Binding Networks & Connecting Services

Business Critical Connectivity

NEVER LOSE A PAYMENT

ALWAYS STAY CONNECTED

A Guide to Point of Sale Connectivity

Caburn Telecom
Part of the CSL Group

caburntelecom.com
+44 1257 543917

A GUIDE TO POINT OF SALE CONNECTIVITY

ALWAYS STAY CONNECTED


Caburn
Telecom
Part of the CSL Group

CONTENTS

DEFINITIONS

What are the differences between Point of Sale (PoS), EPoS, MPoS and SoftPOS Systems?

Point of Sale (POS) payment terminals and systems are commonly used devices in retail and hospitality for authorising and charging for electronic payments. They are used in mobile, fixed, attended, stand-alone or unattended environments. Often commercialised for a range of sectors and industrialised for vending machines, ticket machines and self-service.

Some **Electronic Point of Sale (EPoS)** systems are connected to electronic cash registers (ECR) or sophisticated business management systems. EPoS systems can enable the complete running of the retail transaction process/system and be configured in a variety of forms or levels of sophistication. This can include secure cloud-based systems for extra services such as inventory management or real-time marketing.

To enable **authorisation, billing and data feeds/ configuration**, most forms of POS and EPoS systems are connected either directly or indirectly to a communications network. For example, this can be ubiquitous systems such as mobile networks including 2G/3G/4G/5G (using extra layers of security). While stationary or fixed-position payment terminals often rely of wired networks such as DSL, PSTN, TCP/IP or X.25, they also often utilise secure mobile as a back-up communication method (Fagerberg, 2021). Secure mobile is also often used as the primary communication method for fixed devices, as it removes the need and inconvenience of network cabling or the fallibility of a single landline connection (ibid).

Handheld POS terminals also often rely on short-range wireless connectivity solutions such as Wi-Fi or Bluetooth. Increasingly they incorporate mobile GSM to benefit from independence from unique site contexts or unsecure local networks and to provide maximum range flexibility (ibid).

Mobile Point of Sale Systems (mPoS) tend to be smaller and more portable devices that via a mobile app allow a smart phone or tablet to become a payment acceptance system and register. These are particularly popular will small business owners or those who are highly mobile and visiting clients in a range of locations.

SoftPOS systems are where a phone or tablet can be converted through a secure app to become a highly flexible mPoS terminal. The phone or tablet, however, must have Near Field Communication (NFC) functionality in-built, to permit user/issuers cards to be tapped directly on the phone/tablet. This removes the need for an intermediary bespoke MPoS device, which can help to reduce third-party integration problems. Some view this as a long-term replacement to some forms of mPoS devices and in certain types of use cases.

It is important to remember that for security and privacy, **NFC communications** are used for the communication between the issuer card and the accepting device in contactless settings. This means that communications are limited to a few centimetres and restricts the possibility of mis-payment.

MARKET BACKGROUND & TRENDS

What are the Reasons for the Rapid Adoption of EPoS and mPoS Systems?

Contactless payments systems supply a convenient and trusted transaction medium for consumers in a complete range of settings. This is critical to their use as perceived usefulness and trust significantly influence a customer's intention to use, particularly where biometrics are an authentication method for payment (Sulaiman & Almunawar, 2021).

Tapping a card or a contactless smartphone payment application clearly can provide high levels of convenience for consumers, users, retailers, and service providers. Their adoption was also accelerated, however, by widely held fears of virus transmission during the COVID-19 pandemic via touching shared surfaces (Fagerberg, 2021). Tap and go payment terminals replacing normalised PIN entry also due to feelings of increased security and privacy, providing a 'cleaner' and more personal, 'seamless' service process; therefore, positively informing consumer's affective responses to the buying experience (Oloveze, et al., 2021). Trust and convenience are, therefore, paramount for both consumers and retailers who rely on these systems for their primary physical customer point of contact.

As a result, contactless payments are easily now the primary method of completing face to face or unattended transactions for goods, shopping, personal services or travel experiences. To facilitate this rapid demand, 80 million EPoS terminal units were shipped in 2020 and deliveries are expected to grow to 127 million units by 2025 (Fagerberg, 2021). Retail, Transportation and Hospitality applications are tending to lead growth and also influence the trajectory of new features (Grand View Research, 2022). According to Berg Insight, around 47% of terminals are now being shipped with wireless connectivity in-built, and this is likely to grow moving forward as more devices need extra security, resilience and the extra convenience of untethered mobility (Fagerberg, 2021).

