WHITEPAPER

Mobile Cores for the Internet of Things

INSIDE THE WHITEPAPER

Overview

Wireless communications is everywhere in 21st century life. Every time you make a phone call, send a text, or access a cloud-based service, a complex dance among interwoven technologies unfolds, unseen, in just a few milliseconds. Consumers don't worry about those events, they care only that they happen quickly and reliably.

It's a different story for builders of cellular IoT solutions. Every step of that dance matters. Missed steps and poor timing adversely impacts the speed at which data transfers through the network. Seemingly minor issues in the interconnected systems can combine to threaten the viability of the entire IoT solution.

A key component of any wireless network is known as the core, or *mobile* core. Addressing many common questions related to mobile cores, this whitepaper will show you how mobile cores can impact your IoT solution, why your cellular provider should focus on efficiency and flexibility of their mobile core, and, most importantly, why a mobile core tuned for IoT is critical to the success of your IoT solution.

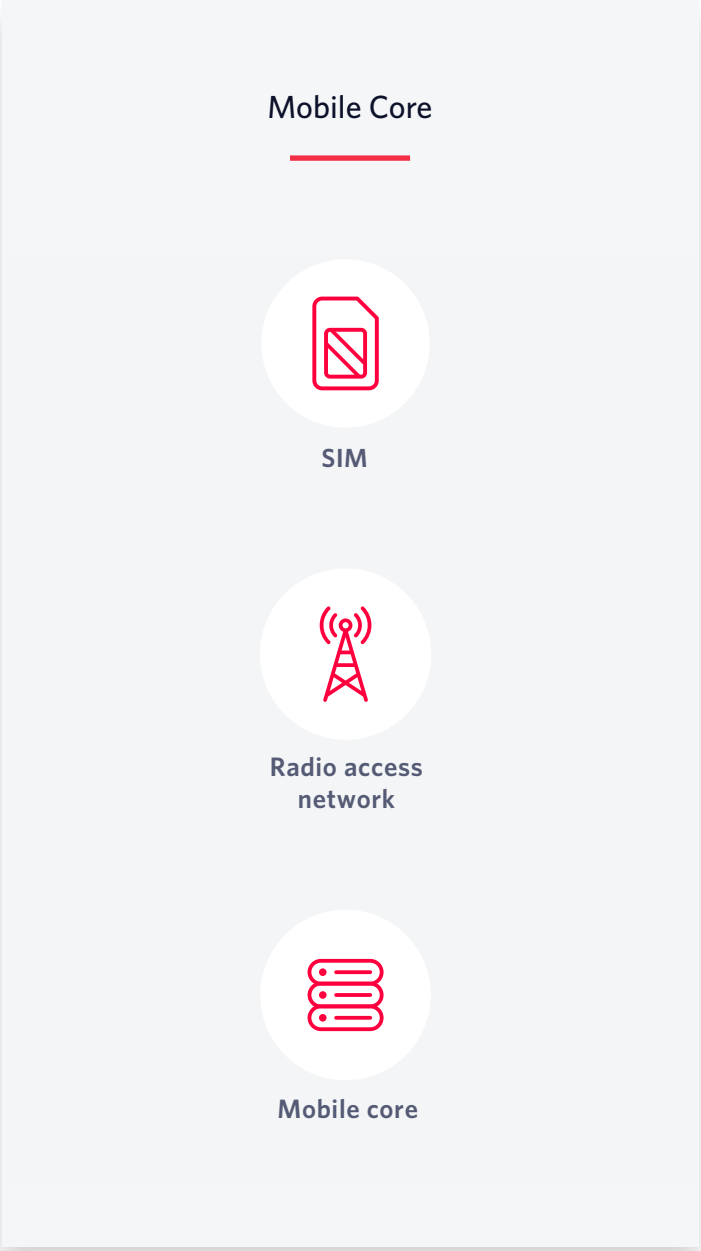
1 What is a mobile core?

While most people think of cellular data networks as the towers and sites that provide the RF (radio frequency) signals used by our devices, the real dance takes place inside what's called a mobile core – effectively the "brain" of a mobile network.

What does a mobile core do?

"The core," as most telco engineers call it, is a set of computing processes that runs on a server. It could be one server in an IT closet, several servers in a warehouse, or cloud servers. At a high level, the core runs processes to operate the mobile network and subscriber devices. It's responsible for managing the interface between the base station radios sitting on towers, buildings, and poles, and other radio access networks, or between radio access networks and external networks such as the internet.

