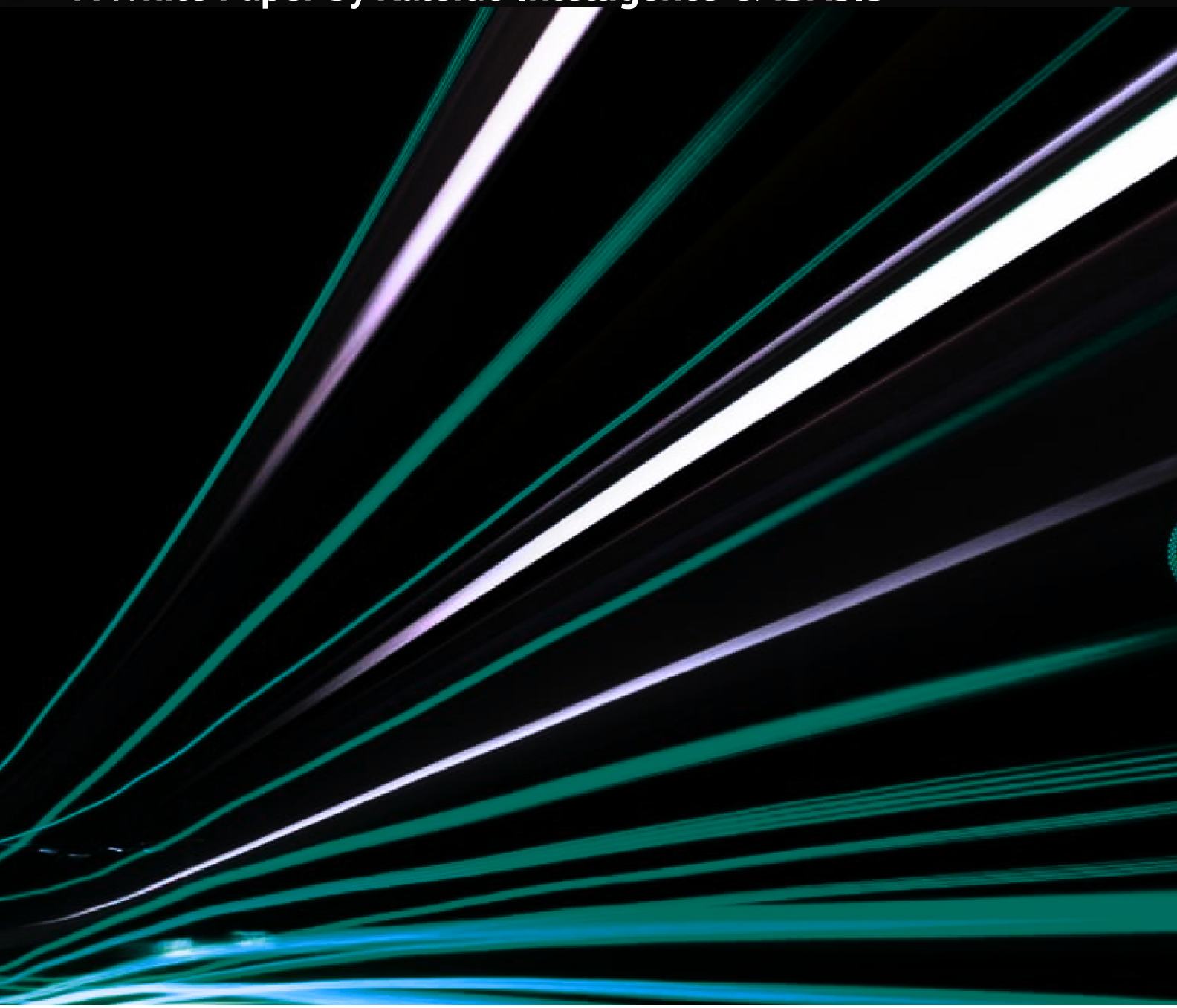
5G ROAMING: MNO REQUIREMENTS & OPPORTUNITIES

A White Paper by Kaleido Intelligence & iBASIS



iBASIS
POWERED BY TOFANE

Kaleido Intelligence

Executive Summary

The race towards 5G network deployment is setting the urgency for developing and implementing next generation roaming services to improve consumer satisfaction and enable new revenue models. This white paper highlights what changes 5G will bring for operators, which must be addressed if successful deployments, customer experience and profitability are to be achieved. Kaleido Intelligence surveyed senior decision-makers in roaming business units across 60+ leading MNOs around the world to learn from their current and future roaming plans as well as commercial and technical requirements for implementing 5G roaming from an IPX, security, clearing and signalling perspective.

KEY SURVEY FINDINGS

Security and high availability are top priorities for 5G roaming. New services, such as network slicing are less important at the moment, likely due to uncertainty surrounding the business model and deployment methods.

41% of respondents from surveyed operators noted that ensuring adequate security levels will be very important while rolling out 5G roaming. SEPP (Security Edge Protection Proxy) and SCP (Service Communication Proxy) implementation were found to the most important security implementation and priority execution requirements.

Local Breakout is currently viewed as important (61%) vs critical (17%), indicating it is a medium-long term priority for operators.

Despite operator hesitance towards LBO (Local Breakout), 61% of respondents believed that LBO will become important in 5G roaming, especially for use cases such as V2X (Vehicle-to-Everything) communications, 4K/8K video services and other low latency applications and services.

Managing increased capacity voted as the most important 5G roaming requirement from IPX providers.

The average consumer data usage by active 5G roamers will be much greater than 4G and 3G roaming. IPX vendors must be capable of managing any capacity requirements. According to the survey, this was found to be the most important factor that operators will take into consideration while deploying 5G roaming, with 44% of surveyed operators considering this as 'very important'.

Signalling interworking is a very important roaming requirement for mobile operators.

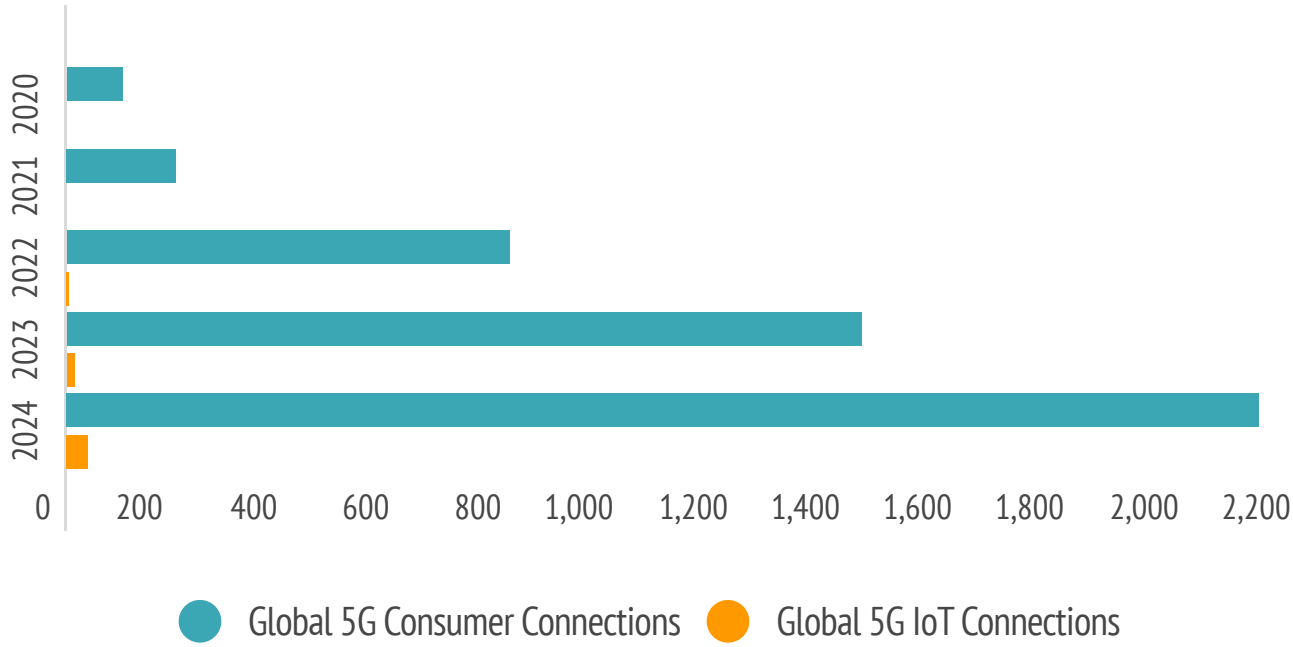
60% of survey respondents confirmed signalling interworking as the most important 5G roaming technological innovation, alongside enabling secure interconnect between 5G networks by introducing SEPP functionality and ensuring end-to-end authenticity and integrity.

