www.ibasis.com www.kaleidointelligence.com

PRIVATE NETWORKS: REALISING THE 5G OPPORTUNITY 2022

A Kaleido Intelligence Whitepaper for iBASIS

iBASIS

Kaleido Intelligence

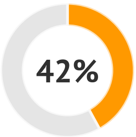
Table of Contents

Executive Summary

This Private 5G white paper from iBASIS and Kaleido Intelligence highlights the opportunities that Private 5G will bring for Communications Service Providers (CSPs), alongside the associated Private 5G requirements and expectations in terms of deployment types, vertical use cases and ecosystem roles. According to Kaleido Intelligence, Private 5G Network deployments are expected to expand considerably over the coming years, registering a 119% CAGR in site growth between 2021 and 2026, and will enable enterprises to leverage best-in-class technology to support critical business operations. In order to take advantage of this opportunity, CSPs must aim to understand the need for Private 5G over Private LTE, how the market in terms of verticals will adopt Private 5G, and what this means in terms of solution development and partnership requirements. This will enable CSPs to maximise the opportunities in this intensely competitive space.

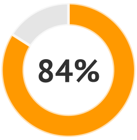
In January and February 2022, Kaleido Intelligence surveyed 92 respondents across tier-1 MNOs, MVNOs and IoT service providers worldwide to learn about their 5G roaming, security and private network go-to-market strategies, and commercial and technical requirements from an IPX and security perspective.

Key Takeaways



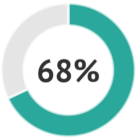
Manufacturing: voted as the top use case to drive Private 5G deployments in future, according to 42% of survey respondents. Healthcare and public safety applications were ranked second each by 19% of the respondent base.

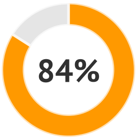
Top 3 Interconnect and roaming use cases: Manufacturing was voted by 97% of respondents as a top use case for inter-site connectivity and roaming. This was followed by healthcare (81%), and transportation and industrial (61%).



Mobility and Roaming: 84% of survey respondents view this as the main challenge to address Private 5G requirements when device component hardware availability and radio spectrum is removed from consideration.

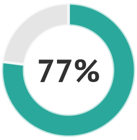
Core network security: 68% see core network security as a fundamental challenge to Private 5G, meaning that best practices at the signalling layer will be a critical area to address.



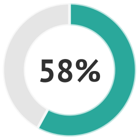


IPX role in signalling security: 84% view the IPX as a key player in monitoring and securing control plane traffic.

Interworking requirements: 77% of survey respondents view the IPX as an important partner for interworking between HTTP/2 and Diameter or SS7.



Key Takeaways



Need for enterprise education: 58% of respondents agree that enterprises still require education on the Private 5G concept, and will thus need guidance at all stages of their journey.

IPX plays a key role: longstanding IPX capabilities in terms of international coverage footprint, security, local breakout, routing, and interworking make these players ideally positioned to meet complex Private 5G requirements.

The Private 5G Opportunity

The last 3 years have seen a significant rise in attention and interest directed towards Private Cellular Networks. The high bandwidth, low latency, high security, reliability, and flexibility afforded by 3GPP cellular technologies bring together the best of alternative solutions such as Wi-Fi and industrial Ethernet while eliminating many of the associated drawbacks.

Until last year, the vast majority of Private Cellular Network deployments involved LTE. These offered an important upgrade over legacy TETRA and Wi-Fi deployments owing to superior reliability and coverage efficiency. However, LTE brings limitations that raise pain points for customers. Cell connection density is limited, for example, and meant that BASF's Private LTE Ludwigshafen production facility in 2020 was only able to connect 600,000 of its sensors, despite a desire to connect 6 million. Private 5G technology allows for 10 times the number of connected devices per cell, which would allow the company to achieve its aims in terms of connected devices.

Additionally, 5G is able to outperform LTE, Wi-Fi and wired communications solutions due to a combination of Gigabit throughput speeds and latency response times of between 6-10ms on average, and under 1ms in optimal conditions. In contrast LTE, offers average latency between 60-120ms. The fact that the technology is wireless allows far greater flexibility over industrial Ethernet solutions, which inevitably causes issues in the context of cable installations and any changes to the physical network design.

Further advantages of 5G include improved device positioning accuracy, which is important in production facilities, logistics hubs and medical facilities. Finally, mobility between cells is improved due to handover commands being issued earlier within the standard, offering greater reliability over LTE.

Private 5G Extends Capabilities

Private Networks using 5G core and radio components offer several advantages over LTE:

10x connected device capacity per cell.

Gigabit throughput using a single antenna, as opposed to 4 antennae using LTE.

Potential for sub-millisecond latency in optimal conditions and 10x reduction in latency compared to LTE on average.

Improved mobility and throughput reliability due to handover commands being issued earlier.

