

# WHITE PAPER

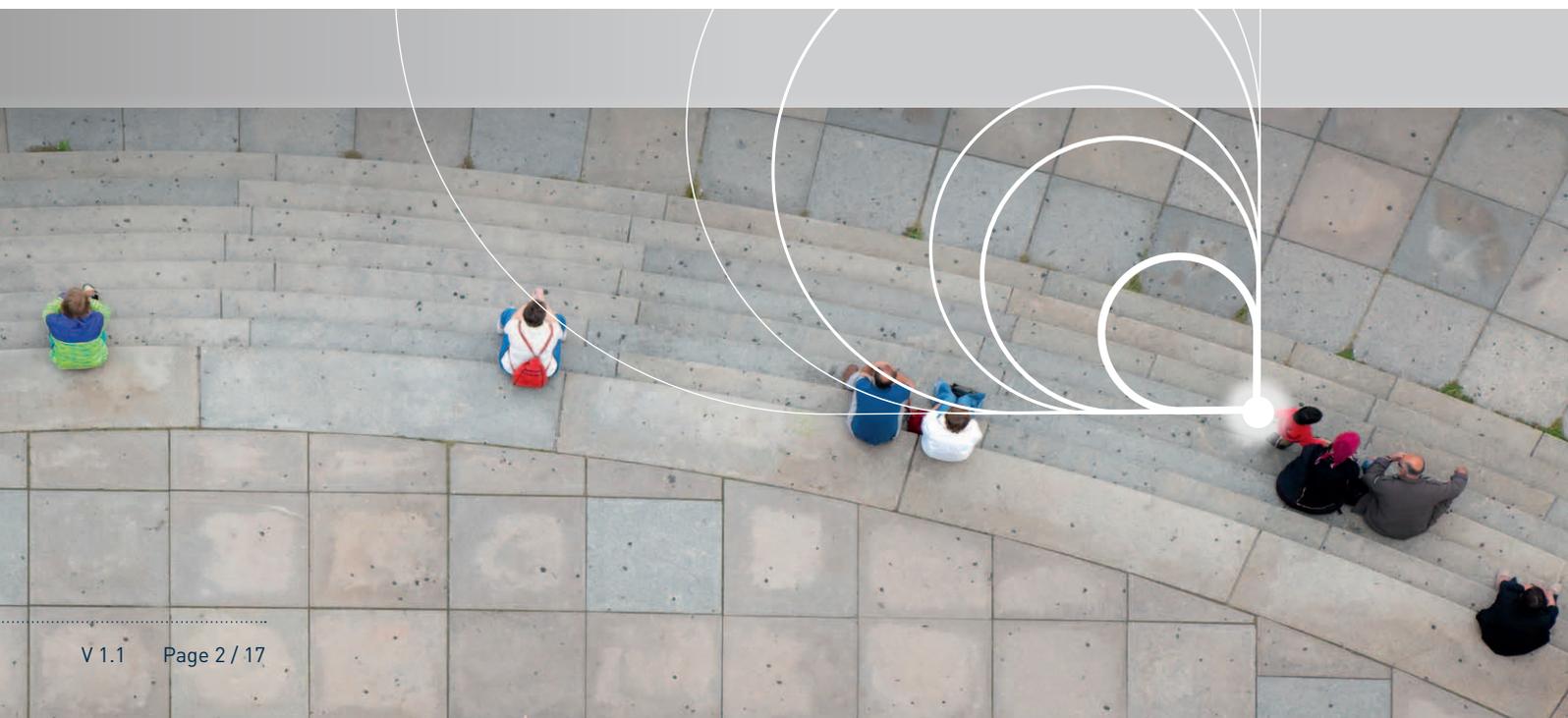
## m2mAIR MISSION

**m2mAIR**

by **Telit** m2m experts

## TABLE OF CONTENTS

	Page
1. Overview	3
2. The m2mAIR Mission Statement	3
3. Challenges	3
3.1. Perception vs. Reality	3
3.2. Major Challenges	4-5
4. m2mAIR Global Services	6
4.1. Global Connectivity Partnership	7
4.2. Managed Services	8
4.2.1. Subscription (SIM) Lifecycle Management – Service Delivery Platform	9
4.2.2. Post Production Feature Access (Remote AT)	10
4.2.3. Module Management	10-12
4.2.4. Security	12-13
4.3. Customer Support and Professional Services	14-15
4.4. Billing and Business Support System	15
5. Benefits For m2mAIR Customers	16



## 1. OVERVIEW

---

The m2m industry is at an interesting evolutionary point nowadays. On the one hand it is still very much a “Do It Yourself” industry in need of stable and common application development standards, protocols, middleware and development tools. When designing and building an m2m application / solution one is required not only put all the pieces together and deal with the complexities of building a working scalable client server application, but also to deal with complex logistic issues like the procurement of global managed and value-added services including connectivity, scalable subscription lifecycle management, and efficient troubleshooting deployment issues as well as various other difficulties that apply to most m2m applications. On the other hand, the industry is growing, applications and solutions across all m2m industry verticals are becoming more complex, pervasive and global and a high quality standard is expected both from the core product and from the operational perspective. m2mAIR by Telit is uniquely positioned to offer managed and value-added services including connectivity that allow m2m application / solution providers to focus on what they really need to do, i.e. design, develop, deploy and run business applications.