The Dawn of the 5G Era

In 2019, several markets switched on 5G networks, with vendors offering new 5G mobile devices, resulting in a strong momentum in 2020. As more countries roll out 5G networks and more devices become available, the number of 5G connections worldwide will exceed 1 billion in 2023. This growth is significantly faster than 4G and 3G adoption witnessed in the past. Along with the growth in 5G connections, 5G roaming agreements are also on the rise: for example, SK Telecom and KT both reported over 1 million 5G connections in late 2019 and announced roaming agreements with multiple Asia-Pacific and European operators. SK Telekom announced further plans to expand 5G roaming to 20 countries in 2020, including the US and Japan; although support remains limited, which is hardly unexpected at this stage.

1 Billion+ 5G Consumer & IoT Connections in 2023

Global 5G Connections in Millions, 2019-2024



Source: Kaleido Intelligence

Deployments so far have been on non-standalone network modes, with standalone networks expected to launch in 2020. In addition, further investment and collaboration between global operators will be required to drive 5G roaming adoption and growth. Standardisation for 5G roaming will play a big role. Besides, roaming strategies will also depend on future IoT strategies from MNOs.

Another challenge is concerning the manner by which traffic can be differentiated to apply appropriate billing to the customer, as well as securing a return on operators' investment. While 5G roaming across consumer and IoT services is an inevitability, there is indeed a lot to be discussed and standardised both at the wholesale and retail level. This white paper discusses the 5G roaming opportunity, operator requirements and readiness from a technical and commercial perspective, as well as the roadmap for 5G roaming deployment strategies.

Unlocking the 5G Roaming Opportunity

What will 5G Roaming Look Like?

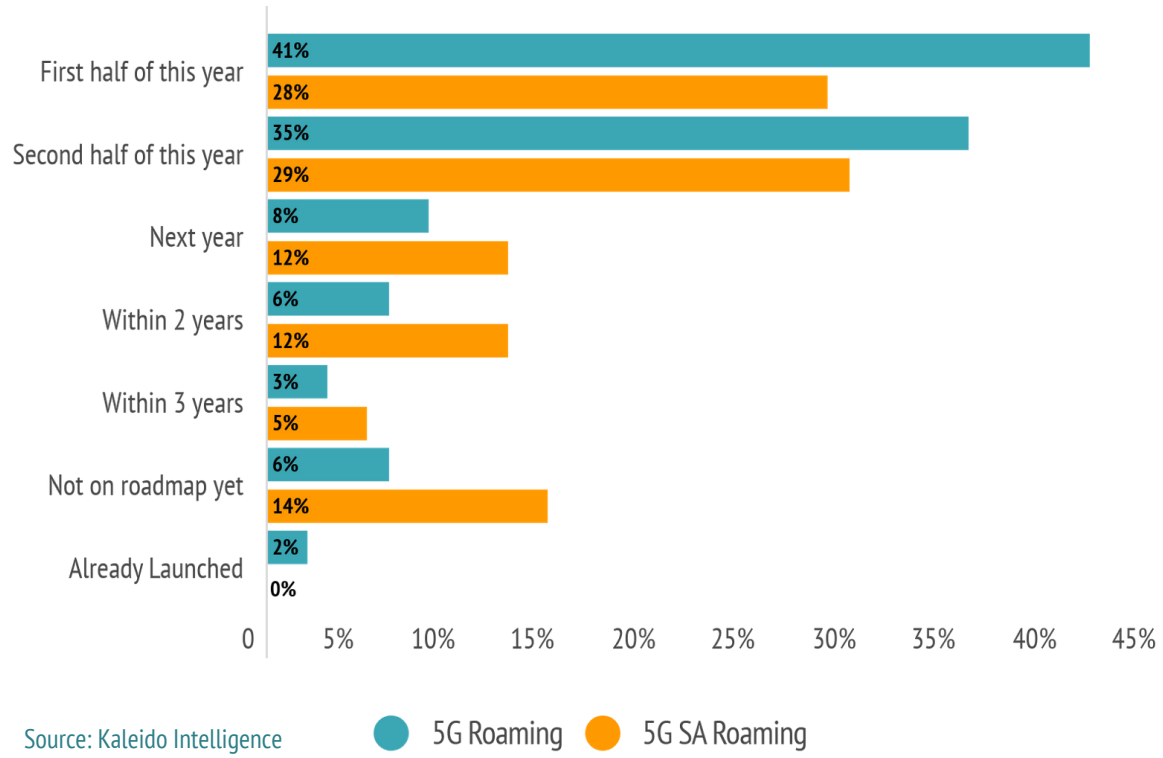
5G network deployment has so far remained a domestic concern for mobile operators. While commercial 5G services are now available around the world, these have been predominantly on a NSA (Non-Standalone) architecture. The NSA deployment models utilise existing 4G infrastructure, i.e. using EPC (Evolved Packet Core) and LTE eNB (Evolved Node B) access. According to the 3GPP, there are 5 possible configurations or options for connecting to an EPC or new 5G core network. The NSA 5G rollout (primarily Option 3 deployment model, where both LTE and 5G NR (New Radio) access are present and controlled by the EPC core) will depend on the use cases that 5G will aim to address initially; for example, eMBB (Enhanced Mobile Broadband) related to 4K-8K videos, AR/VR applications as well as HD communications.

In summary, 5G networks differentiates itself from 4G by enabling the following improvements:

- 100x increase in data rates and traffic capacity
- 100x increase in network efficiency
- 10x decrease in latency
- 10x increase in throughput
- 10x increase in connection density

However, as is evident from current deployments, 5G rollouts will continue to be based on the NSA architecture, in the short- to medium-term. SK Telecom is launching commercial 5G services on 5G SA architecture in H1 2020. The operator added 5G base stations to its 5GC (5G Core) Network to enable the SA (Standalone) architecture with network slicing and mobile edge computing capabilities. Kaleido expects further rollouts to occur in H2 2020 and H1 2021 around the world. Kaleido surveyed 60+ respondents across tier-1 operators around the world on their 5G roaming plans in Q1 2020[1]. Please note that the below timescales for 5G roaming deployments are subject to possible change, following the global impact of COVID-19 on enterprise and operator budgets and operations.

5G Roaming Deployment Plans: When will you launch 5G and 5G SA roaming? n=66



Source: Kaleido Intelligence

Nearly 76% of the operators surveyed announced that they will launch 5G roaming in 2020, with 8% planning to launch next year. In comparison, only 57% expected to launch 5G SA roaming services in 2020. However, a small proportion of operators do not have any specific plans to roll out 5G roaming in their roadmap. In addition, nearly 68% of the operators surveyed stated that they were considering introducing 5G roaming even without having launched 5G network in their domestic market. The rollout of 5G networks around the world, alongside an increasing number of 5G roaming agreement announcements by operators, means that mobile roaming is set to be transformed.

While much of the focus has been around enabling faster mobile broadband for roaming consumers, 5G roaming will also enable new data services for IoT applications, including energy and water meters, alarms, scenarios such as connected cars, robotics, remote patient monitoring and others that can be categorised as mMTC (massive machine type communication) and uRLLC (ultra-reliable low-latency communication) services.

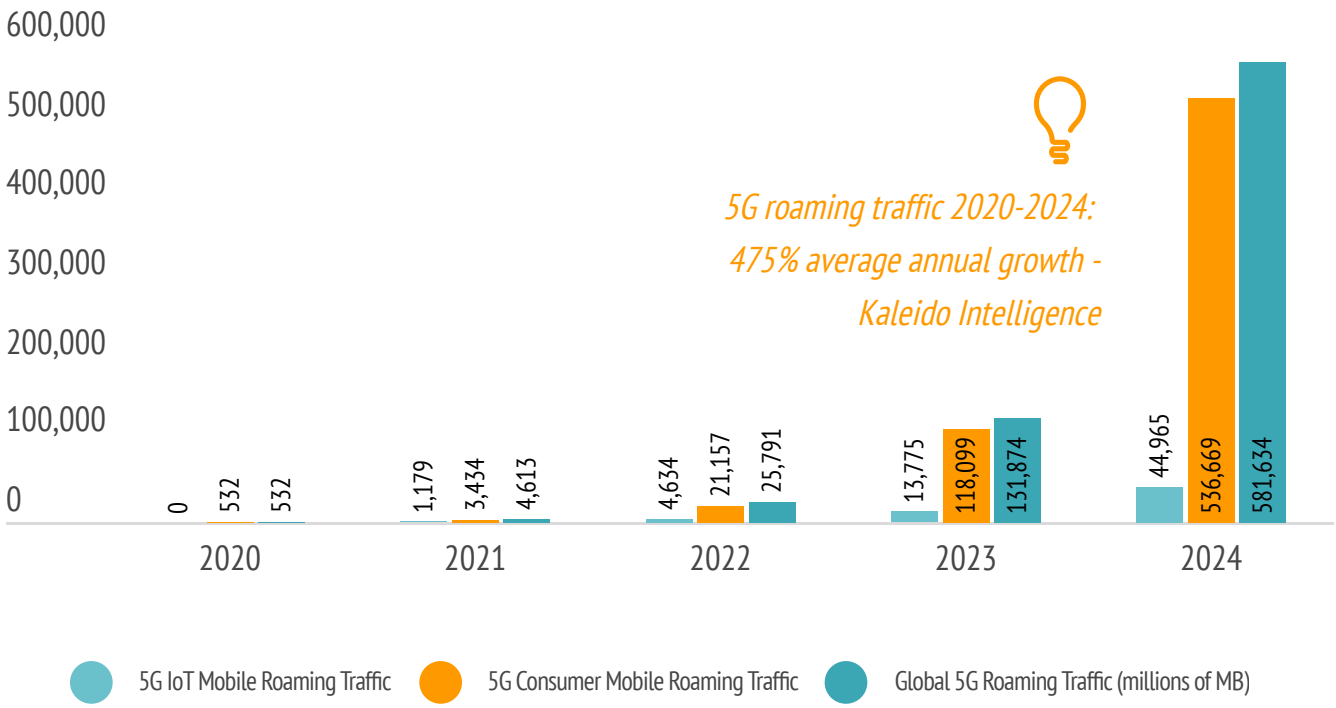
Undeniably, 5G roaming via consumer mobile devices and IoT will generate a substantial surge in data roaming traffic, enabling new value-added opportunities and services for mobile operators. This means that operators will need a reliable, robust and comprehensive IPX solution to support this continued growth in data traffic.