Contactless and smart payment systems also create opportunities for creating new and disruptive service processes. As an example, in transportation, new ways of transacting customer journeys and their payment for them become possible. Tapping-in and out for time or distance-based services such as transport or logistics services become more painless, intuitive, and inherently flexible. Especially compared to pre-purchase highly cognitive consumer processing systems, which by their nature and complexity typically result in the formation of unnecessary and irritating queues. For example, an inconvenience which became normalised in ticketing and parking payment machines at the busiest locations or times of day.

EPoS systems also generate valuable location and time-based business data, which enables organisations to develop data analytics and processing systems to help optimise their business (Marques, et al., 2022). Creating valuable market intelligence and reliable, timely information for warning, analysing and predicting inventory flows, user flows and changing demands, with new layers of financial, spatial and temporal meaning (ibid).

It is also worth noting that many retailers place such a high value on convenient and seamless service delivery, that they will sometimes accept low-level payments off-line if authorisation channels become unavailable. This is to keep customer transactions flowing but are ultimately at the merchant's own financial risk. Of course, transactions are cached and then communicated with their Merchant Services and authorised with the bank/issuer as soon as the service is resumed.

SYSTEM DESIGN

How do Point of Sale (POS)Terminals Attain a Seamless and Reliable Service?

A convenient, trusted, seamless and frustration-free service, requires a fully integrated system. EPoS devices are manufactured by large OEM manufacturers for a variety of clients, with the aim of configuration changes being relatively low-level and (where possible) completed post manufacture. The firmware logic that manages and controls the hardware will also manage their payment communications. This is more fundamental to the correct functioning of the device in use, than, for example, superficial or cosmetic user or merchant configuration changes such as threshold parameters or display branding.

System design is, therefore, key to creating a robust solution. How hardware is selected, and the level of due diligence paid towards the operation of firmware in a range of scenarios can make the difference between an unreliable system and one that is fully considered, secure and resilient in providing a complete end-to-end service.

In distributed systems, communications, secure protocols, API and end-to-end device encryption are clearly fundamental to a robust service. Methods of communication and their understanding of, however, can sometimes be assumed to be out of a service provider's control. This can be a miscalculation, however, as the construction or utilisation of available and alternative forms of local and wide-area communications are determinable with transparent and flexible partners. It can mean the difference between focussing on device hardware failures and ignoring more systemic problems such as poorly planned infrastructure or communications systems. This can be by virtue of their perceived unexplainability or difficulty in providing metrics and some level of quantifiability.

This diligence is fundamental to business-critical mobile communications services and are crucial in successfully delivering business and financial critical communications systems. Only by taking an integrated, end to end approach involving device manufacturers and communications experts can payment devices be designed and configured to provide the highest levels of up-time, thus reducing dissatisfaction and financial risk for retailers, merchants and service providers.

NETWORK QUALITY

What Roles do IoT SIM Cards Play?

'Contactless payments' rightly imply wireless communications are central to the payment process. This is via a variety of mechanisms.

For example, the communication between the payment card, smart phone and device uses NFC wireless communications in very close proximity to each other.

The handheld or static EPoS device or system, however, then needs to communicate upstream via fixed-line or wireless comms.

Micro-business users may use a connected personal mobile phone and merchant approved app for these purposes, utilising their phone providers consumer SIM card or a local Wi-Fi connection which they manage.

Larger applications, however, will require a centrally managed, secure IoT SIM card, secure IT services which are managed on-premises [including Wi-Fi], and/or a securely managed fixed broadband connection.

For **bigger organisations** and **payment service providers**, Wi-Fi connectivity needs to provide a secure, manageable and predictable connection across a broad range of sites (including third-party sites). If these are not correctly set up, a simple local configuration change could easily render payment devices unable to authenticate/bill or be open to malicious/fraudulent interception.

Positioning of Wi-Fi routers also needs to cover all required transaction spots in the building. This can be more of a problem for providers who lack the IT skills or who don't control the premises in their entirety.

For these reasons, payment service providers are now using IoT SIM Cards as the primary or secondary forms of communications for many of their Point-of-Sale Devices. This is not only within the payment devices themselves, but increasingly as the back-haul mechanism for Wi-Fi routers. These technologies help to overcome range problems where payment terminals are taken to the consumer's point of consumption.

Intelligent, SIM card enabled payment terminals are thus able to communicate whether the device is in range of Wi-Fi or not. It also means if there is a hardware or configuration problem with the **Local Wi-Fi router**, then the payment device can still communicate securely over its multi-network mobile connection.

This provides the best of both worlds in terms of reach, but also provides multiple forms of communication resilience. Enabling portable and static POS devices and systems to secure their critical connectivity and eliminate single points of failure across their geographical deployments and site contexts.