Support for network slicing models for the use of existing, but logically separated public radio spectrum.

Improved device positioning accuracy, with 3m indoor and 10m outdoor accuracy achievable 80% of the time.

Recently, the 3GPP completed work on Release 17 for 5G, which brings notable enhancements that will further drive the business case for 5G Private Networks, particularly in manufacturing and industrial environments. Release 17 includes work on positioning accuracy improvements, enabling centimetre accuracy (less than 1m for commercial deployments and less than 20cm for industrial IoT deployments) while also introducing latency improvements to aid in positioning accuracy and remote-controlled machine applications. In addition to this, the latest release includes capabilities to allow devices to be authenticated onto the network using third-party credentials, such as those used to access a public mobile network or alternatively another Private 5G site.

In January and February 2022, Kaleido Intelligence surveyed 92 respondents across tier-1 MNOs, MVNOs and IoT service providers worldwide to learn about their 5G roaming, security and private network deployment plans, and commercial and technical requirements from an IPX and security perspective. An initial question was aimed at identifying key vertical growth areas for Private 5G networks.

Manufacturing was found to be the top use case for Private 5G, owing to customer requirements concerning latency, positioning, and capacity, with 42% of survey respondents ranking this use case as the most promising. Healthcare and public safety applications were ranked joint second in terms of Private 5G potential use cases; here, video content is often vital to support such applications, with 5G capable of offering ample bandwidth. Industrial use cases ranked in third, achieving 23% of the vote in that rank.

Private 5G Vertical Opportunities

What are the top 3 segments that you believe have the highest potential for private 5G network deployments?

#1 Manufacturing

#2 Healthcare, public safety

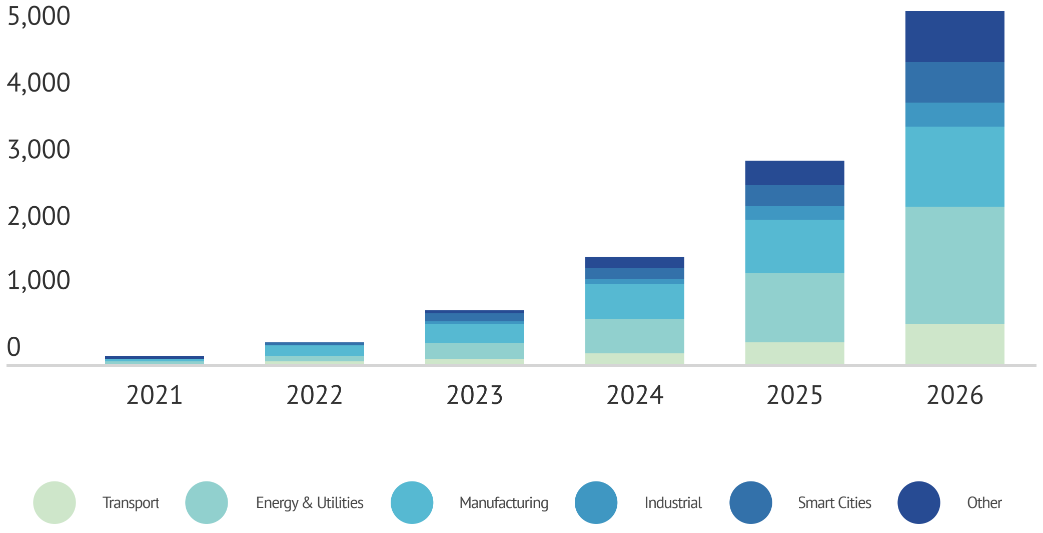
#3 Industrial

Source: Kaleido Intelligence

These survey results are matched with Kaleido's own projections for the Private 5G market, which show that manufacturing and industrial use cases will account for 30% of all Private 5G sites by the end of 2026.

> ***Overall, Private 5G is expected to be deployed in 33% of all Private Cellular Network deployments in 2026, with site deployments growing at an average annual rate of 119%, compared with 55% for LTE-based deployments.***
>
> **- Kaleido Intelligence Data Hub Q1 2022**

Kaleido Intelligence Data Hub Forecasts: Global Private 5G Site Deployments, 2021-2026



2026

5,339 Sites

Private 5G site growth will grow at 119% CAGR between 2021 and 2026, versus 55% CAGR for LTE sites

Source: Kaleido Intelligence

Although 5G brings many notable benefits, as discussed earlier, the market remains at a relatively early stage, although in some instances, the same is true for LTE. Private Cellular Network deployments are dependent on spectrum allocation: some countries have allocated specific spectrum ranges for enterprise use cases, while others have not, and will require partnerships with incumbent MNOs to access required spectrum.

Dedicated 5G Spectrum Launches/Plans - Country Examples

Canada

MNO route required.

Brazil

MNO route required.

France

Mid-band & mmWave spectrum earmarked for dedicated enterprise consumption.