5G Roaming Traffic: Regional & Global Outlook

According to Kaleido Intelligence, 5G data roaming traffic generated by consumer mobile devices and IoT applications will exceed 500 Petabytes in 2024, an average annual growth of 475%.

500PB of 5G Data Roaming Traffic in 2024

Global 5G Roaming Traffic in Millions of MB Per Annum, 2020-2024



Source: Kaleido Intelligence

Understandably, initial growth in mobile roaming traffic will be driven by consumer mobile broadband usage, accounting for 350 Petabytes in 2024 and an average annual growth rate of 444%. In comparison, IoT roaming high volume traffic will be driven by verticals such as security, vehicle applications and to an extent connected healthcare services.

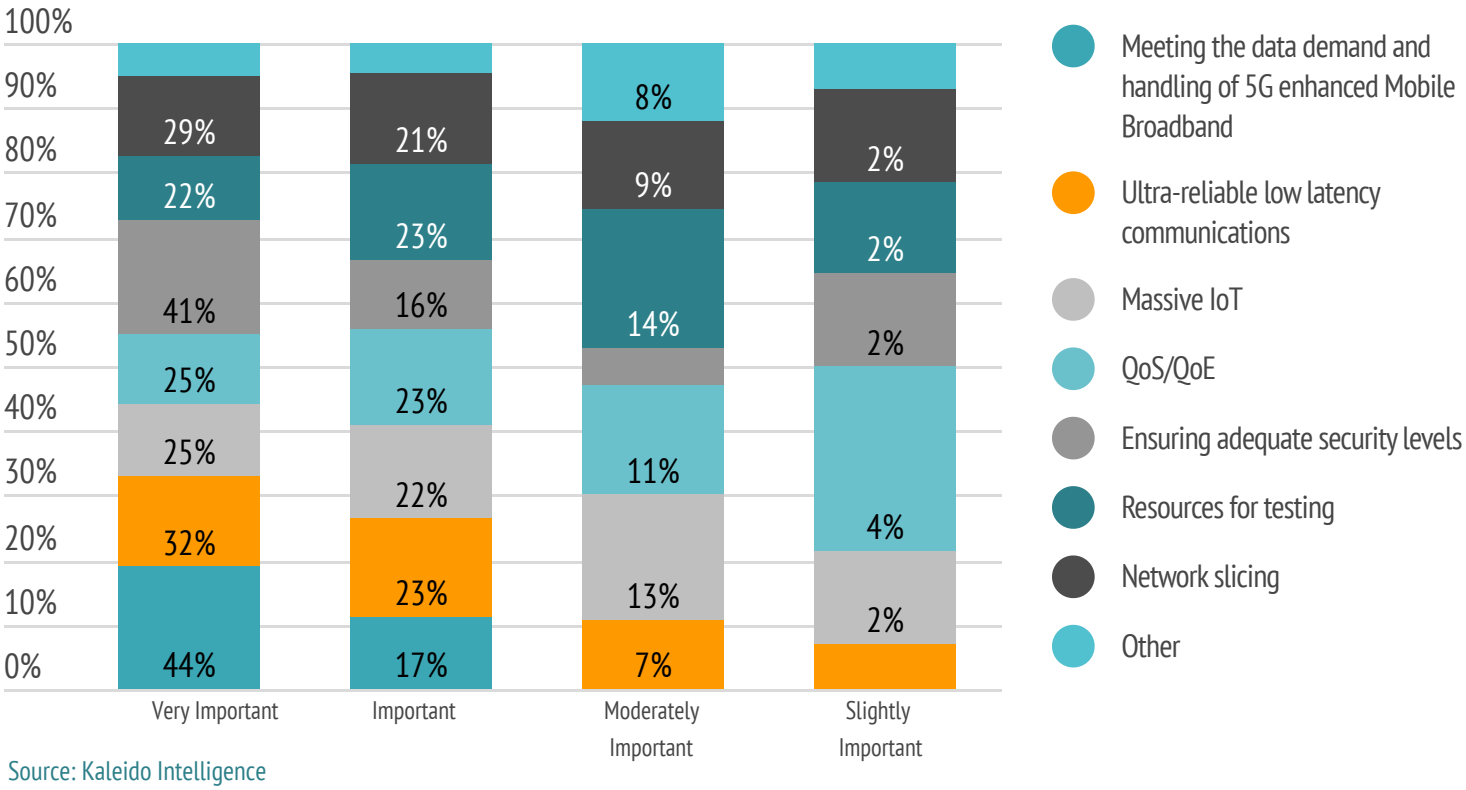
The average consumer data usage by active 5G roamers will be much greater than 4G and 3G roaming, with 5G roaming traffic representing nearly 25% of global data roaming traffic in 2024. In comparison, this was less than 1% in 2020.

Maximising the 5G Roaming Potential

5G roaming presents operators around the world with an opportunity to innovate and deliver new smarter and consumer-focused data services. However, this means that operators will need to focus on a few key areas:

- **5G spectrum and device challenges.** Operators will need to address 5G roaming on different spectrum bands. This is also a handset vendor issue.
- **Enterprise and consumer roaming usage.** Understand the most important use cases that will drive 5G roaming services and plan network resources accordingly to target commercially viable use cases across both consumer and enterprise sectors.
- **5G signalling and interworking.** Support for the new 5G networking protocol based on HTTP/2 alongside 4G and 3G signalling protocols is required. In addition, a converged interworking solution (2G/3G/4G and 5G) will be required from the IPX partner.
- **IPX capacity enhancement.** With the increase in data traffic, the operator's IPX vendor must be capable of managing any capacity requirements. Indeed, faster speeds has always given rise to increased data consumption demands. According to the survey conducted by Kaleido, this was also found to be the most important factor that operators will take into consideration while deploying 5G roaming, with 44% of surveyed operators considering this as very important.
- **Network slicing, where a portion of the available network is sold and run as a separate entity from the rest of the network.** From an IoT perspective, operators will need their IPX vendor to address different 5G slices and standardised business models.
- **Technical requirements.** 5G SA means heavy upgrades to the network side as well as technical expertise. This means prioritising the operator's 5G roaming roadmap. New services mean the need for upgrading existing roaming services including steering, analytics and settlement. Real-time financial clearing (22%) alongside support for IoT/M2M business models (21%) alongside advanced fraud prevention services (20%) were found to be the top 3 operator requirements from a 5G data and financial clearing perspective, according to the survey.
- **Deploying SEPP for the control plane.** Sourcing this is an important and mandatory requirement for 5G networks interconnect for roaming in a SA architecture. Nearly 41% of surveyed operators noted that ensuring adequate security levels will be very important while rolling out 5G roaming.

Drivers for 5G IPX Deployment: What are the most important factors you consider to be needed for 5G IPX deployment? n=66



Source: Kaleido Intelligence

44%

Meeting the 5G data demand and capacity requirement is critical.

29%

Only 29% of respondents considered network slicing to be very important.

With data traffic volumes expected to surge, operators will need to partner with the right IPX vendor capable of delivering a robust and dedicated interconnect network to accommodate data demand across a range of new consumer mobile and IoT roaming applications.