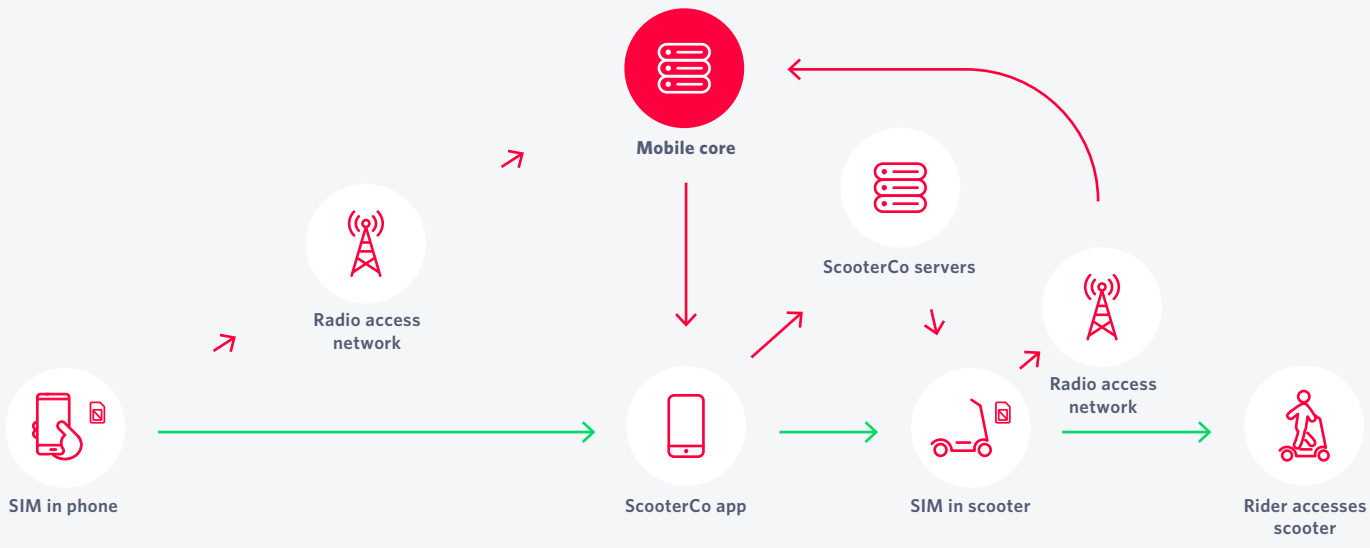
The mobile core choreographs the mobile network dance. It determines if a given device may attach or connect to the network. If the device is approved, then the core passes data through the network to external networks—which can be either private or the public internet. It determines the path which user data takes as it moves around a country—or around the world. The mobile core authenticates the Subscriber Identity Module (what you probably know as the "SIM") inside the subscriber's device. After authenticating the SIM, the core authorizes various services for the user device, and allocates an IP address to the user device to route data traffic as mentioned above. All of this happens in a matter of milliseconds.



ScooterCo: a mobile core example

Let's illustrate how a mobile core works with an example. Imagine a fictional on-demand scooter company, ScooterCo, and the complex dance of interlocking systems that happens when a rider wants to unlock a scooter through the ScooterCo app. If the SIM in the rider's phone is properly authenticated by the cellular data network's mobile core, she's allowed to access the internet, and the mobile core establishes a data connection between her app and ScooterCo's servers which may be in another city – or another country. Then the core creates the path that data takes across the internet with routing algorithms. Once the rider's username and password are confirmed by ScooterCo's servers, and the rider's chosen scooter is identified by the app, the app "asks" the ScooterCo server to unlock the scooter, which is also connected to the cellular data network – through its own SIM and thus identity on the network. Presuming all is in order, the ScooterCo server orders the rider's chosen scooter to unlock and our rider is happily on her way. Because all of this happens within a few milliseconds, the rider's experience is heavily dependent on the speed and reliability of this seemingly simple transaction. Figure 1 demonstrates this visually.

Figure 1: Role of the mobile core in connecting a rider to a scooter



2 Key components of a mobile core

Components of a mobile core may be instantiated in geographically-separated systems, or contained within a single system, but all mobile cores provide the following functionality:

- Access to the Home Public Land Mobile Network (HPLMN) – your service provider's own network
- Access to Visited Public Land Mobile Network (VPLMN) – the network of other providers that grant your device access while roaming
- An IP Backbone

Before we dive into this functionality a little deeper, let's quickly review a technical element used by the mobile core: **the International Mobile Subscriber Identity (IMSI)**. It is a globally unique numeric code formed from combining the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscription Identification Number (MSIN), which is a unique number assigned to a device SIM. In a sense, the IMSI is the unique "address" for any given mobile device. For example, the MCC for the United States is 31X (where X ranges from zero to six), and the MNC for T-Mobile is 260. Combined with an MSIN of, say, 4071237654, you would get 3102604071237654 as a globally unique IMSI for a particular device's SIM. Figure 2 illustrates the composition of IMSI numbers.