Germany

Mid-band & mmWave spectrum released for dedicated enterprise consumption.

Finland

mmWave spectrum released for dedicated enterprise consumption.

Netherlands

mmWave spectrum released for dedicated enterprise consumption.

Japan

Mid-band & mmWave spectrum released for dedicated enterprise consumption.

United Kingdom

Mid-band & mmWave spectrum released for dedicated enterprise consumption.

Australia

mmWave spectrum released for dedicated enterprise consumption.

United States

Mid-band spectrum released for dedicated enterprise consumption.

Source: Kaleido Intelligence

Additionally, the processes for enterprises to access any dedicated spectrum vary considerably across the globe: for instance, Germany offers a relatively simple process whereby enterprises can apply directly to BNetzA (the regulator), players in Japan must deal with local authorities, while the US and several other countries have, or intend to hold spectrum licence auctions which often means that enterprise customers must deal with a third party (the licence holder) to enable the deployments. Meanwhile, where dedicated spectrum is not available, MNOs typically have a gatekeeper role in that they own the relevant spectrum for any 5G deployment. Here, relevant players must consider spectrum leasing or RAN sharing models to support Private 5G initiatives.

This fragmentation has presented a challenging set of choices for chipset and module makers aiming to address the Private 5G opportunity, as it is difficult to reach desired economies of scale without broad spectrum harmonisation. Nevertheless, according to the GSA, there are now 56 chipset platforms and 17 discrete modem solutions with 5G NR compatibility available on the market, while several module OEMs have now launched products to address 5G Private Network requirements across several regions.

Addressing the Private 5G Enterprise Need: Service Provider Strategies

Most historical Private Cellular Network deployments have been architected to ensure that all signalling and user plane traffic is fully isolated to guarantee maximum security and performance. This approach comes with drawbacks, mainly in the form of elevated capital expenses in addition to the inability to address connectivity needs when assets and workers move to locations outside of the Private Network coverage zone. **The result of this is that many service providers have now developed so-called hybrid Private Network models, whereby dedicated radio components remain on-site, but core network functions are delivered from virtualised environments. Delivered via as-a-service models, hybrid deployments can significantly reduce the capital outlay required to launch a Private 5G network and thus lower entry barriers for smaller enterprise customers.**

Additionally, an increasing number of enterprises have shown a desire to maintain connectivity continuity across Private Network sites and between private and public Network infrastructure. In essence, this means that devices must be capable of authenticating either with more than one Private 5G site or private and public HSS and billing systems, with multi-site and multi-network access required in some cases.

Hybrid Private Network deployments and inter-site and public network connectivity requirements are now driving the need for interconnect and roaming services to extend Private Network services over and above what was typically demanded in historical projects. Supporting these services requires expertise in several areas:

A broad connectivity footprint to enable assets and workers moving outside of the Private 5G network to maintain connectivity continuity. If this is to be addressed at global scale, the service provider must have secured a substantial number of roaming partnerships with MNOs across the globe, with appropriate wholesale agreements to service both M2M as well as 'consumer'-type communications requirements.

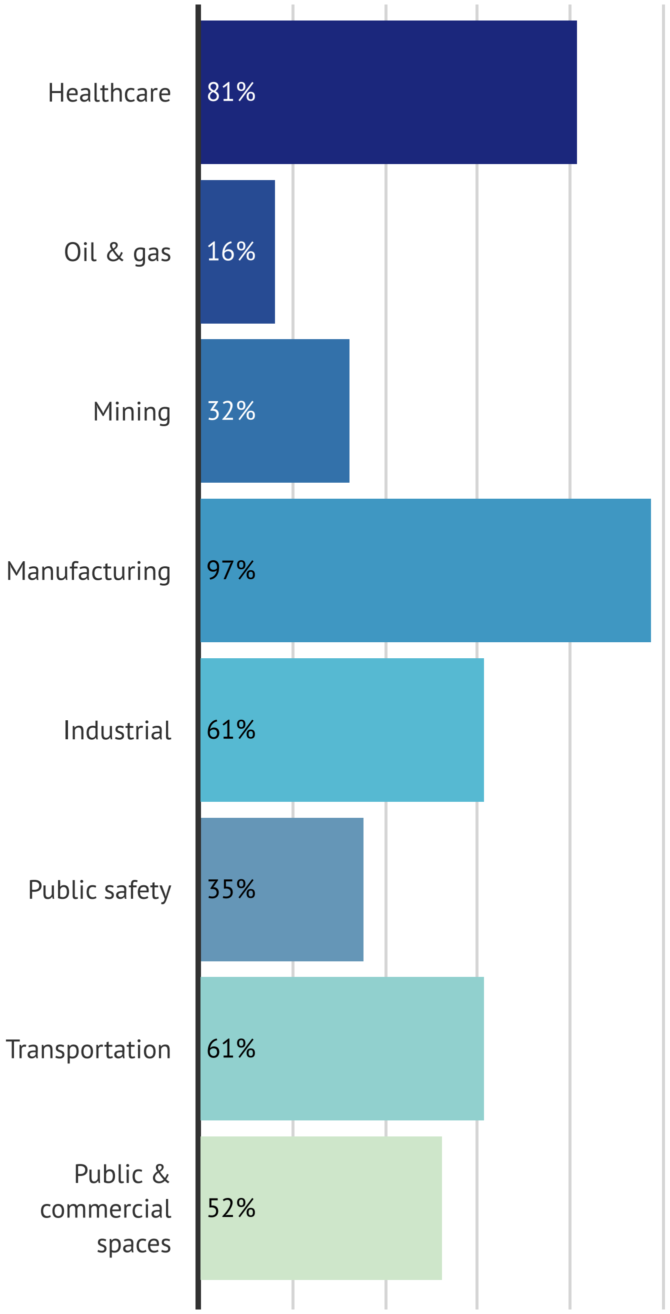
Secure routing and traffic separation capabilities, to allow business-sensitive user plane data to remain fully isolated from public network infrastructure, while allowing signalling data egress to the virtualised core network off-site.