Security Risks & Mitigations Enabled by 5G

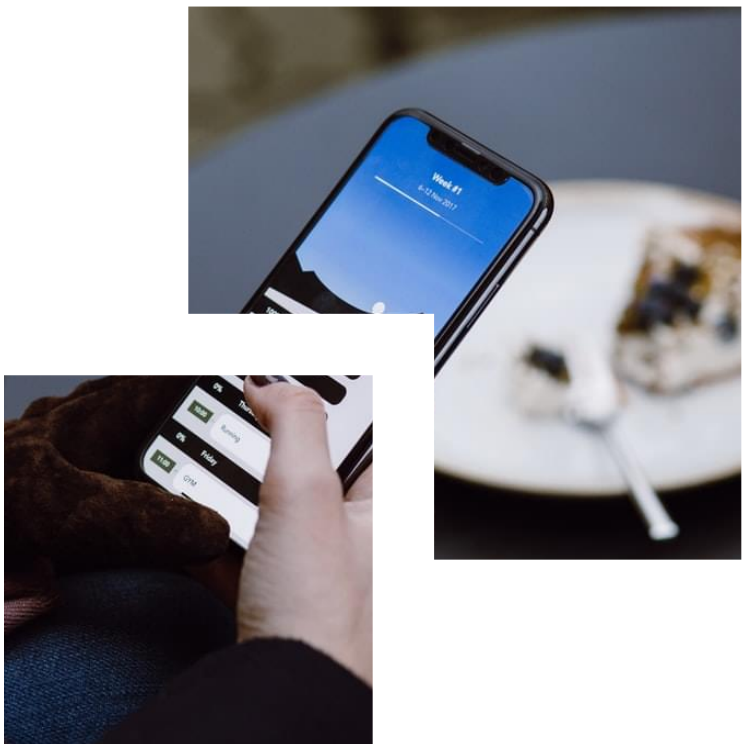
Migration to 5G entails new risks and attack vectors that are realised in line with the phased transition from 5G NSA to SA core architecture, with 5G NSA risks presenting a considerable challenge. As operators move to 5G NSA solutions, GTP (GPRS Tunneling Protocol) signalling via the S8 interface will remain as a legacy protocol from GPRS networks. Mitigation solutions, such as GTP firewalls have long been in existence but have seen comparatively little uptake among operators during the 4G era owing to relatively low levels of roaming, as well as a view that the implemented trust model of authentication methods and roaming agreements were 'good enough'.

Given the likelihood that 5G NSA will be in use for some years to come, GTP threats will continue to exist at least until migration to 5G SA and HTTP/2 is complete. In reality, GTP is but a single (yet major) concern posed by the network transition to 5G.

The fact is that devices utilising up to 4 generations of 3GPP standards will co-exist on the same networks and require support for some years to come: indeed, currently the only standard in obsolescence is 1G! As such, players must take steps to become aware of the type of devices roaming on their networks and establish appropriate risk profiles and counter-measures.

Additionally, the relatively long migration to 5G SA will mean that access to the IPX signalling network will continue over SS7 (for 2G/3G) and Diameter (4G) protocols, both of which have several known security flaws. While this is not a problem in itself, with security best practices having been established, problems may arise when operators begin treating this traffic with the same level of confidence as 5G SA traffic, which will utilise the more secure SEPP protocol over the N32 interface (with the latter ensuring that traffic is encrypted).

Meanwhile, for those with 2G/3G/4G networks, some form of protocol interworking must be established for devices to communicate with 5G cores. For IoT devices, this is a critical factor to bear in mind for roaming service providers, particularly as a substantial portion of cellular IoT devices are not produced within the country of operation and are thus roaming once deployed. Indeed, many IoT devices continue to use SS7 as a means of opening a data channel to the network, which, given the lack of encryption over the SS7 protocol, shows obvious flaws.



Given expected connected device volumes, virtualised architecture and exposure to multiple signalling protocols across the network, the baseline risk for 5G migration is higher than was present in legacy networks. This means that operators and CSPs along the value chain must adopt new approaches to mitigate threats as appropriate to the level of risk that their networks are exposed to.

As ever, there is no one-fits-all situation, as traffic and device type and volume will vary significantly from place to place. What is certain however, is that roaming traffic will increase on a global level, which means that players along the value chain must prepare for a situation where the potential attack surface has been greatly increased.

Work has been underway to mitigate possible security concerns across 5G NSA and 5G SA architectures:

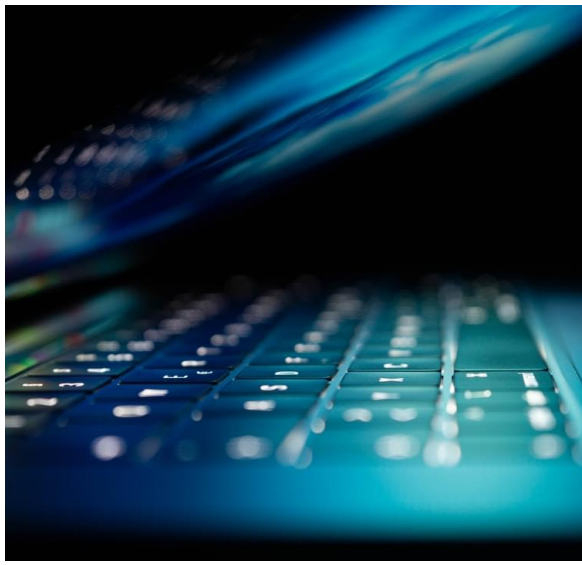
5G NSA

- Employment of GTP application layer firewall serves to mitigate the issues described earlier in this document until 5G SA is fully established between operators.
- The 3GPP Release 15 specification allows for small data packets/messages to be transmitted over the Diameter protocol. Given the latter's support for TLS encryption, this will aid in migrating unsecured legacy SS7 IoT traffic to a more secure protocol.
- For 4G/5G roaming devices, this capability is extended via the SCEF (Service Capability Exposure Function) gateway, which allows for low-power, non-IP traffic to be transmitted securely.
- Migration away from standalone protocol appliances (which are often constrained in their capability to be updated to address security best practices) to converged solutions capable of managing interworking and security across a single interface.

5G SA

- SEPP is a mandatory element of 5G SA core interconnect. The SEPP offers end-to-end security for roaming interconnect messages, offering substantial security enhancements over the simple transport encryption offered by Diameter, and no encryption offered by SS7.
- Authentication between operator SEPPs is required in order to prevent unauthorised communication between networks.
- The N32 interface is introduced to function alongside the SEPP to ensure that sensitive data between SEPPs is protected.
- The SCP offers networks support in case of any malicious traffic traversing over the network. It increases the resilience of the network by mitigating network overload instances (such as through signalling storms) and prioritising message handling in cases where the network is overloaded.

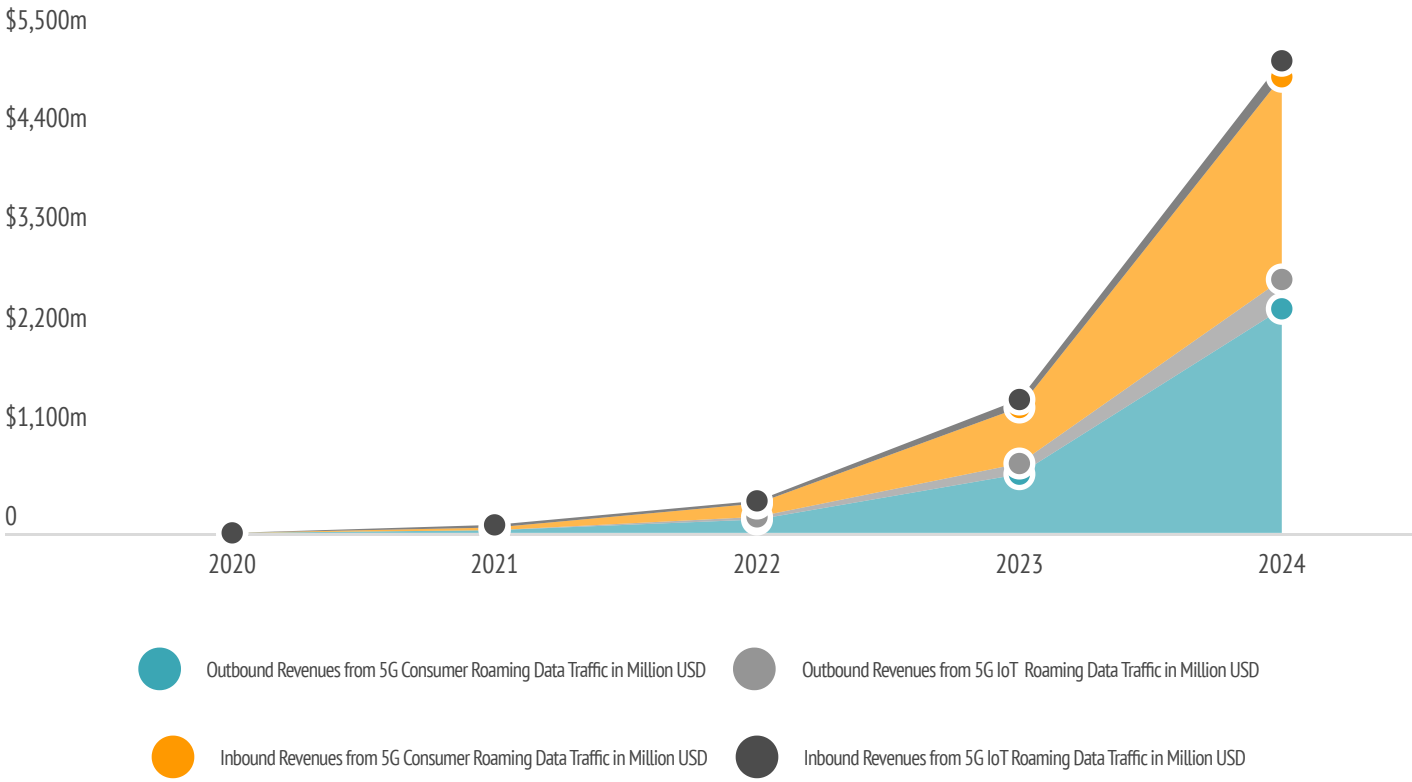
5G will vastly increase the attack surface of mobile networks, with challenges particularly apparent across the control plane. It will be important to have a flexible, robust approach during the transition from 5G NSA to 5G SA.