Figure 2: Sample IMSI

IMSI	310170265624299	
MCC	310	USA
MNC	170	SPRINT
MSIN	265624299	

Home Public Land Mobile Network (HPLMN)

This is the "home network" for any given device in a mobile data network. If a mobile device is not in its home network, the visited network, through which it roams, will contact the home network (via messages through – you guessed it – the mobile core) to confirm that the device is authorized to access the network. This is what happens when you use your phone in a foreign country. The HPLMN is a network owned by the owner of the IMSI, i.e. the service provider you have a contract with – say, T-Mobile or Telefonica. All HPLMNs require the use of a Packet Data Network Gateway (PGW). The PGW manages connectivity between the device to external packet data networks, enforces policies, filters packets, and assigns IP addresses and Domain Name Service (DNS) servers. The Domain Name Service (DNS) converts human-readable addresses like "www.twilio.com" into numerical addresses usable by network routers. Finally, the HPLMN requires a Home Subscriber Service (HSS). The HSS generates an authentication vector (or challenge) using a private key stored in the device's SIM which is sent for SIM authentication.

Visited Public Land Mobile Network (VPLMN)

The benefit of mobile data networks is portability and flexibility, where a device can cross the borders of its home network and still be connected. It is important to understand that the mobile core plays a crucial role here, as the Visited Public Land Mobile Network (VPLMN) communicates with the HPLMN via the mobile core. **This is why the mobile core performance has a major impact on efficiency of the system as a whole when devices are not in their home network**. So how does the VPLMN work? The VPLMN uses a Serving Gateway (SGW) to route user data, deactivate idle data paths, and page the user equipment when downlink data is queued for downlink. Then, the Mobile Management Entity (MME) interfaces with user equipment (such as the cellular modem in the ScooterCo example), chooses the SGW, authenticates SIMs via the user's Home Subscriber Service, and enforces roaming restrictions. Now that the device is authenticated, the VPLMN uses a Diameter Routing Agent (DRA) to manage routing and throttling of Diameter messages between MMEs and SGWs and other data nodes, and acts as a load balancer.

IP Backbone

The whole point of IoT is to get data. That data needs a pathway across different networks. In a cellular mobile core, that pathway is managed by the IP Backbone. In cases where data is exchanged between dissimilar networks (such as a voice call between two carriers using different air interface technologies,) the data is converted into a common language (IP - a key protocol of the Internet) before transiting across the IP Backbone. The IP Backbone defines protocols such as GPRS Roaming and CDMA Roaming. The IP Backbone includes the IP Exchange (IPX), GPRS Roaming Exchange (GRX), and CDMA Roaming Exchange. It's responsible for routing data between the HPLMN and VPLMN networks, as well as handling inter-operator peering across IP networks.

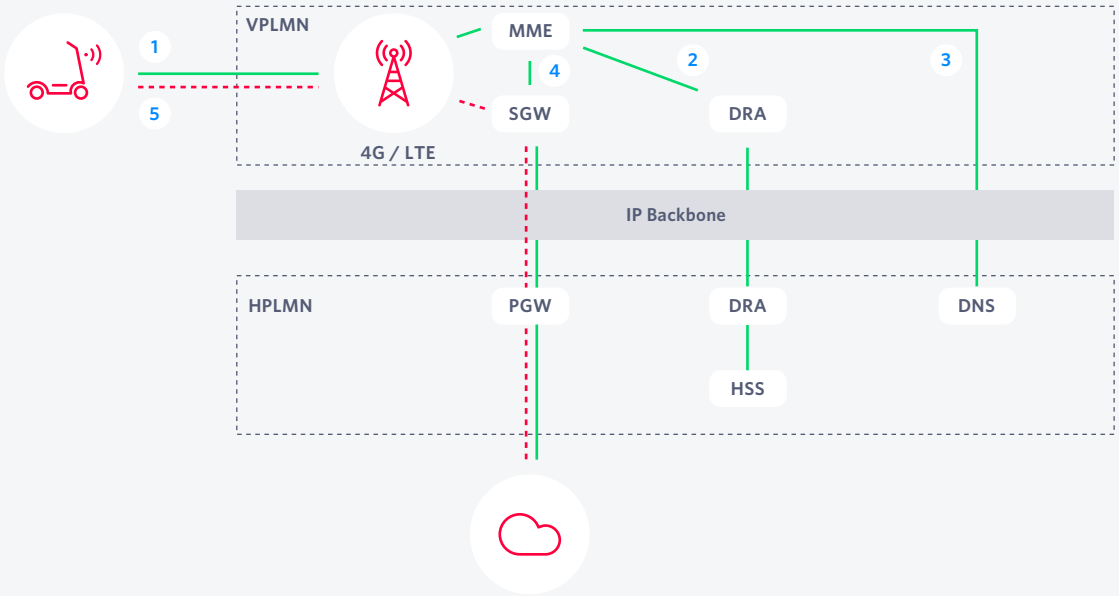
What does this have to do with IoT?