Network authentication and handover management capabilities to allow endpoints to register with appropriate private and public networks. Presently, 3GPP standards for handover have not been built with public-private network roaming in mind, and as such some customisation is required to avoid the end-user manually forcing the device to switch between networks, such as SIM applets or via customised network management solutions.

Beyond the Private 5G Firewall: Vertical Opportunities

When asked which verticals are most likely to require interconnect services (ie inter-site connectivity or roaming) for Private 5G networks, respondents emphatically reported manufacturing as a key use case. This vertical was named by 97% of surveyed individuals. Meanwhile, healthcare was also seen as a vertical likely to require such services, with 81% of respondents agreeing. This was followed by transportation and industrial use cases, with 61% of survey respondents naming each of these verticals as most likely to require interconnect. At this stage it is important to understand how various vertical industries might use the interconnect to augment the Private 5G deployment:

Which 5G Private Network segments do you believe are most likely to require interconnect through IPX?



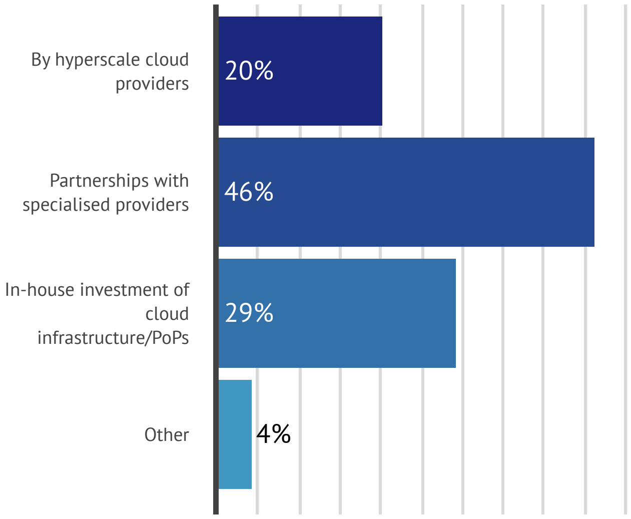
Source: Kaleido Intelligence

- **Manufacturing & Industrial use cases**: in many instances, products made or produced within the plant or production complex carry embedded connectivity. These products are then shipped to other locations around the globe, with connectivity continuity desired by the Private Network customer. The globally distributed nature of supply chains means that roaming coverage is essential in this instance so that the connected asset can maintain connectivity wherever it is shipped. Additionally, remote data sharing is often desirable, requiring interconnect between 2 separate Private 5G networks. For instance, Ford intends to connect its EV powertrain production facility with a welding specialist partner using Private 5G to allow expert workers to support operations between the sites.
- **Healthcare use cases**: demand for telehealth applications has been growing rapidly in recent years, and has only accelerated in light of the ongoing COVID-19 pandemic. With many healthcare facilities now looking to upgrade their sites from unreliable Wi-Fi to cellular technology, customers will be looking to establish a secure pipe between Private Network sites to maintain a high level of security to support use cases such as staff and equipment tracking, telehealth applications, and pop-up care. Core to the business case are remote sensor applications for remote patient monitoring, in addition to connected pacemakers and defibrillators for chronic disease patients.

- **Transportation use cases:** ports and logistics hubs have formed many of the historical client base for Private Cellular Networks, with airports now signalling an increased interest in establishing sites to improve back-office functions and passenger-facing services. The nature of these industries means that workforces and assets frequently travel all over the world and that employees need to remain connected to provide or receive support. Meanwhile, assets require tracking and monitoring as they journey and land at their destination.