5G Roaming - The $7 Billion Opportunity

Kaleido predicts that revenues from outbound and inbound roaming traffic generated by consumer mobile and IoT devices will exceed a combined total of $5 billion in 2024 and a cumulative revenue of $7 billion+ over the next 4 years.

Global 5G Roaming Inbound &Outbound Revenues in USD Million Per Annum, 2020-2024



Source: Kaleido Intelligence

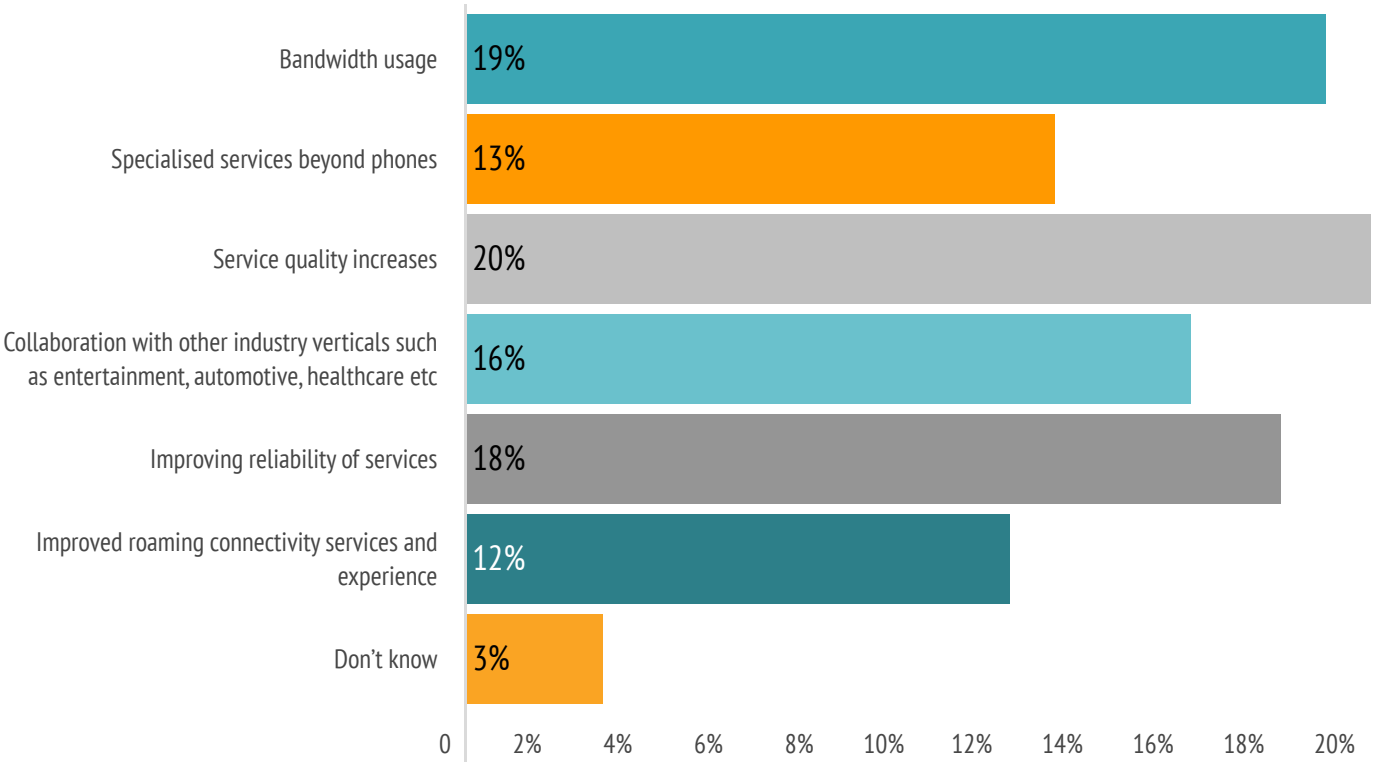
As the race to 5G rollout continues, outbound roaming revenues generated by consumer mobile roamers will drive 5G over the next 5 years. Consumer roamers will drive this uptick in revenue and traffic only if operators are able to charge prices that will resonate with the consumer similar to current pricing levels.

Even though 5G data traffic cost per MB will be lower, outbound bundles will be priced at a premium or offered as a superior bundle to the highest tier of user during the early years of launch. According to the survey conducted by Kaleido, operators noted that the increase in service quality and bandwidth afforded by 5G, followed by specialised services beyond consumer use cases within key IoT verticals, will be the primary revenue drivers for 5G roaming.

Within enterprise and IoT roaming, it is expected that new applications and use cases in the mMTC and uRLLC will drive roaming revenues for the operators. It is Kaleido's view that while new and disruptive use cases in mMTC and uRLLC have still not been established, IoT will indeed become the dominant traffic generator for 5G roaming in the future, however, this is at least another 7-8 years away.

According to the survey conducted by Kaleido, operators noted that the increase in service quality and bandwidth afforded by 5G, followed by specialised services beyond consumer use cases within key IoT verticals, will be the primary revenue drivers for 5G roaming.

5G Roaming Revenue Drivers: What will be main drivers for 5G revenue increase? n=66



Source: Kaleido Intelligence

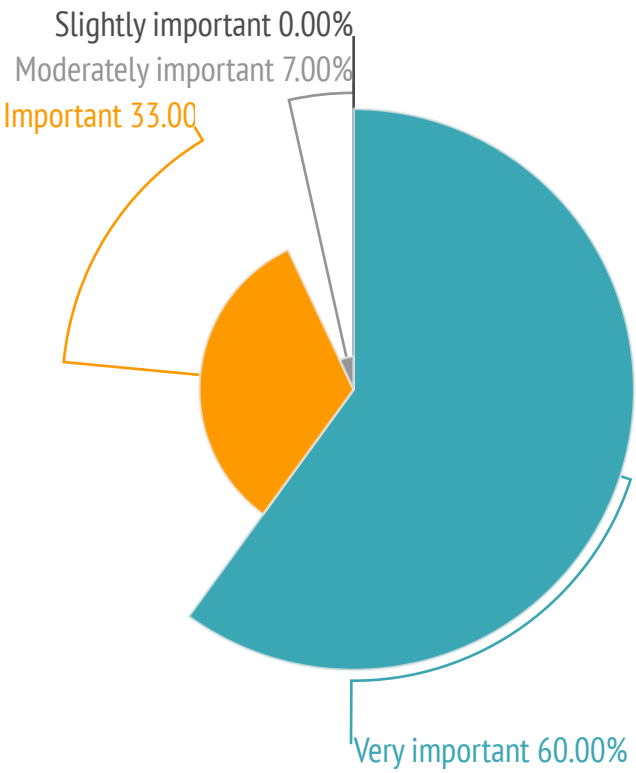
Ensuring a 5G Success. The Essential Ingredients

Signalling Evolution

In terms of 5G signalling requirements, operators require a more robust and comprehensive solution from the IPX vendor.

Signalling in 5G will be based on SCP, BSF (Binding Support Function) and SEPP functions. 5G will also require a new core network signalling protocol: HTTP/2. Operators will need to introduce this to 5G SA network architecture during the early stages of upgrade. IPX vendors must be prepared to offer this as a single and unified solution as operators migrate domestic and roaming networks to 5G SA architecture.