IoT deployments demand more flexibility, control, monitoring and scalability than a carrier's mobile core can provide; after all, carriers initially designed and built their networks for our phones. This opens up the market for agile software companies to build a flexible and scalable software-based core, designed and optimized for the needs of IoT fleets. It virtualizes the HPLMN and VPLMN and should be architected as a distributed or "cloud-based" mobile core. This architecture should differ from a traditional mobile core in several important ways, all of which benefit IoT solution providers and end users alike. Chapter 3 will address these differences.

Back to the ScooterCo example

In the ScooterCo example above, our scooter rider unlocked the vehicle with her mobile phone. Behind the scenes, all of the aforementioned systems played a role in making that happen. The rider's smartphone provided its IMSI to the nearest tower and requested permission from the local network to send and receive data. The local network contacted the rider's home network via the mobile core to confirm her account was active and allowed to send data. Once that permission was given, the mobile core handled the exchange of data between the ScooterCo app and the ScooterCo servers. Likewise, the scooter she chose communicated with the ScooterCo servers across a data connection managed by the mobile core. Figure 3 illustrates these components working together.

Figure 3: Components of a mobile core in connecting a rider to a scooter



1. The modem contained in the scooter scans for the nearest cell tower to connect. This procedure is typically initialized by the base stations and terminated at the MME node of the VPLMN. The MME is one of the central components of the VPLMN. The MME identifies whom the IMSI belongs to by extracting the MNC and MCC fields. **If the device is roaming**, then the MME will need to talk to the HSS of the HPLMN in order to authenticate and authorize the scooter to connect to the network.

2. The protocol used for exchanging authentication, authorization, and accounting messages between the MME and the HSS is conducted by the DRA.

3. Once the HSS gives an "OK", the MME determines which internet gateway to use for sending internet traffic. In LTE architecture, the PGW is used. In order to figure out which PGW to use, the MME performs a simple DNS query to get the PGW's IP. This is handled via a simple DNS lookup of the access point name to the HPLMN DNS server.

4. Once the selection is done, the MME instructs the SGW to establish a GPRS Tunnel Protocol tunnel with the selected PGW.

5. Once the required tunnels are established, the device can connect to the internet.

3 Why Distributed IoT Mobile Cores are better for your IoT solution

In the world of cellular connectivity providers, we can distinguish between the following 2 types of companies:

- Traditional carriers, or Mobile Network Operators (MNOs)
- Resellers, or Mobile Virtual Network Operators (MVNOs)

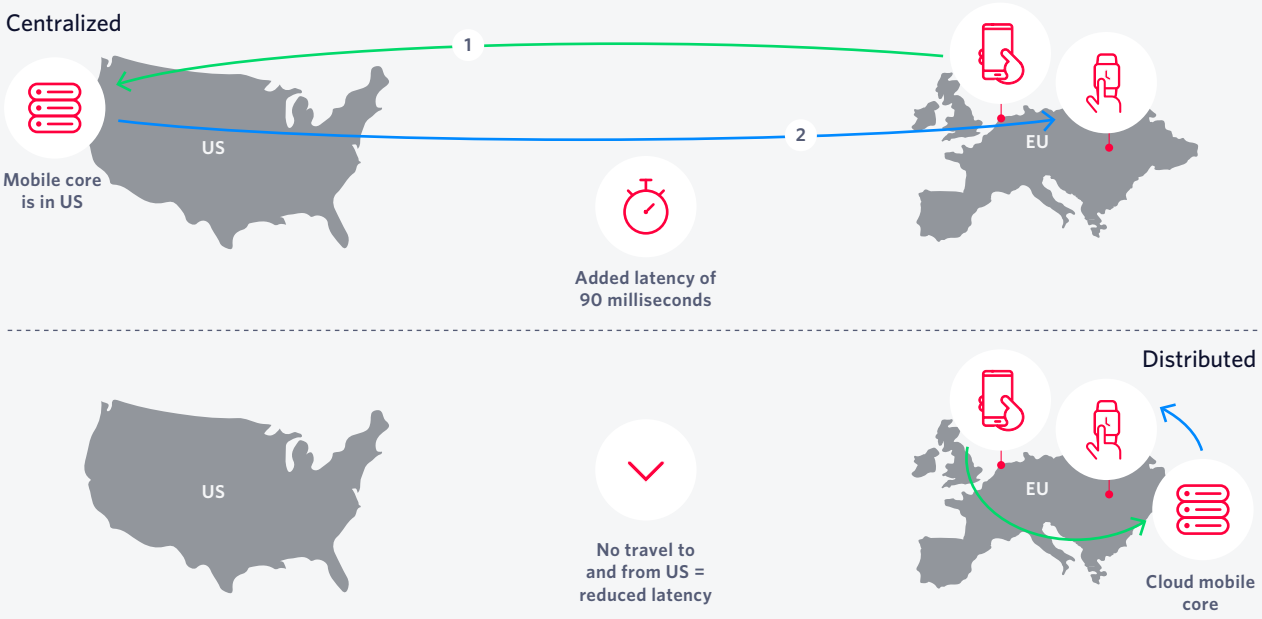
A third type is emerging: cloud software companies who build and run their own mobile cores, dedicated to IoT.