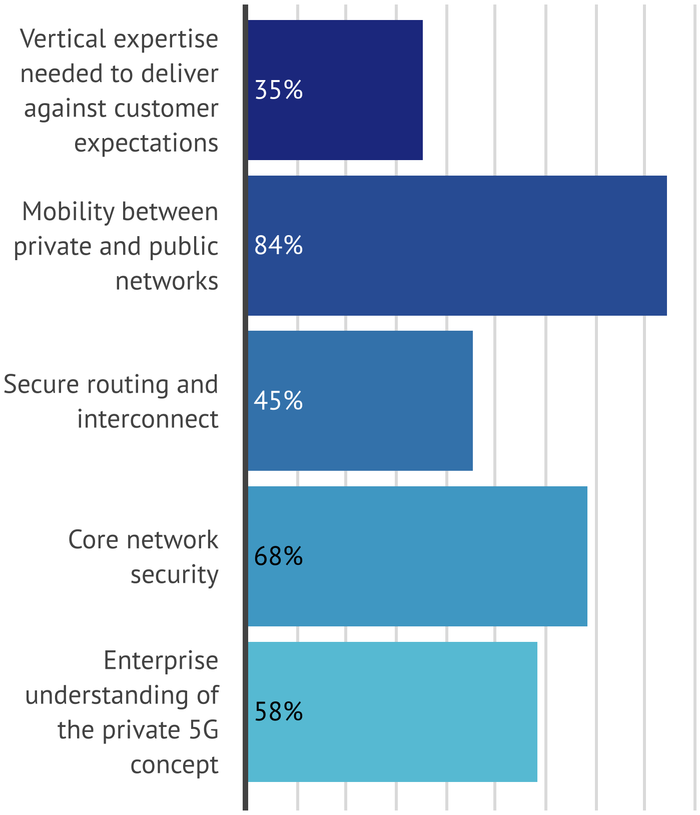
While we have established that several Private 5G use cases will require mobility between public and private networks, it is important to understand that this is not a trivial feat to accomplish. Indeed, 84% of survey respondents view this as the main challenge for Private 5G networks, when issues such as modem, chipset, and spectrum availability are taken out of the equation. Additionally, 5G core network security is seen as a critical issue, with 68% of survey respondents seeing this a fundamental challenge.

How do you believe MEC/virtual core services will be rolled out in future?



Source: Kaleido Intelligence

Aside from spectrum and hardware availability, what do you see as the main challenges in serving and deploying private 5G networks?