5G Roaming Services & Innovation Requirements: What kind of services or innovation you expect from your IPX provider? (Respondents answering with Signalling Interworking) n=66



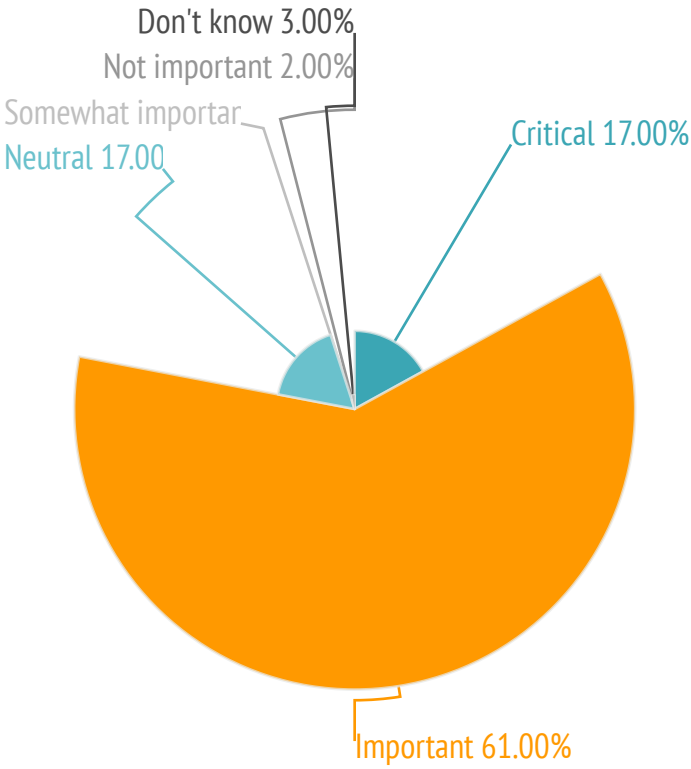
Source: Kaleido Intelligence

In addition, signalling interworking is a very important requirement for the mobile operators, with 60% of survey respondents confirming this innovation as very important, alongside enabling secure interconnect between 5G networks by introducing SEPP functionality and ensuring end-to-end authenticity and integrity.

These new protocols will enhance the protection against any new or known inter-exchange/roaming vulnerabilities.

The Need for Local Breakout

Importance of LBO in 5G Roaming: What role do you see for local breakout versus home routing? n=66



Source: Kaleido Intelligence

With home routing, data traffic is tunnelled back to the home network and then to the internet. In comparison, LBO enables roamers to receive data services directly from the visited network instead of tunnelling back to the home network. Indeed, all architectures have their respective advantages and disadvantages, depending on the complexity and diversity of the application and retail roaming commercial requirements.

However, with 5G supporting various enterprise and consumer use cases, there is a need to support both LBO and home routed architectures. It is evident that LBO will be required for use cases such as V2X (Vehicle-to-Everything) communications, 4K/8K video services and

other low latency applications and services where offloading data to the local network is recommended.

Indeed, for mission-critical uRLLC applications, local processing via edge computing nodes will be required. However, this will mostly be driven by private network deployments.

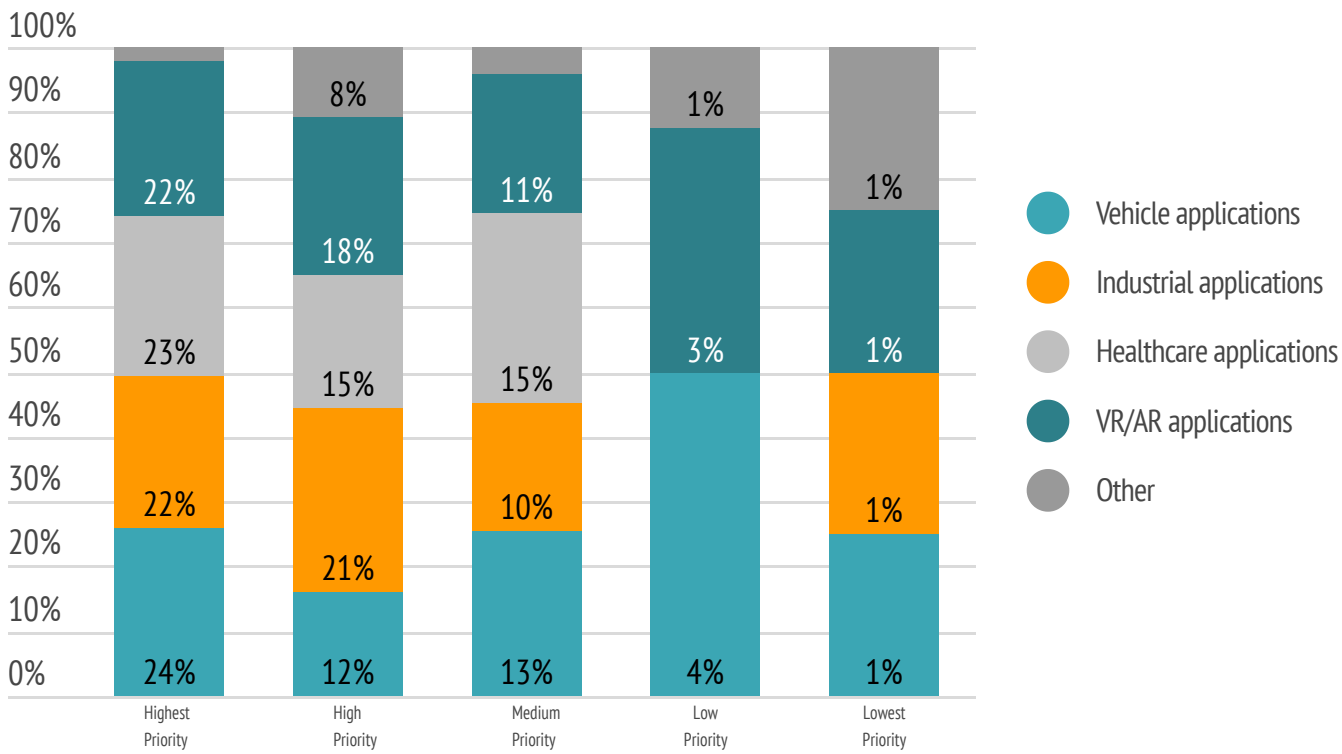
It is imperative that operators start preparing for the full transition towards 5G roaming. Consequently, operators will expect IPX providers to offer both regional and local breakout to support their 5G roaming needs. This will enable specific traffic profiles to be differentiated and optimise 5G roaming.

Edge Computing in 5G: Operator Role & Opportunities

Tying in with LBO relatively closely, the potential for edge computing services in 5G is relatively clear: localised computing assets can be used to deliver uRLLC services, offload computing power from end user devices as well as support network slicing. It is certainly the case that several key verticals could benefit from edge computing support:

- Industrial applications, by virtue of uRLLC services that cannot be offered by traditional, centralised mobile networks;
- Automotive use cases, where V2X and autonomous vehicle technologies will rely on reliability and low latency;
- AR/VR applications, where current mobile solutions are not fit-for-purpose for a mass audience. Computing power can be offloaded to the edge, reducing device power consumption, improving performance and offering the potential for form-factor design advances.
- Healthcare telemedicine applications which benefit from connection reliability, low latency and improved data security.

uRLLC Roaming Services Rollout: What are your plans for uRLLC services? Specifically, which international ones? n=66



Source: Kaleido Intelligence

These verticals were reflected in Kaleido's 5G roaming survey to operators, who indicated a relatively mixed bag when asked to rank how they saw demand for uRLLC services. Analysing the data and ranking responses into order of priority reveals this result:

1. Vehicle applications
2. Healthcare applications
3. Industrial applications
4. VR/AR applications

12% of our survey respondents have not yet considered how, or when to deploy uRLLC services.

2021	Industrial, & smart city applications: to support private network deployments via local core functionality, fog computing and micro/macro network handover
2023	Network slicing: driven by consensus around business models and increased network architecture automation
2024	Mobile AR/VR: growth constrained by edge node availability, power & handover complexity
2026	Vehicle applications: Driven by uptick in V2I/V infrastructure build-out

While edge computing will almost certainly play a key role in 5G, the delivery of edge computing services, particularly in cases where SIMs are roaming, will be rolled out to address specific use cases that will take time to gather market traction:

- Mobile consumer low latency services, such as gaming and VR/AR applications are presently at a very early phase of adoption. Edge computing will be deployed to handle much of the computing power required: however, supporting a substantial number of users per node will require considerable challenges in terms of planning and power supply: this will inevitably take time, while there is a risk of potential low demand from users themselves.
- Current precursor technologies that will eventually support autonomous vehicles, such as V2I and V2V (Vehicle-to-Infrastructure and Vehicle-to-Vehicle) will not emerge as mainstream vehicle technologies until the middle of the decade.
- Network slicing, a much-touted feature of 5G revenue opportunity, will require advanced automation capabilities within networks.