Traditional cellular carriers typically own their mobile cores. There are other vendors who own cores and either lease them to telecom providers or use them to enhance their own cellular offerings. Twilio is an example of that emerging 3rd category: a provider who owns a mobile core exclusively for IoT. Traffic in a carrier-owned mobile core typically routes to public or private IP networks via PGWs in the carrier's home country. That means traffic from an SGW in another country is routed inefficiently. This causes a big problem for IoT solutions: increased latency. Why? To answer this, it's important to understand what **Distributed IoT Mobile Cores** do differently.

What is a Distributed IoT Mobile Core?

A Distributed IoT Mobile Core is a virtual, cloud-based, pure-software mobile core that is architectured specifically for the needs of IoT devices, and deployed globally with regional internet breakouts. **If you have a cellular IoT solution deployed in multiple countries, then you're probably used to customizing device behavior based on the underlying network characteristics. With a Distributed IoT Mobile Core, you don't have to do that anymore.** This translates into lower operational overhead and a more seamless customer experience. IoT solutions demand performance and flexibility that traditional carrier mobile cores often cannot provide. Unlike mobile handsets and tablets, most IoT devices are autonomous and must be monitored and controlled by the connectivity provider. IoT devices intended for non-fixed use cases, such as the dockless scooters we discussed above, or devices deployed across several different countries or regions, must be able to attach to different cellular networks without human intervention. Let's say you have an IoT solution with connected devices all over the world. Suppose you're using a traditional carrier-owned core physically located in the US, and that core is serving an IoT device physically located in Germany. The round-trip latency would increase by 90 milliseconds. Now suppose that IoT device makes its way to Singapore; the roundtrip latency would increase by 245 milliseconds.This is a significant problem for mission-critical IoT solutions. Now imagine the same IoT solution, but in place of a US carrier, you use a Distributed IoT Mobile Core that is virtualized on a server in Germany and Singapore. The round-trip latency is greatly reduced. Suppose you had someone with a smart phone trying to call someone through a wearable device with voice calling enabled. Now consider a scenario where both devices are in Germany, but a centralized mobile core is in the United States. Figure 4 illustrates how a centralized versus a distributed mobile core orchestrating data impacts latency.

Figure 4: Distributed IoT Mobile Core vs Centralized Mobile Core



The key takeaway here is that **IoT deployments using a traditional carrier-provided mobile core cannot offer the flexibility needed for fleets of globally distributed IoT devices**. Besides latency, there are additional reasons why that is the case. Carriers primarily implement a mobile core to support voice, text messaging, and general-purpose data access for consumer access. They typically have a long "to-do" list of requested features from the carrier's customers for these types of usage, and must support a wide range of device types and technology generations. Consequently, they cannot always prioritize issues and enhancements that will benefit a specific user profile such as IoT. Not to mention, update cycles are infrequent at best.

Using a Multiple-IMSI approach for IoT

The benefits of using a Distributed IoT Mobile Core come primarily from the ability to optimize both device data latency and enable the use of multiple IMSIs in one device (known as "multi-IMSI solutions"). Multi-IMSI solutions allow the IoT devices to attach to different mobile networks as needed. This creates better device performance - often resulting in a better customer experience - while it minimizes configuration challenges when your devices are moved across country borders. **With Multi-IMSI, connected devices no longer have to be reconfigured as they traverse network boundaries from one operator to the next.**

Benefits of relying on a Distributed IoT Mobile Core

Mobile cores built for IoT provide several benefits to IoT product managers and developers.

Enhanced supply chain

With a Distributed IoT Mobile Core, developers can access better support with deeper visibility for the most efficient deployment of multi-IMSI solutions. Furthermore, they can remotely modify an IMSI by adding or removing networks. This is a huge value-add when you want to move an IoT device from one country to another.

Optimized performance and costs

As an IoT product manager, you can rely on a Distributed IoT Mobile Core to get the best out of costs and performance. You can choose networks that best suit your business model. For example, you can disallow an IMSI if it doesn't currently provide best performance or pricing. If performance is the priority, you can enable in-region internet traffic breakouts to provide the lowest possible latency for user data. This allows you to lower data latency for devices, even when deployed globally - all while providing consistent connectivity behavior.

Control

A Distributed IoT Mobile Core gives you control over the bandwidth and network resources. For example, by accessing regional internet breakout of data traffic, you're able to do things like guarantee your customers low latency, or constrain a customer's data traffic into specific regions for data privacy. This would be critical for your customers in Europe who may not want their traffic routed through the U.S. or Asia.