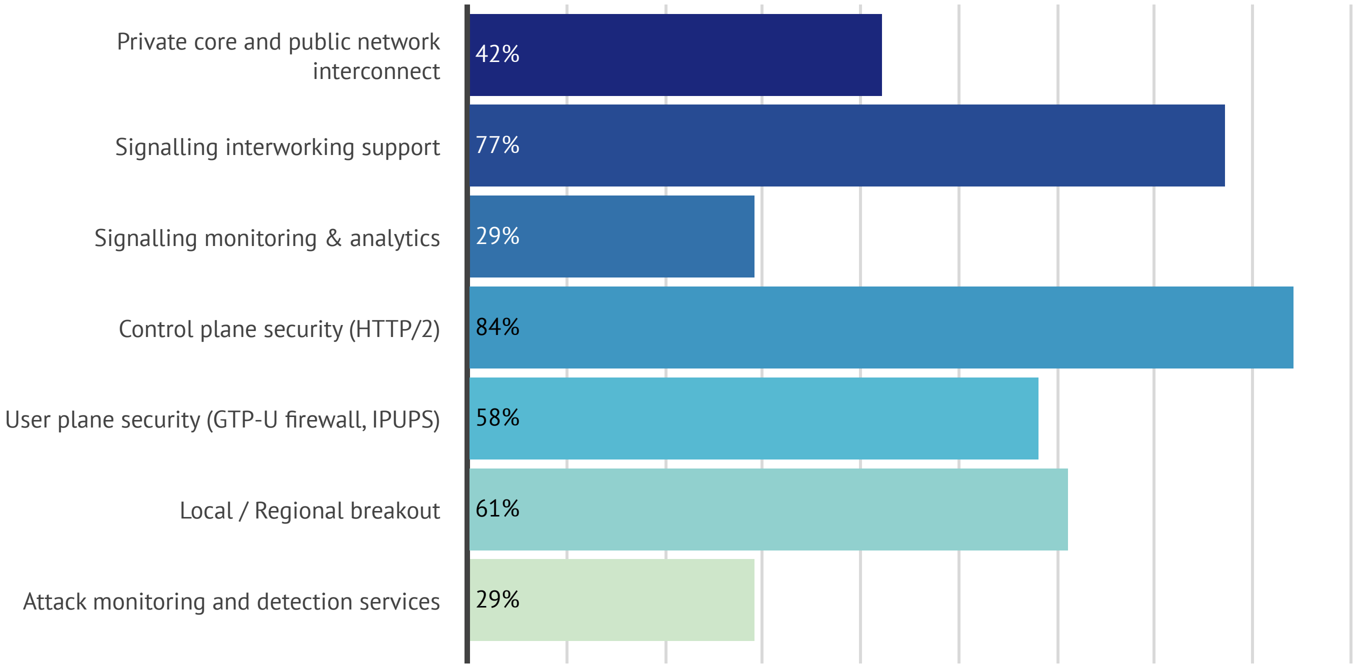
Source: Kaleido Intelligence

At this stage, the question arises as to what type of market player is best positioned to address enterprise needs and Private 5G challenges. On the one hand, one might assume that hyperscale cloud service providers are more than capable of establishing interconnect services for inter-site connectivity. Nevertheless, a similar study conducted during January-February 2021 by Kaleido Intelligence (which saw nearly 70 respondents across tier-1 operators around give their opinions on the evolution of IPX roles in the 5G era) found that 70% of respondents did not see their relationship with IPX providers changing in the face of new MEC and virtual core enablement. Only 20% of the respondent base saw hyperscalers as well-positioned to enable MEC, and virtual core interconnect services.

IPX Roles in Private 5G

Additional support for the IPX role in enabling advanced Private 5G services is gathered when considering the international aspect of connectivity requirements. Today, IPXs are fundamental in enabling one-to-many inter-operator connections, with very few MNOs having established direct interconnects with partners to enable roaming services in the visited network. This means that, from the outset, the IPX has transport solutions to several hundred mobile networks across the globe to enable assets and workers to leverage connectivity continuity away from the Private 5G site, and securely enable that. Indeed, many IPX providers have additional expertise in signalling security, which is the primary attack surface for cybercriminals when roaming fraud and security is considered. The ability to monitor and manage any security threats that arise across signalling protocols is a key core competency required to maintain security of the core network, and is especially important when considering the fact that off-site virtual core networks are now demanded as a means to lower capital expenses. It is thus not surprising to see that 84% of survey respondents view the IPX as critical in maintaining control plane security. Meanwhile, 77% of survey respondents reported that signalling interworking support is a key IPX role: while Private 5G Networks will use the HTTP/2 protocol for signalling, many public networks around the globe will either not yet have a live 5G core, or have established 5G standalone roaming services. As such, interworking between HTTP/2 and Diameter (for LTE networks and LTE roaming), or SS7 (for 2G/3G networks and roaming) in some instances, is an important capability. As with other services mentioned earlier, IPXs have significant experience in this domain to offer reliable services.

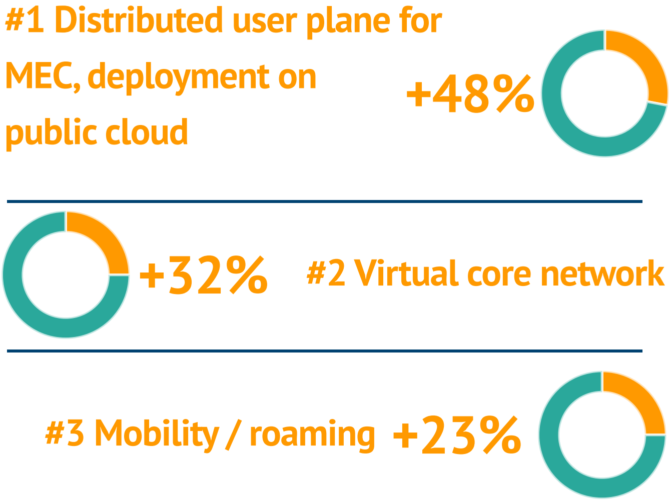
What services do you expect from your IPX provider to support private 5G use cases?



Source: Kaleido Intelligence

The importance of leveraging IPX relationships to aid in the security of advanced Private 5G deployments becomes apparent when considering that the survey revealed that a distributed user plane for MEC, deployment on public cloud as well as mobility and roaming services ranked within the top 3 Private 5G security concerns among survey respondents.

What are the top 3 elements of a private 5G network deployment that you perceive as the most challenging to mitigate in terms of security risk?



#1 Distributed user plane for MEC, deployment on public cloud +48%

#2 Virtual core network +32%

#3 Mobility / roaming +23%

Source: Kaleido Intelligence

The Essential Actions For Private 5G Success

This white paper has demonstrated how the Private 5G market is set to see substantial growth over the next 5 years as enterprises within verticals such as manufacturing, industrial, healthcare and transportation seek to optimise business processes and leverage cellular technology over other options such as Wi-Fi and TETRA. While there is evidently a significant opportunity for CSPs to capture a share of the market, presenting the best business quality and value will depend on a best-in-class proposition that can cater to the unique demands of the enterprise customer.

