claire de l'industrie contre l'éco blanchiment.

IDEMIA s'engage dans le plan IMPACT, à réduire l'empreinte carbone de ses activités de 25% à l'horizon 2025. L'ensemble des activités de la société sont concernées. La stratégie environnementale s'inscrit dans la méthodologie SBTi, notre société est par ailleurs accompagnée par des auditeurs externes. IDEMIA s'est également engagé à soutenir les opérateurs mobiles dans leur propre transition en leur proposant des cartes SIM écoresponsables qui les aident à réduire leur empreinte.

3.10 > Mutualisation

Question 32 à 33 :

La création de cellule, localisés, peut permettre à certains endroits de fournir une connectivité avec certaines spécificité (par exemple grande bande passante). Néanmoins, il est difficile pour l'opérateur de cette "cellule de connectivité" d'être responsable de l'activité des personnes avec qui celle-ci est mutualisée. Dans certains endroits, la mutualisation est intéressante. C'est principalement l'utilisation aujourd'hui des "hot spot wifi" (par exemple; Aéroport, gare etc..)

3.11 > Questions spécifiques par bande de fréquences

Question 34 à 38 :

N.A.

3.12 > Les fréquences harmonisées au niveau européen qui pourrait faire l'objet d'une attribution à court terme

Question 39 à 78:

N.A.

3.13 > Les fréquences identifiées à l'UIT en cours d'harmonisation européenne

Question 79 à 87:

N.A.

3.14 > Des bandes prospectives, en cours de discussion mondialement

Question 88 à 97:

N.A.

3.15 > Autres sujets éventuels

Question 98:

Il pourrait être intéressant de permettre des moyens pour détecter et circonvenir à la mauvaise utilisation de fréquences par un terminal. Par exemple un opérateur responsable d'un réseau privé devrait avoir des moyens "relativement simples" de détection (et localisation) d'un appareil "brouillant" la bonne communication dans son réseau.

IDEMIA RESTRICTED



www.idemia.com