For simplicity and resilience of deployment, most payment service providers use pre-installed IoT SIM Cards in their devices. Relying on secure multi-network mobile connectivity and the geo-resilience that it provides, together with maximum service up-time, flexibility and safeguarding measures.


Caburn
Telecom

DEVICE COMMUNICATIONS

How do Multi-Network IoT SIM Cards Help Payment Systems Work More Securely and Reliably?

Multi-Network systems enable devices to communicate using any of the locally available mobile radio mast access networks. For example, in the UK, this would mean EE, Vodafone, O2 and 3; or a subset of these depending upon price and availability. This provides maximum geographic flexibility for national deployments and the ability to communicate using whichever local radio network is the strongest or most available in terms of data throughput. Normal consumer SIMs do not allow this and are fixed to one provider. This means that if a signal from a network provider is poor in a location or attenuated due to building conditions, or is suffering a local or national outage, then a point of sale device loaded with an IoT SIM card can hop to another network.

To work reliably, however, it is important to select payment devices that can intelligently select the most appropriate network for their needed type of communications and the forms of network systems available.

Payment devices are manufactured with integrated modems, which support a variety of GSM radio frequencies and protocols for certain types of mobile communications. If, for example, the device modem only supports 4G LTE communications and not 2G or 3G, but the strongest signal available is a 2G one, then if the payment device (as many are) is only configured in firmware to select the strongest signal (dBm), it could mean the point-of-sale device selecting the 2G [very low or no data] network, when a slightly lower strength 4G signal but much higher data-bandwidth one is available. It is not unknown for devices to hang onto these 2G networks as devices will usually only switch if the 2G network signal strength (dBm) drops below a certain preconfigured signal (not data) threshold. This can be particularly catastrophic as the device may never have cause to try another network and is unable to communicate as a result when needed.

It is important, therfore, (for multi-network SIM cards to work effectively), that manufacturers and payment service providers configure their network selection processes in consultation with IoT SIM card providers and experts.

MULTI-NETWORK SIM CARDS

Dual-SIM Options

Multi-network IoT SIM cards deliver significant resilience and performance benefits over single-network SIM cards when used in EPoS payment systems. Dual discrete-pathway multi-network IoT SIM cards, however, can also be selected and integrated as an even more resilient option.

Multi-network SIM cards provide access to all radio access mobile networks locally available. The signalling pathways for all traffic over these networks must, however, be authorised by a single IoT roaming agreement provider using their core infrastructure and Home Location Register (HLR). The highest quality systems are designed for high resilience, geo redundancy and are supported by sophisticated Network Operation Centres (NOC). Even the highest quality systems, however, can sometimes suffer temporary outages or suffer service degradation during pre-warned maintenance windows. If the core systems are interrupted for some reason (although rare), then data sessions cannot be authorised. Two SIM cards by two different and discrete IoT core infrastructure roaming providers, therefore, offers the potential for complete end to end and temporal resilience as it is highly unlikely that both network roaming provider's core infrastructure would degrade at exactly the same time.

For the absolute maximum possible theoretical levels of resilience, two IoT Multi-Network SIM cards can be used as the primary/back up, independently or in conjunction with Wi-Fi or wired LAN communications. This, however, requires intelligent dual SIM support in the payment terminal hardware (i.e., intelligent dual SIM selection capability to be implemented within the payment device's hardware and firmware). It can also sometimes be helpful to enable the selection of preferred switching or cost loading parameters. For example, implementing a Dual SIM approach means the hardware and firmware of the device must support and manage the utilisation of both SIM cards. In some cases, two SIM slots may be supported in the hardware, but this does not mean that the device manufacturer has implemented the firmware to support both. They may not have also implemented software that intelligently manages switching between the two SIM cards based during normal use and every-day real life scenarios. Switching SIM cards unnecessarily, could create problems. For example, during a successful transaction. If one of the selected cost plans is more expensive. It might be preferred that the device reverts to the lower cost SIM card plan when in normal use.

Control of or influencing the hardware and firmware design of devices becomes imperative for both security and resilience. It is important for the payment device to not only make informed decisions in-session and between sessions, but also to ensure that the device is monitoring and selecting networks in-between transactions or during device down-times to ensure that the device is connected and ready for use as soon as it is needed. Any significant attenuation or loss of a particular network would therefore be dealt with proactively and in advance of the service for the consumer and the retailer being interrupted. For example, implementing heartbeats can mean that any significant network problems can be dealt with proactively, but also based upon the surety of an appropriate number of retries before SIM switching. Having a sophisticated implementation also means that the data plans for each SIM card become more predictable.