Understand the evolving needs of Private 5G Networks

As with almost all industries, much of the market's future growth is likely to be driven by enterprises that do not have the significant upfront capital required to deploy Private 5G Networks where all network components are positioned on-premises. As-a-service models are critical to moving costs towards Opex-based models, and lower the barrier to entry. Therefore, deploying dedicated core network infrastructure in virtualised environments either on a country or regional basis is a crucial requirement moving forward. This can either be achieved in-house, with many IoT MVNOs now moving towards this type of capability or by partnering with core network software specialists who have experience delivering solutions for Private LTE and 5G deployments.

Due to the challenges still surrounding Private 5G in terms of spectrum and radio component availability, enterprises may still wish to leverage Private LTE if they have immediate needs.

As such, the capability to ready and define an upgrade path for the core network infrastructure is a key tenant behind overall cost reduction for the customer, should it wish to migrate from LTE to 5G in future. It is thus important to work with the customer from the outset to define long-term goals for any deployments, and help it understand the implications of technology choice, how the upgrade path is achieved, and the cost implications of doing so. As enterprises are largely unfamiliar with the nuances of 3GPP technologies, education remains a significant part of helping customers through the journey of concept to live deployments. Indeed, we have seen earlier that 58% of survey respondents agreed that enterprise understanding of the Private 5G concept is one of the market's key challenges.

Understand how IPXs can help deliver advanced Private 5G services

As we have seen earlier, interconnect and roaming services are likely to be leveraged by many Private 5G customers, where international coverage, routing, security, reliability and QoS can offer differentiation points. Moreover, these types of deployments offer CSPs an elevated revenue opportunity as connectivity continuity becomes a factor in international scenarios and helps deliver additional value to the customer. As IPX providers have a long experience in all of these areas, these players are likely to become crucial partners in enabling service extensions to the Private 5G network, and may offer additional benefits in the form of sponsored roaming to extend the international coverage footprint.

Additionally, One of the main benefits of 5G technology is its capability to reduce latency to enable advanced connected solutions such as robotics and remotely controlled applications and services. Additionally, asset management, automotive and aviation use cases often require that significant volumes of data are offloaded locally at high speed. Here, traditional home-routed roaming architectures will not be sufficient, driving the need for local or regional breakout services to enable this. The rise of 5G Multi-Access Edge Computing (MEC) architecture to process data locally will additionally play an important role in enabling this, alongside local or regional breakout services.

CSPs with their own capabilities to deploy virtualised GGSN/PGW instances on a country or regional basis must examine the ROI potential of instantiating new infrastructure for client requirements, while also considering the fact that partnerships may be available to help reduce costs in addressing specific markets. Without a doubt, those CSPs without such capabilities looking to tap into the Private 5G market must aim to develop relationships with service providers to enable this type of solution. There are a number of providers on the market capable of addressing this, although from a cost-benefit and complexity point of view, it may be prudent to investigate existing IPX relationships as these providers often have a significant number of breakout gateways already deployed.

Focus on a vertical and expertise, and develop the portfolio around that

The Private 5G market expected to become an intensely competitive space, with competition exacerbated by the fact that 5G network slicing models have still not been broadly commercialised. In the connectivity space, this means that MNOs, neutral host providers, and MVNOs are all turning their focus towards the market as a key opportunity to monetise 5G network capabilities beyond FWA and consumer mobile applications over public networks. Through the survey results, we have observed how several verticals are poised to see an increase in Private 5G demand due to specific performance and service quality requirements. It is important to understand that no single provider will be able to dominate the market. In the same manner as the broader IoT market, enterprise requirements are typically bespoke, although in the Private Network space, an understanding of specific vertical needs and challenges becomes even more important. Private Network customers have already observed this in the market, where work with traditional mobile network vendors resulted in challenges since these providers have historically worked with MNO clients to deploy networks rather than directly with enterprises.

How the portfolio is developed thus becomes immensely important if a differentiated solution is to be developed. On the one hand, establishing key partnerships with Systems Integrators (SIs) represents a major step towards developing the solution, as relevant SIs will have a deep understanding of both vertical requirements and the ecosystem providers best positioned to deliver against those requirements. On the other, the development of the CSP's own core competencies will be a defining factor of market success in the connectivity space.

Aim to understand and address the technical requirements for public-private network authentication

3GPP standards offer limited support for more complex Private 5G deployments where authentication on the private as well as public network is required. In essence, there is no built-in mechanism to ensure that network handover is completed seamlessly, and the industry has historically resorted to cumbersome mechanisms such as forcing the user to switch networks manually. This is clearly not a suitable mechanism for M2M devices, which may not even have an interface with which to complete the switch back to private network access as they roam in. Providers are thus now moving towards models based on multi-IMSI or eSIM, whereby differentiated IMSIs or SIM profiles can be leveraged to authenticate on each network type, often with support in the form of an applet to gauge signal strength and implement a deterministic handover mechanism.