Flexibility

When you use a Distributed IoT Mobile Core, you can use SIMs with advanced features. For example, Twilio's Super SIM enables you to be carrier-agnostic across countries and regions. You can even isolate subscribers in case you need to manage and adapt your own fleet or make changes based on changes in the serving carrier networks - nationally or internationally.

Real-time analysis of device behavior

When your IoT solution is supported by a Distributed IoT Mobile Core, you can access custom traffic analysis. This includes everything from real-time analysis and tools that easily scale to large numbers of devices in geographically separate regions, to the analysis of the edge-to-edge behavior of individual devices. Additionally, you can easily manage situations where customer assets are stolen or hacked.

Scalability and workflow optimization

With a custom API that abstracts the network and turns your fleet of SIMs into a programmable software object, you can integrate fleet management into your existing workflows and significantly increase operational efficiency.

Continuous improvement

The key advantage of owning a cloud-based and pure-software mobile core is the ability to easily upgrade it and thus allow continuous innovation. For example, Twilio adds features every week to the mobile core and deploys new features right away. With a physical mobile core, software upgrades are much harder to accomplish - typical upgrade cycles for physical cores occur only twice a year. Twilio's mobile core deploys a new version of the PGW every day.

What about MVNOs?

Some IoT solution providers or enterprises with IoT projects in the field use mobile virtual network operators (MVNOs), instead of going directly with a carrier. However, these connections are especially at the mercy of carrier performance and feature limitations, because core update requests from MVNOs are deprioritized relative to changes the carrier itself wants or needs to make to support their voice, SMS, and general purpose data network customers.

In order to support multiple networks and international operation of user devices, those IoT solution providers or companies having IoT projects in the field today that use MVNO connectivity must secure and maintain agreements with multiple carriers in various countries and regions, and they must implement and maintain SIM delivery and management processes. What's worse, since each carrier has different technical implementations of their mobile cores, IoT device builders will need to accommodate these differences in their technical implementations, e.g. by leveraging different APIs. At best these requirements drive up support costs, and they can lead to delays in feature releases and updates because all carriers must complete the provider's requested changes before the provider can release any new feature updates. An MVNO-based IoT provider seeking to simplify their SIM delivery and management process might opt for a multi-IMSI SIM, but this is effectively impossible without a Distributed IoT Mobile Core, and latency quickly becomes an issue if that mobile core is not cloud-based and distributed.

Disaster and outage resiliency are another consideration. If an MVNO connectivity provider's static core is located in another country, and for some reason that core goes down or is unreachable from the device's location, IoT devices will be offline. By instantiating the core in a globally distributed and cloud-based manner, devices may still function if the network and core nearest them remains operational.

4 How IoT-only mobile cores power modern IoT solutions today

Rather than discuss the benefits of a Distributed IoT Mobile Core in the abstract, it's worth looking at several case studies that showcase how this alternative to carrier-owned or MVNO mobile cores benefit companies offering IoT solutions and their customers today. You'll meet a parent, inspired by the trauma of losing track of a child in an amusement park, who had a vision for a consumer wearable that would work around the world. You'll take a tour with a real estate developer that needed an easily-deployable access control and security solution for showing properties during the pandemic. And you'll take a drive with a vehicle telematics solution provider that turned to Twilio to help them bring IoT-based tracking and safety monitoring capabilities to their customer's rental car fleets.

CASE STUDY

Kiwip decreases latency of smart wearables for children

Nearly all parents have experienced at least one incident where they've lost track of a child. Whether it's in a crowded shopping mall, an amusement park, on a beach, or at a playground - children tend to wander off. This is especially true for parents of children with very curious minds, parents of special needs children with autism or other cognitive variances, or children who need to get themselves to and from school. After the founder of Kiwip lost track of his child inside Disneyland Paris, he began looking at the question of how to build a child-friendly smart wearable. He reasoned that giving children a trackable smartphone wasn't a viable solution, because children tend to misplace things, so he decided that a smart watch would be ideal.

Kiwip's child smartwatch had many design requirements. Just to name a few: it had to leverage reliable voice communications between the parent and child, offer location reporting and geo-fencing, ensure the ability to define points along a path, and generate alerts when the wearable passes those points. Their solution allows two-way voice communication so that a parent can use a phone to call the child through the watch.

For Kiwip to create the product they dreamed of, they needed an unparalleled connectivity platform that could handle the vast needs of a cellular connected wearable. The wearable had to work in several countries across Europe, Asia, and the Americas, without Kiwip needing to reconfigure the SIM for each device for each country. Furthermore, they required very low latency so that the quality of two-way voice was not disrupted by delays in traffic. This is where a multi-IMSI and a Distributed IoT Mobile Core approach matters most. With Multi-IMSI, connected devices no longer have to be reconfigured as they traverse network boundaries from one operator to the next. That multi-IMSI functionality can only be achieved by leveraging a Distributed IoT Mobile Core. As a result, Kiwip was able to achieve better device performance - and better customer experience - while minimizing configuration challenges when the wearables are moved across country borders. Without a multi-IMSI approach, Kiwip faced challenges to scale and profitize their business due to the cost of operations. Most importantly, the experience of using their product would suffer and likely result in poor customer satisfaction.