Where a dual SIM hardware/firmware option does exist, it is important, therefore, to test the functionality based upon a number of live-use scenarios. As a guide, switching core networks can take anything from 15 seconds to well over a minute. It is, therefore, best to only switch SIM slots under known and controlled circumstances, i.e., when a catastrophic connection failure is detected and verified by the device.

MORE INFORMATION ON IoT SIM CARDS & CONNECTIVITY

WHAT IS IoT?

Further Information on IoT, IoT Connectivity and IoT SIM Cards.

What is IoT?

IoT is an acronym widely used for describing the Internet of Things. Typically for a vast range of devices viewed as inanimate objects designed to serve a particular function or use. IoT devices, by their nature, tend to be geographically dispersed and installed at scale. Therefore, to perform effectively, they require some level of device intelligence, resilience, secure and legitimate connectivity, and the capability to be remotely managed.

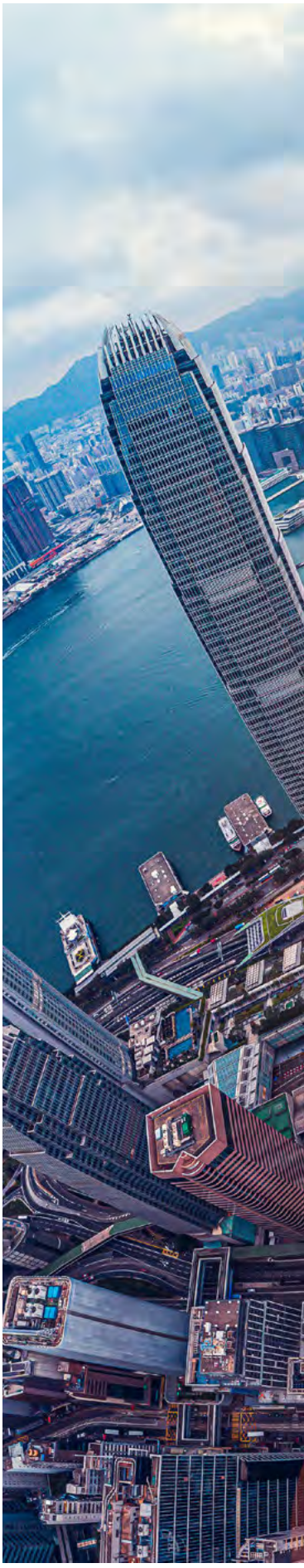
What is IoT Connectivity?

IoT devices can offer a range of valuable public and commercial services for business and users but require secure and resilient connectivity to operate beneficially and profitably. IoT Connectivity can take a range of forms, but due to the benefits of portability, flexibility, and ubiquity, predominately use wireless systems. This most typically involves use of the mobile GSM infrastructure.

What is an IoT SIM Card?

An IoT SIM Card is a SIM card designed to be installed in a range of IoT Devices. The SIM Card supplies the secure authentication for the IoT device to connect correctly to mobile networks. Ensuring the signalling and traffic is routed securely and reliably via the correct system checkpoints and network-nodes. These SIM identifiers are also used for extra network features such as Virtual Private Networks (VPN) and for setting and blocking certain features. SIM provisioning codes ensure billing is correctly apportioned to each radio and routing network, the originating user devices and the various service providers.

Typical use cases for IoT SIM cards include vehicle telematics, insurance, tracking, road signage, traffic management, environmental monitoring, smart building access, payment terminals, ticket and vending machines, smart meters, electric vehicle charging devices, remote routers, CCTV, incident dashboard cameras. lone worker protection systems, digital advertising, and elderly telecare and fall detection devices.



IoT SIM CARD CONNECTIVITY

How do IoT SIM Cards Differ from Ordinary Consumer SIMs?

IoT SIM cards differ from ordinary consumer SIM cards as IoT SIM Cards are explicitly designed for industrial and business IoT applications. IoT SIM Cards being securely coded at manufacture and then provisioned by the IoT Mobile Virtual Network Operator (MVNO) for an assorted range of approved IoT applications.

IoT SIM cards provide legitimate access and network traffic for IoT devices for which they critically depend, both day to day and for their longevity. This is available due to commercial agreements between mobile network operators (MNOs), IoT Virtual Mobile Network Operators and infrastructure providers who authorise and enable their use and connection within specified IoT use cases. This is important as each typically involves several expected working parameters including, signalling frequency (used for authorisation purposes and not usually charged for), data payload sizes (chargeable) and any voice or SMS traffic (chargeable). If devices produce too much signalling and insufficient revenue for mobile network operators and are not authorised via commercial agreements, then they can be switched off.