There is no formal standard for network slicing, with trials still underway. 38% of survey respondents in Kaleido's 5G roaming survey believe that network slicing will be deployed via common standardised slices between roaming partners; 27% believe that self-service models should be implemented while 25% believe in a federated slicing model.

Kaleido believes that the earliest opportunities for edge computing in a 5G roaming context will be seen in the industrial and manufacturing sector, smart cities and public spaces sectors where there is already appetite for private network deployment using 4G connectivity. MEC (Multi-Access Edge Computing) will be required to handle the localised core functions, as well as any handover between the micro and the macro network. This trend will undoubtedly continue as 5G progresses, although the route to private network deployment will vary:

- Some countries, such as Germany, are issuing spectrum licences to players. This reduces the potential role that operators can play.
- Other countries will rely operators to deploy and manage their private networks.
- 5G NR-U (Unlicenced) has been formally standardised, which will be of particular interest to players looking to deploy in public spaces and, to a lesser extent, industrial applications.
- Private networks can be deployed in several fashions:
- Local radio hardware connecting to the macro network, with the private network allocated logically via network slicing. The operator is a key service provider, with MEC providing some of the computing power to handle operations and data processing.
- A similar architecture to the above, albeit with a local core deployed close to the private network. MEC will likely power the core as well as provide fog computing power.
- As standalone networks with dedicated spectrum. MEC nodes will likely be controlled and operated by enterprises deploying this type of network.

According to Kaleido's research, the industry consensus was that almost all private networks will benefit from some kind of connection with the macro network. This means that roaming connections will, in many instances, require access across private and public network instances. It is here that additional opportunities will be afforded, as customers will likely desire specific service levels, both at the local and international interconnect: certainly, affording a high level of security will be in demand, while other customers will look to achieve lower latencies where possible. Sensitive data carried inside a private network becomes vulnerable once that network is connected to a wider public access network. Kaleido's 5G roaming survey revealed that security best practices, innovation and implementation consistently ranked as highest or second highest in priority across operators' implementation plans as well as in the context of IPX service provision.

In the medium-term, broader edge computing use cases will begin to emerge, as sufficient infrastructure is rolled out. Planning ahead, focus must centre on the needs of application developers. High-demand applications such as AR/VR will certainly require the ability to hand off computing power to a number of MEC nodes, meaning that high availability will be needed. If it is not possible for operators to address this directly (most will not be able to), discussions on how to develop business models surrounding edge aggregation and how APIs can expose multi-edge workloads must be initiated in the near-term to plan ahead and maximise the opportunity.

Ensuring Robust Security Across the Network

Once again, it is important to emphasise that the need for interconnect in roaming environments, as well as the flat architectural nature of IP-based mobile networks means that the compromise of a single network entity potentially puts the rest of the network and any interconnected networks at risk.

Common Security Practices Must Still be Observed

- Logical separation of the network to mitigate the impact of any breach. In some cases where data is very sensitive, it may be prudent to separate parts of the network using physical appliances, rather than using virtualised instances .
- Perimeter security remains as important as ever. As such, firewalls to examine signalling and user plane traffic are critical, while additional measures to mitigate DoS attacks are also critical.

Ensure Legacy Threats are Not Ignored...

- 5G NSA roaming exposes networks to SS7 as well as Diameter signalling traffic: the most effective way of managing this is to deploy software-based solutions capable of extending firewall capability across the range of signalling protocols that emerge on the path to 5G SA.
- GTP traffic vulnerabilities must be addressed by a GTP application layer firewall.

...and Adapt to Address New 5G Business Model Opportunities

- Network slicing requires access to sensitive data inside partners' NRF (Network Repository Function, which may raise security concerns given the potential diversity of network slice users, which could be both MNO to MNO as well as MNO to a third party. One possible route towards mitigation of this concern is for an IPX provider to act as a trusted intermediary between the network slice provider and customer.

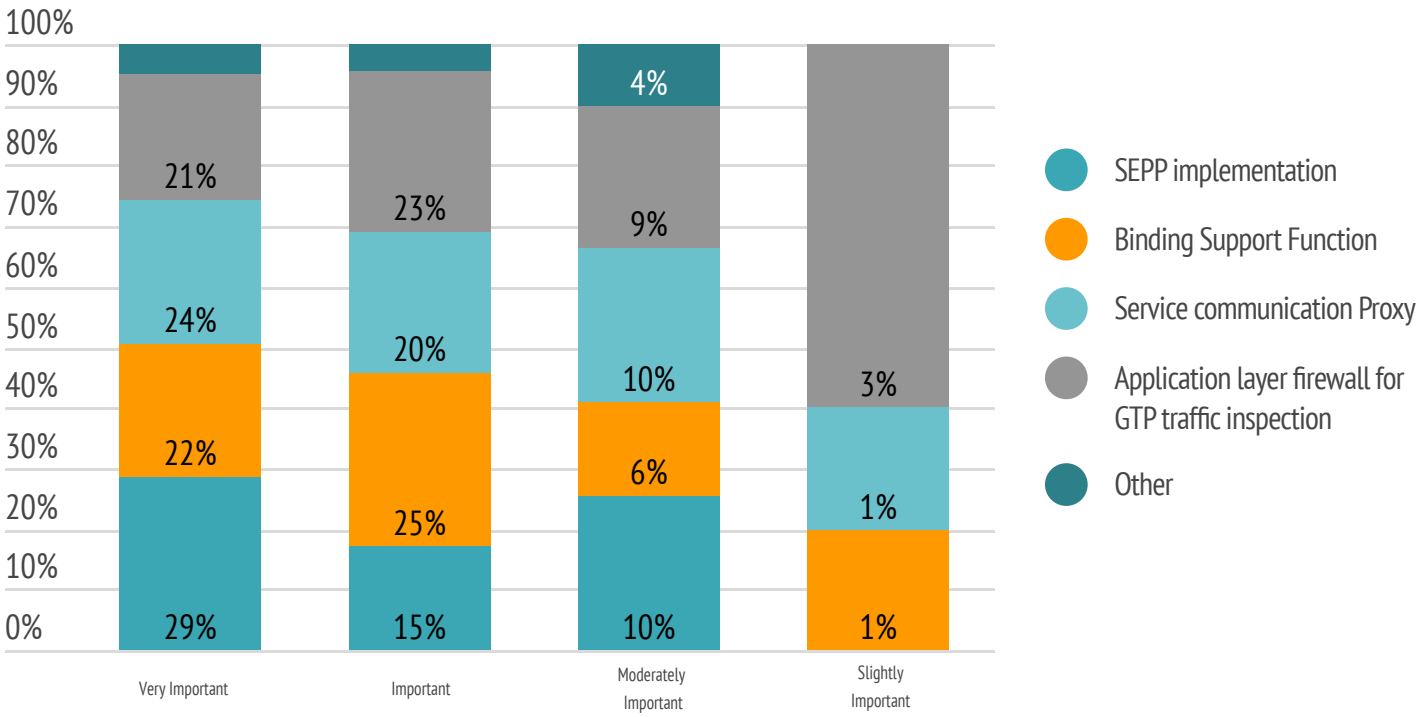
Consider VAS Implications when Deploying the SEPP Firewall

- For 5G SA roaming the deployment of a SEPP firewall is required. In a straightforward deployment end-to-end encryption means that VAS provision at the interconnect level becomes challenging in terms of policy control, RLAH, Welcome SMS, CAMEL and so on.
- This is concerning not only for IPX providers, but also for operators themselves wishing to optimise the consumer roaming experience by lowering the potential for monetisation. How this will be handled while retaining a high level of security remains under discussion, although one possible route is for the IPX provider to host the SEPP; it may also lead to an increase in the number of direct interconnects between operators.

Perhaps one of the most important steps for players to take in the context of 5G security is to ensure that the skillset within players' organisations is fit for purpose. Migration to 5G SA entails not only a new signalling protocol; HTTP/2; but also, several other features:

- Web-based APIs, where exploitation of API logic is a strong possibility, requiring detailed understanding of API design principles;
- JSON message data format, protected by JWE (Java Web encryption) and JWS (Java Web Security) functions;
- Tremendous increase in virtualisation and software-abstracted network functions.

Security Requirements for 5G Roaming: What are your security requirements for 5G & how do you expect your IPX provider to address these? n=66



Source: Kaleido Intelligence

As such, it is key that players become well-versed in multi-protocol security, given that even when 5G SA roaming is rolled out, the overlap between 5G SA and earlier mobile generations will exist for years to come. Meanwhile, at least some of the security onus will fall onto operators' IPX providers: when asked in Kaleido's 5G roaming survey how security requirements for 5G should be managed and how operators expected their IPX provider to address these, they responded as per figure above.