Achieving this handover in the most seamless manner possible will be an important factor moving forward as a means to maximise QoE and potentially reduce excessive customer connectivity costs that might be incurred if devices do not attach to the private network in a timely fashion. Meanwhile, it is important to consider how the 'roaming out' of devices and workers is managed and optimised. Should coverage on the public network be required in diverse international locations, it is important to consider both the roaming footprint and any capabilities to localise connections with operators in the country of operation. On the roaming side, this means ensuring that roaming rates are not excessive, while also ensuring that a minimum of 2 network operators are available to attach to in the visited network. The ability to have control over network steering would be an additional benefit, should the customer have specific requirements. In the context of localisation, eSIM becomes more important, with many CSPs having limited capabilities in this area, and would likely benefit from a partnership to ensure that profile selection, where available, can be optimised OTA as a means to address specific cost as well as compliance requirements in certain countries.

Conclusions

Private 5G is fast becoming a requirement

We have observed how 5G offers significant enhancements over LTE as well as wired communications solutions. The need for expensive cabling installation is minimised, while the physical network design can be repurposed without the disruption involved with Ethernet. Meanwhile, 6-10ms latency is achievable on average, in addition to Gigabit throughput speeds, centimetre-level positioning accuracy, and the capability of connecting 1 million devices per cell. These features mean that Private 5G is rapidly driving interest from several industry verticals, such as manufacturing and industrial use cases, transportation, and healthcare applications.

The Private Network is evolving

While Private Networks were historically deployed as standalone entities on-premises, enterprise customer demands for solution capabilities are evolving. Many customers now wish not only to interconnect disparate Private Network sites, but also wish to ensure that connectivity continuity is maintained even as devices move beyond the Private Network coverage zone. New business models are emerging, where the mobile core network is located off-site, frequently in a virtualised environment.

These factors mean that solution providers must be capable of delivering against the need for roaming capabilities, while ensuring that the highest levels of security are adhered to to ensure that traffic flow between public and private networks is not compromised. Additionally, some industry verticals will have specialised requirements, where high performance and low latency will be needed both inside and outside the Private Network footprint. CSPs must be capable of offering local or regional breakout services to address this, as traditional home-routed roaming architectures are unlikely to meet customer requirements.

IPX choice will be key

The IPX is expected to play a major role in signalling interworking, customer Private 5G 'roam in, roam out' requirements, local breakout services and signalling security. These players have significant experience in ensuring that trust between roaming operator partners is maintained. This experience translates well to the security frameworks and requirements introduced in Private 5G Networks. Additionally, IPX providers typically offer robust coverage footprints and breakout services to the extent that few other players can match.

Choosing an appropriate IPX provider will be fundamental in ensuring that best-in-class services are offered to Private 5G enterprise customers in instances where deployments beyond a fully isolated Private Network architecture are required.

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator, Top 3 LTE IPX vendor with 700+ LTE destinations, and a leading Carrier Cloud Communications player and IoT solution provider. iBASIS today serves 1,000+ customers across 21 offices worldwide.

iBASIS is taking major steps to help mobile operators prepare for 5G Standalone (5G SA) roaming enablement with a flexible step by step approach. iBASIS has deployed a 5G SA testing hub, a comprehensive and evolutionary trial environment with new service based architecture, and is now in the phase of connecting Mobile Operators. The 5G SA hub allows to test a full range of technical operations, including the signalling interconnection scenarios as recommended by the GSMA, data exchange, voice call flow testing, as well as 4G-5G interoperability and SEPP outsourcing. Additionally, iBASIS plan to expand the scope to test a real live 5G SA peering as well as slice based routing scenarios and 5G SA roaming VAS.

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

mjamli@ibasis.net

For more information, please visit iBASIS.com.

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 & Connectivity research service covers industry leading market intelligence and publications on Wholesale & Retail Roaming, eSIMs, 5G Roaming, IPX, Private Networks, IoT MVNOs, IoT Roaming and Roaming Analytics & Fraud. 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

Publication Date: 15th June 2022

Kaleido aims to provide accurate information. The information provided here is designed to enable helpful data and insights on the subjects discussed. References to companies are provided for informational purposes only and Kaleido does not endorse any operator, vendor or service included in this research and market study. While information and content of this publication is believed to be accurate at the date of publication, neither Kaleido Intelligence nor any person engaged or employed by Kaleido Intelligence accepts any liability for any errors, omissions or any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication. This white paper consists of the opinions of Kaleido and should not be construed as statements of fact. It contains forward-looking statements and market forecasts that have been developed based on current information and assumptions. These are subject to market factors such as, not limited to, unforeseen social, political, technological and economic factors beyond the control of Kaleido Intelligence.