IoT SIM cards are also manufactured in a range of form factors and chipsets to suit a variety of IoT devices. This can include a variety of sizes and embedded chips that are designed for more miniature or environmentally challenging environments such as high levels of motion or vibration.

IoT SIMs are critically demarcated from ordinary consumer/tourist roaming SIM cards used in mobile phones via the types of agreements. In the consumer roaming profile, the host MNO expects the SIM to visit their mobile network but leave after an expected and reasonable time-period. While IoT devices also roam into other countries periodically (especially in transport use cases), they are often deployed there permanently, or based upon their usage become static there. Staying permanently on a particular MNOs radio network is problematic if it is not their native SIM card and is not an approved IoT SIM Card. For their continued long-term connection, it is therefore crucial that they are identified as an authorised IoT device and remain protected by legitimate commercial IoT device agreements with those host mobile network operators who are vital for providing the radio and base station switching networks. Most MNOs welcome authorised IoT agreements with credible and trustworthy IoT MVNOs as they provide reciprocal forms of revenue streams without the headache of excessive or unconstrained signalling which can significantly degrade general network performance.

IoT SIM cards also need remote management capability as they cannot be locally managed by their user/owners or retail outlets as is the case with Mobile Phones. IoT SIMs, therefore require configuration changes to be made remotely and securely, their costs to be continuously monitored and controlled independently of the Mobile Network Operator's systems.


Caburn
Telecom

MULTI-NETWORK IoT SYSTEMS

Why use Multi-Network Connectivity for IoT Devices?

Most IoT devices use multi-network systems. This means that IoT SIMs can connect to any radio network within a particular country. Motivations for using multi-network connectivity are typically;

i) to enlarge geographical coverage,

ii) increase service up-time,

iii) ensure resilient and cost-effective cross-border roaming,

iv) avoid local, regional, national or international service outages on a single network,

v) enable management of connectivity beyond the retail services major individual networks provide (whose limited support is geared towards consumer mobile users or the very-largest corporate accounts),

vi) manage medium to large scale SIM deployments and assets.

Multi-network systems provide substantial benefits for IoT service providers, provided they are carefully managed. Consumer mobile phones typically remain connected to one network due to the competitive nature of that use case. By employing commercial IoT roaming agreements and investing in interfacing systems and technologies, however, IoT Mobile Virtual Network Operators (MVNO's) can deliver multi-network capability for IoT devices. Allowing them to connect to the most favourable network based upon their local, physical, geographical, or temporal circumstances. Using the existing GSM mobile network infrastructure in this way, therefore underpins most public and commercial IoT services. Providing the ubiquitous access needed and the ability to legitimately authenticate devices on the various mobile networks and their visitor location registers.

A managed IoT SIM with robust connectivity plans will, therefore, enable its associated IoT device to connect to multiple networks, supplying resilience, flexibility, and service performance. As IoT devices are released and move or travel, the ability to connect to the widest variety of mobile networks in a region or across borders, ensures services are not interrupted, while avoiding unexpected out of zone penalties. In mobile environments, such multi-network capability helps increase overall capacity and improves data rates (Zhang, et al., 2018).

It is also key that IoT SIM cards are supported by a SIM Management Platform together with a flexible approach and the ability to change tariffs and suspend SIMs. IoT devices cycle through various lifecycles which to be cost effective require that the connectivity and associated costs be switched off during these downtimes.

GEOGRAPHICAL COVERAGE

Single Network Coverage Claims?

Each individual network's extent of mobile radio coverage is contentious (Fida & Marina, 2018).

Coverage maps are usually provided by Mobile Network Operators (MNO's) themselves (Jarvis, et al., 2018) or via crowdsourcing mechanisms (Marina, et al., 2015).

Coverage can be patchy, however, and newer technologies are usually deployed based upon likely returns on investment or economic factors. Meaning rural or poorer areas are usually less well served (Koutroumpis & Leiponen, 2016; Perlman & Wechsler, 2019). Service voids remain and local availability of 2G, 3G, 4G and 5G operational infrastructures vary (Alay, et al., 2020). Indeed, coverage maps tend not to objectively reflect the operational experience of users (Jarvis, et al., 2018).

This is particularly important for national deployments which may require service ubiquity and high coverage. Indeed, cities are not exempt. Buildings and indoor locations can attenuate networks which means an alternative mobile network is needed. High general usage can also reduce performance of an individual network, which means alternatives need to be available.

Crowdsourcing data conflates indoor and outdoor measurements and does not reflect device characteristics, handling or limitations (Marina, et al., 2015). Confusing the significant effects that buildings and structures have on reducing signal strength (ibid). Similarly, the impact of attenuation, poor weather, radio-shadows, operational voids, weak-signals and temporal variations tend not to be considered (Fida & Marina, 2018).