"Our customers are relieved to know that the kid's watch works anywhere in the world. Twilio makes that possible."

David Ughetto
Co-Founder and CTO
Kiwip

To meet these goals and needs, Kiwip leveraged Twilio's Super SIM, supported by Twilio's Distributed IoT Mobile Core. Twilio provided Kiwip with a well-supported and inexpensive global data connectivity solution with a multi-IMSI approach. This solution allowed Kiwip to scale as they moved from concept to deployment and global deployment. With one SIM that worked anywhere in the world, Kiwip didn't incur massive roaming charges when operating outside the family's home country. As a result, they are able to adjust the connectivity configuration of in-use devices, without human support. Best of all, their customers had a better experience with reduced latency for two-way voice calling.

CASE STUDY

SmartRent optimizes contactless access around the world

In early 2020 the rise of the COVID-19 pandemic, infections forced nearly every business to adapt quickly to shelter-in-place and social distancing protocols. In many cases, technology played a major role in those adaptations, and the real estate industry was no exception. Prior to the pandemic, walk-throughs with property managers and agents were de rigueur. In order to keep operating, property managers and agents needed to give prospective tenants a way to tour properties while maintaining social distancing.

In response to this need, SmartRent leveraged Twilio's Super SIM to build and rapidly deploy an IoT-based electronic access and monitoring solution. This IoT-powered service empowers property managers to continue working with prospective tenants by giving them the option to view properties on their own, and optionally provide a self-guided tour functionality, making safe real estate transactions possible even during a pandemic.

SmartRent's technology consists of traditional smart home technologies including sensors, cameras, and door locks communicating via a centralized wireless hub. The "hub" allows property owners and managers to monitor properties for issues, while also allowing selective access to properties. There was just one problem. The wireless hub needed to work out of the box, with simple installation. Cellular connectivity was clearly the technology of choice, but it had to work anywhere in the world.

By leveraging the Twilio Super SIM - powered by Twilio's Distributed IoT Mobile Core - SmartRent was able to easily deploy an IoT technology solution. Because their application was supported by a Distributed IoT Mobile Core, SmartRent was able to be carrier-agnostic across countries and regions. This functionality allows SmartRent to isolate subscribers when they need to manage and adapt their devices - nationally or internationally. Even during a global pandemic, property owners and managers were able to use this smart property management system while maintaining social distancing, without the need for on-site installation support.

"Since Super SIM leverages Twilio's Distributed IoT Mobile Core, it works seamlessly across the world. And we have been able to expand to new areas not only within a property itself but also to completely new geographic regions. Today we are operating our solution nationwide, with expansion efforts in Canada, Europe, and Asia."

Mitch Karren
Co-Founder and CPO
SmartRent

CASE STUDY

Telemax scales international fleet tracking solution

Vehicle telematics enable fleet managers to monitor vehicle safety and remotely diagnose problems, creating efficiencies in operation and reducing costs. Fleet managers want telematics, but in a highly competitive market they cannot afford to be debugging and resolving telecommunications issues in the telematics system – the solution must be "plug and play", highly reliable, and capable of working in all locations where cellular data connectivity is available. In short; a good telematics solution solves problems, and does not create different problems. Telemax, a provider of vehicle telematics systems for car rental and car-share companies in the Pacific region, leveraged Twilio's mobile core and Super SIM to enhance the value and efficiency of their solution.

Telemax wanted to remove the complexity of cellular connectivity for their rental car and care-sharing customers. Consequently, Telemax found themselves in uncharted territories as they navigated the cellular world. From pre-launch to fleet management, they needed to ensure they could adequately troubleshoot connectivity issues. They also needed to ensure connectivity – with optimal performance – for vehicles as they crossed country lines.

Twilio's IoT-focused mobile core provides Telemax visibility into the data usage of each deployed device, enabling them to track costs and predict financial impacts. It also helps Telemax understand how their devices are performing, and to troubleshoot issues quickly. This includes everything from including real-time analysis and tools that easily scale to large numbers of vehicles in geographically separate regions, to the analysis of the edge-to-edge behavior of individual devices. Finally, Telemax can easily manage situations where customer assets are stolen or hacked. In fact, this happened to Telemax at the start of the pandemic. A vehicle was stolen while it was not activated on the network. Thanks to the flexibility and visibility of Twilio's Distributed IoT Mobile Core, Telemax was able to locate and recover the stolen vehicle. Overall, their new business model was a massive hit with customers – and it wasn't long before Telemax earned almost 50 percent market share of the rental car and car-sharing market in the Pacific region.