Analysing these results further, it is apparent that implementation importance is viewed in the following order:

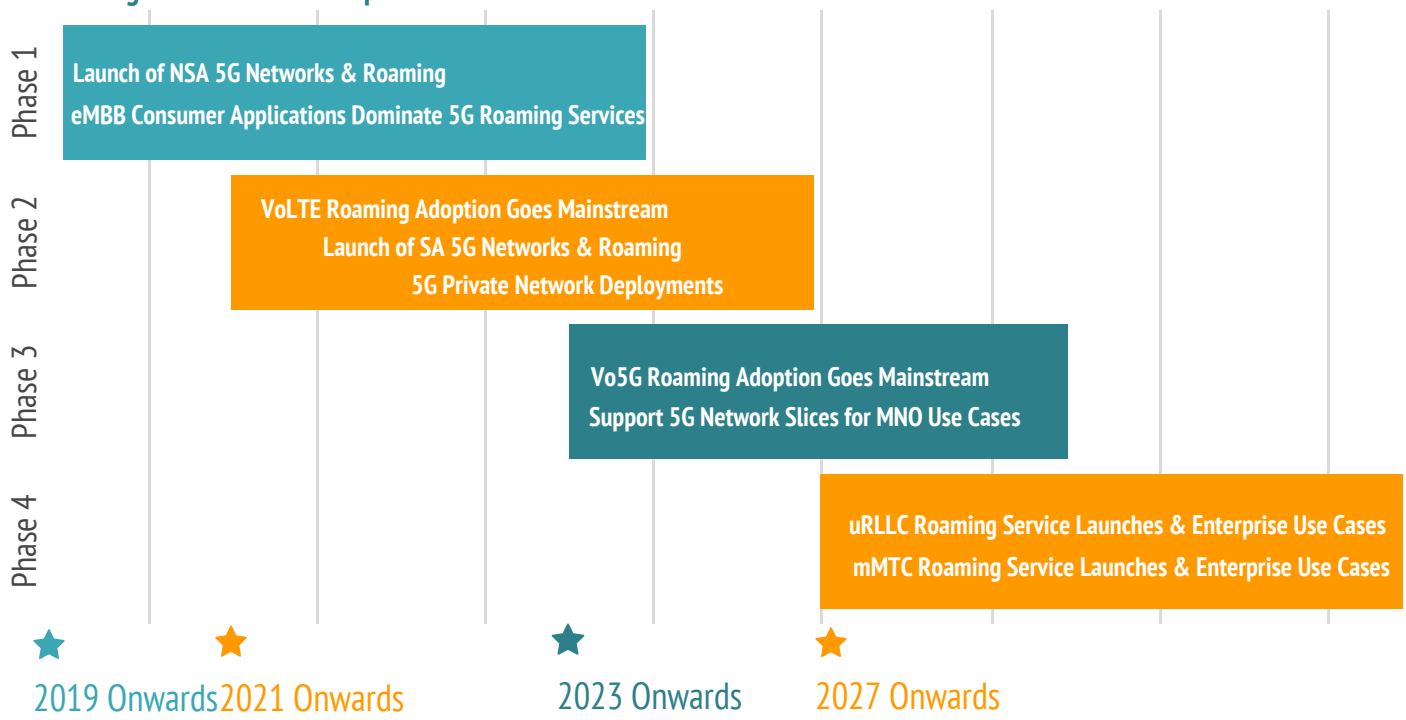
1. SEPP implementation
2. Service communication Proxy
3. Binding Support Function
4. Application layer firewall for GTP traffic inspection

Interestingly, some level of uncertainty continues to exist among the operator community: 15% of the respondents noted that they did not know which innovations should be implemented by their IPX provider.

The 5G Roaming Roadmap

Based on the various key requirements we discussed above, the below roadmap graphic illustrates our view on key milestones for 5G roaming and outlines our recommendations on what operators need to put in place and when.

5G Roaming Outlook & Roadmap



Source: Kaleido Intelligence

Kaleido recommends that operators prioritise and define a 5G roaming strategy and work with their IPX vendors to overcome all technical challenges with an emphasis on capacity, security and introducing new signalling and interworking protocols and functions.

In 2020, operators will need to focus on progressing the migration from 4G core to 5G and enable the transition from NSA to SA network architecture. This also means that operators will necessitate any work towards expediting VoLTE rollout as the transition towards 5G SA commences. In addition, following the launch of 5G NSA and commercial roaming agreements, eMBB applications will drive traffic over the next 4-5 years.

Following this, interworking with 4G and private networks will become critical as well as extending IPX to support all new possible roaming use cases delivering massive IoT and low latency communication services. This means that operators will need to build the foundation to handle any capacity requirements, support new use cases, provide slice management, integrate testing platforms for these new use cases, from at least 2021 onwards.

However, to fully capitalise on the 5G roaming opportunities presented by uRLLC and mMTC services, Kaleido believes that these use cases must be first established. IPX vendors will therefore need to prepare operators by delivering greater flexibility and scalability in terms of 5G roaming solutions and infrastructure, ranging from signalling and steering to clearing and settlement. It is our view that while network slicing will play an important role in future IoT roaming networks, it will not see significant growth until after 2023.

Prior to this, operators will rely on private LTE, and eventually private 5G networks, for the above-mentioned use cases. Finally, Kaleido believes that the rollout of 5G roaming services for uRLLC and mMTC use cases, when established, will be highly dependent on operators' ability to secure a return on investment. These will only be ascertained beyond 2027, meaning the immediate focus of network operators and IPX vendors will be on network upgrades to 5G SA and improving capacity to meet eMBB requirements.

Conclusion

5G is expected to enable numerous use cases, with roaming services delivered with consistent experience and improvements in delivering high-bandwidth mobile broadband and low-latency communication services. It is evident that 5G roaming will be dominated by 5G NSA in the short-medium term, with wider adoption of 5G SA roaming anticipated in the longer term. With most operators expected to continue to launch domestic 5G NSA (Option 3) networks, that is compatible with existing 4G roaming architecture and procedures, operators will need to begin to prepare for 5G SA roaming.

Operators will need a reliable, robust and comprehensive IPX solution to support the expected growth in roaming data traffic alongside support for newer protocols such as HTTP/2. Operators will require a converged interworking solution and will depend on partner vendors delivering a robust and dedicated interconnect network to accommodate data demand across a range of new consumer mobile and IoT roaming applications. There is also the future need to address different 5G roaming slices and standardised business models. Operators will also require both regional and local breakout to support their 5G roaming needs. However, while not an immediate requirement, local breakout will be required for use cases such as V2X communications, 4K/8K video services and other low latency applications and services where offloading data to the local network is recommended.

Kaleido recommends that operators collaborate and partner with the right vendors to accelerate their 5G roaming roadmap and the commercial introduction of 5G roaming services and business opportunities, alongside fostering innovations in signalling, clearing and security.

OPERATOR SURVEY METHODOLOGY & DEMOGRAPHICS

[1]This operator survey was conducted by Kaleido Intelligence in Q1 2020. The questionnaire was developed by Kaleido in partnership with leading industry stakeholders and contained 20 Questions (available on request).

The survey was completed by 60+ respondents across tier-1 operators around the world and were typically from the roaming business units. The demographics for regional distribution are provided below:

- Americas: 17%
- Europe: 34%
- Africa & Middle East: 14%
- East Asia & Pacific: 19%
- South Asia: 16%

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, the new iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator and Top 3 LTE IPX vendor with 700+ LTE destinations. With the integration of Tofane's acquisition of the Altice Europe N.V. international voice carrier business in France, Portugal, and the Dominican Republic, iBASIS today serves 1,000+ customers across 18 offices worldwide. iBASIS is taking major steps to help mobile operators experience a fast, secure and easy migration to 5G roaming with a flexible step by step approach. iBASIS is now introducing its 5G signaling exchange testing platform for 5G Stand Alone (SA), a comprehensive trial environment in preparation for launching commercial 5G roaming services with new service based architecture including new signaling protocol -http/2-.

To know more about the multiple scenario and use case testing please contact:

contact@ibasis.net

ABOUT KALEIDO INTELLIGENCE

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record delivering telecom research at the highest level. Kaleido Intelligence is the only research company addressing mobile roaming in its entirety. Our Mobile Roaming research service covers industry leading market intelligence and publications on Wholesale Roaming, IoT Roaming, 5G Roaming, IPX and Analytics & Fraud in Roaming. Research is led by expert analysts, each with significant experience delivering roaming insights that matter.

For more information on this market study or if you have further requirements, please contact:

info@kaleidointelligence.com

iBASIS
POWERED BY TOFANE

Kaleido Intelligence