Device connectivity also depends upon a dynamic range of local and core-network system interactions, which affect performance and service levels (Alay, et al., 2020).

For these reasons, and due to the nature and complexity of mobile networks, it is recommended that actual user experiences (client-assisted-data) forms part of the measurements (Sen, et al., 2011). Being continuously checked to factor in environmental, temporal, and contextual changes (ibid).

These practical problems mean experienced IoT service providers typically extend geographical and temporal service levels via a multi-network approach. In the consumer and business markets, the main mobile network operators are competing, making neutral cross-relationships unworkable. Multi-network providers such as Caburn Telecom, however, work to deliver a structure that allows devices to select and communicate with the best network available. This is achieved by producing a SIM that is accepted by each of the MNOs via long-term agreements. A high-quality multi-network provider ensures these roaming agreements reflect the type of devices and their expected connectivity profiles. For example, while early M2M devices and their traffic tended to involve small data packets, increasingly devices require human interaction or supply some level of service experience for the user. Beit voice quality, latency, speed of service, privacy, or security. Increasingly, much broader use applications recognise the benefits of multi-network connectivity and look to integrate them into wider service offerings. Mission critical services for vehicle telematics, insurance, lone-workers, tele-health, telecare, assisted-living, epos terminals, hot-spots, routers, personal security devices, CCTV, bodycams, asset security and management systems all rely on multi-network connectivity.

In these sorts of user and device interactions, it is important to consider not only quality of service, but also quality of experience (Alay, et al., 2020) as well as providing real-time monitoring and warning systems.

FLEXIBLE & SCALABLE CONNECTIVITY

Mobile Systems and Device Interrelationships

Mobile systems are convoluted and when combined form complex ecosystems (Alay, et al., 2020). Ubiquitous access depends not only upon the specialised SIM variant, but also the devices compatibility with; the various radio frequencies and the variety of network evolutions supported by each network (Fida & Marina, 2018). For example, approved modems, the access technologies available and each network provider(s) regional and national implementation and disposal of 2G, 3G, 4G and 5G infrastructure (Alay, et al., 2020).

Multi-network characteristics of devices are also affected by the capabilities of the IoT device itself (Fida & Marina, 2018). Vast arrays of devices have different levels of network intelligence or selection logic. Some are battery powered and others connected to the mains supply. Remaining connected to the network, or the need to close connections in sleep and hibernation modes to conserve battery life will therefore vary by circumstance. Some will have simple network selection algorithms based upon signal strength, while others will have more astute selection procedures. For example, the firmware can be designed to select networks manually or automatically. More intelligent devices can use network evaluation steps/algorithms for selecting the best network to connect with. While the most primitive devices will select based upon strongest signal only, irrespective of bandwidth or services available, others can select based upon the availability of the required services, unique communication requirements, or will ping certain data services to first measure end-to-end data connectivity. For instance, selecting network based simply on signal strength may mean that a 2G or 3G network is selected, when a slightly lower strength 4G one is available. This may not matter for those applications requiring a simple voice connection, but for those needing data only, it can severely affect service or performance.

This device capability is important as devices may need to intelligently select or switch networks in certain circumstances. i.e.;

i) If the local strongest measured signal by the device is 2G, but data connectivity is required.

ii) One of the MNO's suffers core network issues, which to the device appears that a network is available when end to end connectivity on that network is not possible.

iii) Other contextual or temporal factors meaning the loss of a radio connection or time-outs, which the device will need to have processes in place to manage. Network selection criteria becomes especially important when there is congestion on one of the networks, or an outage.

This is crucial as a catastrophic failure on an individual MNO core-network could result in hours of down-time on that network, while investigation, rectification and recovery works are implemented. This can sometimes involve load balancing and management of traffic congestion through points of failure or constriction. The ability to select another network in this scenario is invaluable. Eliminating such periods, where none of the population of IoT devices can communicate for an extended period.