"Twilio fueled a 10 percent growth in our monthly subscriber base by helping us create a differentiated fleet solution, which includes connectivity, and works anywhere in the world."

Ash Phayer
General Manager
Telemax

Conclusion

IoT is increasingly a part of our 21st century lives. Every time a fitness tracker, shared-mobility scooter, connected vehicle, or smart home device connects to your servers or accesses a cloud-based service, a complex dance among interwoven technologies unfolds, unseen, in just a few milliseconds. For IoT, the mobile core is the key component that can make or break your project. You should choose an IoT mobile core that gives you:

- Control over your connectivity
- Regional breakout of data traffic
- Carrier-agnostic flexibility across countries and regions
- Real-time analytics
- Scalability and workflow optimization
- Continuous Improvement

End users don't care about these details, they care only that the service works quickly and reliably. For IoT developers and product managers, every step of the IoT connectivity dance matters. The real action takes place inside the mobile core. Twilio's Distributed IoT Mobile Core is built for IoT. Contact Twilio today to obtain a test SIM and learn how we can help you take your solution all the way to the top.

Glossary

Telecommunications can be very technical and hard to grasp. This whitepaper mentions a lot of acronyms and some terms that might be new to you. Use this glossary to better understand the key terms.

Diameter
a protocol for authentication and authorization in a mobile network. "Diameter" evolved from the earlier "RADIUS" protocol.

Diameter Routing Agent (DRA)
manages routing and throttling of Diameter messages between MMEs and SGWs and other data nodes, and acts as a load balancer.

Distributed IoT Mobiles Cores
a mobile core that was created and is currently operated by a cellular IoT provider – exclusively for IoT. These mobile cores allow for lower operational overhead, more control over connectivity, and a more seamless customer experience. By being cloud based, the mobile core can occur anywhere in the world with multiple instances.

Domain Name Service (DNS)
converts human-readable web addresses into numerical addresses usable by network routers.

Home Public Land Mobile Network (HPLMN)
the "home network" for any given device in a mobile data network. If a mobile device is not in its home network, the visited network will contact the home network (via messages through the mobile core) to confirm that the device is authorized to access the network.

Home Subscriber Service (HSS)
generates an authentication vector (or challenge) using a private key stored in the device's SIM for SIM authentication, and assigns services to the device, based on the SIM having an entry in the HSS database of authorized (i.e. valid account) subscribers

International Mobile Subscriber Identity (IMSI)
a unique numeric code formed from combining the Mobile Country Code (e.g. the MCC for the United States is 31X – where X ranges from zero to six), the Mobile Network Code (e.g. the MNC for T-Mobile

is 260), and the International Mobile Subscriber Identity (IMSI) number which is a unique number assigned to a device SIM. In a sense, the IMSI is the unique "address" for any given mobile device.

IP Backbone
manages the path that data takes as it transits across different networks. In cases where data is exchanged between dissimilar networks (such as a voice call between two carriers using different air interface technologies, the data is converted into a common language (IP) before transiting across the IP Backbone. This includes the IP Exchange (IPX), GPRS Roaming Exchange (GRX), and CDMA Roaming Exchange. It also routes data between HPLMN and VPLMN networks, handles inter-operator peering across IP networks.

Mobile Core
a set of computing processes running on a server to operate the mobile network and subscriber devices. It's responsible for managing the interface between the base station radios sitting on towers, buildings, and poles, and other radio access networks, or between radio access networks and external networks.

Mobile Management Entity (MME)
interfaces with user equipment (such as the cellular modem in the ScooterCo example), chooses the Serving Gateway (SGW) and Packet Gateway (PGW), authenticates SIMs via the user's Home Subscriber Service, and enforces roaming restrictions.

Multiple-IMSI
allows IoT devices to attach to different mobile networks as needed, creating a better customer experience while also minimizing configuration challenges when your devices are moved to different countries or global regions.

Network Address Translation
conserves IP addresses by enabling private IP networks that use unregistered IP addresses to connect to the Internet.

Packet Data Network Gateway (PGW)
manages connectivity between the device to external packet data networks, enforces policies, filters packets, and assigns IP addresses and DNS servers.

Serving Gateway (SGW)
routes/forwards user data, deactivates idle data paths, pages the user equipment when downlink data is queued for downlink, and replicates data as needed for law enforcement interception.

Subscriber Identity Module (SIM)
a physical or virtual card inside a mobile device or IoT device carrying an identification number unique to the owner.

Visited Public Land Mobile Network (VPLMN)
communicates with the HPLMN via the mobile core – so the performance of the mobile core has a major impact on efficiency of the system when devices are not in their home network.

Thanks for reading

Want more resources on choosing and IoT connectivity provider?

Get more resources

Twilio powers the future of business communications, enabling phones, VoIP, and messaging to be embedded into web, desktop, and mobile software. We take care of the messy telecom hardware and expose a globally available cloud API that developers can interact with to build intelligent and complex communications systems.