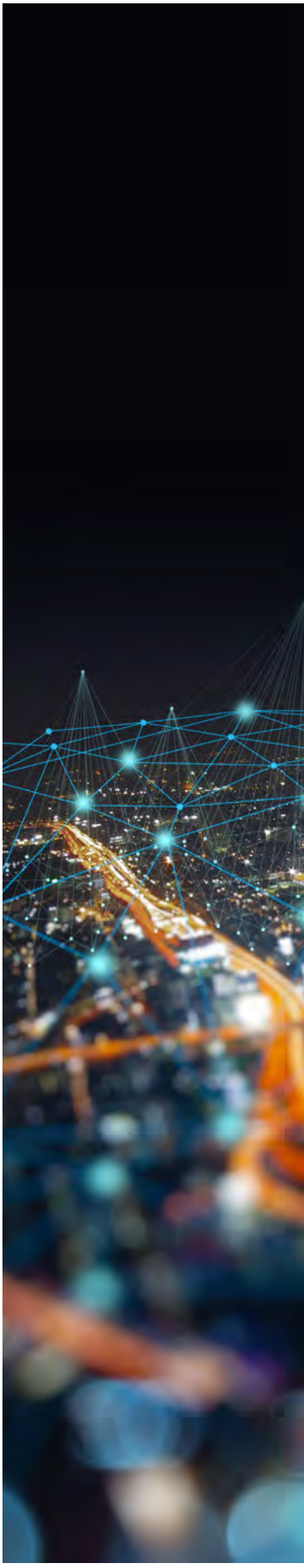
SELECTING THE RIGHT CONNECTIVITY PARTNER

What Roles do IoT MVNO's and IoT SIM Providers Play in the Sector?

Selecting the right connectivity and SIM partner is critical, not only in helping choose, configure, and optimise device's connectivity with the necessary long-term commercial agreements, but also to provide real time advice and support should any of the MNO's networks or devices suffer issues. Indeed, some compatibility issues may require more involved investigations. This is where a partner with high levels of telecom network expertise and resourced support structures is invaluable. Close relationships with our customers and partners also ensure that providers such as Caburn Telecom constantly monitors and tests networks; often advising MNO problems to our clients in advance of the networks detecting problems themselves. Caburn Telecom's large client network also helps us to continuously monitor service levels and user experiences. Forming a responsive and far-reaching mobile ecosystem (Sen, et al., 2011) for establishing high levels of quality of service and user experiences.

The right connectivity partner can also help future-proof roll outs. This is achieved by advising in good time of network features, upgrades, or sunsets. Safeguarding technologies which match the desired evolution and lifespan of devices is important, as the costs of a retrofit of dispersed devices is viewed as a failure of foresight.

A high-quality connectivity partner also ensures communication plans and agreements match use cases. MNO's dislike their networks being infiltrated by undisclosed M2M / IoT device signalling and closely monitor these situations. Spotting SIM profiles not in-line with their connectivity plans and pre-agreed commercial arrangements, means they may unilaterally apply extra surcharges for those groups of devices, or permanently block those ranges of SIM's. A high-quality provider, therefore, also invests in optimising and upgrading their networks and works closely with MNOs to create strong, mutually beneficial relationships.



ABOUT CABURN TELECOM

Technical Implementation

Caburn Telecom are a leading global provider of connectivity for Internet-of-Things (IoT) devices. Our focus being the development of advanced mobile connectivity solutions and associated management systems. Our SIMs, chip-SIMs and eSIMs, provide the flexibility and high service levels vital for distributed IoT devices to operate effectively. We provide multi-network capability together with the streamlined management of SIM populations. Our secure client portals deliver easy to use interfaces for understanding and administering the connectivity of devices. Traffic details and actual (and predicted) costs can be viewed at the group(s) and the individual level. Our innovative and flexible connectivity packages allow IoT service providers to maximise their assets and manage the operational life cycles of devices.

Caburn Telecom technical implementation focusses on delivering important IoT features such as connectivity management, SIM provisioning and administration, cost control features, regulation of SMS services, VPN (Virtual Private Network), secure data storage, dash-boarding and detailed traffic records. The Caburn Connect brand can also provide important user features such as voice control, allocation, and management of local telephone numbers, and dynamic 'approved telephone number lists', which are important security features for lone worker, telehealth, and telecare sectors. We also provide a high level of dedicated support. This is critical as multi-network systems are more complex than single network offerings, requiring interfaces between a variety of operators and systems. If professionally managed, they deliver the obvious benefits for users and services.

Caburn Telecom Provide:

i) IoT SIM Cards.

ii) Connectivity and SIM management platform/portals.

iii) The SMS administration and delivery management service.

iv) Network status sites.

v) Client/subscriber user access and interfaces.

vi) Client API (Application Programming Interfaces) for automated control of connectivity and secure VPN.

The management platforms involve; a) the aggregation of multiple sources of network data into a logical, organised and manageable structure for clients; b) the selective presentation of data and management information into easy to understand web interfaces; c) the availability of live and historical tables and histogram charts; d) the provision of secure user types and their administration; e) contact management; and f) the ability to automatically communicate incidents by email or SMS to appropriate stakeholders or by posting on the status site.

CABURN GROUP OVERVIEW

Binding Networks And Connecting Services

Caburn Telecom is a leading, global provider of IoT and M2M mobile connectivity services. Providing you with the ability to remotely and securely manage device connectivity and the necessary, associated large SIM populations. We have coverage in more than 190 countries and offer flexible approaches to IoT deployments. Our extensive SIM management platform gives you complete visibility and control of your network usage, while our teams excel at providing you with dedicated operational support.

Caburn Technologies provides similar services to our Telecom division, but with a specific focus towards the USA, Canada, and Mexico. Delivering securitised and localised IoT connectivity and highly scalable services which recognise the unique communications infrastructure, diversity, and geographical reach of these important regions.

Our **Caburn Connect** services provide the mission-critical surety of those IoT services seeking to protect or preserve life. For example, the emergency services, building alarms, telecare for the elderly, vulnerable lone-workers and employees, health, well-being & assisted-living applications. These types of services require resilient multi-network voice services, real-time traffic monitoring/testing and extra service features.

Caburn Solutions focus on the development of ground-breaking connectivity services, managed gateways, sensors, and associated platforms. We develop, incubate, and deliver innovative/specialised IoT solutions. Integrating our own and a range of our partner's technologies for the environmental, building, home and health, well-being, and personal monitoring sectors.

The Caburn Ethos

Across our businesses, we provide a highly customer referenceable service. Our satisfied customers include some of the largest and most demanding businesses across the IoT/M2M sector and due to the expertise of our technical service and support teams we have built a reputation for reliability and proactivity.

Our business ethos and quality of our support team members means that we are also able to support our customers in the connectivity plans and services.

Our Focus is the development of advanced mobile connectivity solutions and associated management systems, facilitating optimised cost-control and operational scale.

Our SIMs, chip-SIMs and eSIMs, provide the flexibility and high-service levels vital for distributed IoT devices to operate effectively. We provide multi-network capability while our secure client portals deliver easy-to-use interfaces, empowering our customers to understand and administer the connectivity of their devices themselves.

REFERENCES

Alay, O., A. Lutu, R. G. & Peon-Quir, M., 2020. MONROE: Measuring Mobile Broadband Networks in Europe. s.l.:Simula Research Laboratory, IMDEA Networks, Celerway Communications, Karlstad University, Politecnico di Torino, Nextworks, Telenor Research.

Fagerberg, J., 2021. POS Terminals and Wireless M2M - Fifth Edition, s.l.: Berg Insight.

Fida, M. & Marina, M. K., 2018. Impact of Device Diversity on Crowdsourced Mobile Coverage Maps. Rome, 14th Grand View Research, 2022. Contactless Payment Market Size & Share Report, 2021-2028. [Online] Available at: https://www.grandviewresearch.com/industry-analysis/contactless-payments-market

International Conference on Network and Service Management (CNSM), pp. 348-352.

Jarvis, C., Midoglu, C., Lutu, A. & Alay, O., 2018. Visualizing Mobile Coverage from Repetitive Measurements on Defined Trajectories. Vienna, 2018 Network Traffic Measurement and Analysis Conference (TMA), pp. 1-6.

Koutroumpis, P. & Leiponen, A., 2016. Crowdsourcing mobile coverage. Telecommunications Policy, 40(6), pp. 532-544.

Marina, M., Radu, V. & Balampekos, K., 2015. Impact of indoor-outdoor context on crowdsourcing based mobile coverage analysis. s.l., Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges, pp. 45-50.

Marques, C., Guedes, A. & Bento, R., 2022. Tracking changes in tourism demand with point-of-sale data: The case of Portugal. Tourism and Hospitality Research, p. 14673584221075175.

Oloveze, A., Oteh, O., Nwosu, H. & Obasi, R., 2021. How user behaviour is moderated by affective commitment on point of sale terminal. Rajagiri Management Journal.

Perlman, L. & Wechsler, M., 2019. Mobile Coverage and its Impact on Digital Financial Services. s.l.:s.n.

Sen, S. et al., 2011. Can they hear me now? A case for a client-Assisted approach to monitoring wide-Area wireless networks. s.l., Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conf.

Sulaiman, S. & Almunawar, M., 2021. The adoption of biometric point-of-sale terminal for payments. Journal of Science and Technology Policy Management.

Zhang, P., Durresi, M. & Durresi, A., 2018. Mobile privacy protection enhanced with multi-access edge computing. s.l., 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, pp. 724-731.

Caburn Telecom

Part of the CSL Group

caburntelecom.com

+44 1257 543917

Caburn Telecom
Part of the CSL Group

NEVER LOSE A PAYMENT

ALWAYS STAY CONNECTED

caburntelecom.com
+44 1257 543917