---

## 2. THE M2MAIR MISSION STATEMENT

---

The m2mAIR mission statement is “Making m2m connectivity seamless”. The m2mAIR approach to accomplishing this objective is straight forward: Making m2m connectivity seamless is about ensuring that managed and value-added services including connectivity come “out of the box” and that they are easy to deploy and use. Customers should not be concerned with procurement procedures, complex logistics and integration into their own solutions and applications. In m2mAIR we believe that when connectivity is seamless, well integrated and easy to use it will become pervasive, be embedded, used and integrated everywhere, and evolve into a powerful managed services eco-system.

---

## 3. CHALLENGES

### 3.1. PERCEPTION VS. REALITY

---

The premise that most people have, including m2m application / solution developers, is that scalable, multiple geography and even global connectivity is seamless and that it is fundamentally easy to procure, implement and manage. This premise is based on the personal experience that people have with their advanced consumer mobile handset / smartphone that costs between several dozen to several hundred USD and that is designed to cater to the needs of subscribers who generate monthly ARPUs ranging into the multiple dozens of USD.

The driving assumption when designing and implementing, not all, but many m2m applications / solutions is something along these lines: “Let’s build the box, invent an application level protocol, write a device side application that works with the com-

munications module and implement a backend that can receive information from many boxes and do something with it. Then, we’ll purchase a bunch of SIM cards, stick them in the terminals and it should just work for thousands or even millions of subscribers, everywhere the boxes go, much like it does on a mobile phone and everything should be fine”.

At a naïve and very high level this is a correct assumption; this is how mobile connectivity should work. But, the reality of commercial, scalable, cross geography solution deployments is somewhat different and commercially deployed, enterprise grade m2m solutions have unique managed services and connectivity needs and they pose challenges that differ from the consumer market.

m2mAIR is based on both grassroots and high level knowledge of the challenges facing real life m2m deployments. This knowledge comes from the deep understanding of device side mobile connectivity and application development that exists at Telit and the m2mAIR business unit within Telit that includes mobile network and application development experts. m2mAIR has a business partnership with a leading global connectivity provider, Telefónica, and an underlying service infrastructure (subscription lifecycle management, BSS, VAS, technical support and professional services) to deal with these challenges, allowing m2m application / solution providers to get all that from the m2mAIR “one stop shop” and focus on their core business.

## 3.2. MAJOR CHALLENGES

---

The scope of m2m application / solution challenges is wide, but those that are related to m2m connectivity can be divided into the following business, logistic and technical challenges:

### 1.

---

Procuring scalable cross-geography connectivity with minimum impact on the application / solution Bill of Materials (BOM) and a reasonable impact on the solution's Total Cost of Ownership (TCO) for the application / solution operator or end customer.

Customers with an actual or potential near term deployment of several thousands of units often experience lack of access to reasonable pricing for managed services and connectivity that will ensure that their applications / solutions are competitive.

This type of customer is still too close to a "regular" or "single" scale subscriber from the point of view of consumer Mobile Network Operators and they struggle to deal with the pricing, billing, geographical footprint and technical support requirements. As a result the solution they offer is too expensive and inflexible.

### 2.

---

Procuring scalable cross-geography managed services and connectivity from the minimum number of providers as possible to streamline logistics, operations, finance handling, etc.

m2m application / solution providers often have special operations and logistics needs, e.g. they are required to address issues like scalable subscription lifecycle management. Some have large numbers of SIM cards in stock for a while before they actually deploy them in mobile units and they need the subscriptions to be in a non-active state and transfer to an active state only after a certain amount of time passes or a certain amount of traffic is consumed by the unit. Sometimes they need these subscriptions to deactivate under certain conditions and to change the pricing model appropriately, etc.

Another typical requirement of large scale m2m applications / solutions is the need for consistent connectivity for a large geographical footprint across multiple countries and regions. Buying from multiple local suppliers with different pricing and billing plans, different technical and logistic capabilities and different qualities of service and technical support can pose major operational issues. At best these issues become logistic and financial hassles, but in some cases they can be detrimental to the core functionality and business model of the application / solution.

### 3. Real time cost control

---

There is a clear need to be able to verify that the cost of connectivity on units is not running rampant and thereby avoid unpredictable bill shocks that may compromise the m2m application / solution pricing and business model.

The fact is that most m2m applications / solutions are extremely cost conscious since the ARPU of a single subscription is typically quite low compared with a regular "human" subscription. This makes m2m subscriptions sensitive to deviations in single unit level network consumption patterns. Sometimes, a single "high runner" unit consuming overage network traffic due to intentional misuse or a software defect can cause an unpredictable "bill shock" that compromises the profitability of a large deployment for many months.

### 4. Consistent Roaming Service / Network Coverage

---

A major challenge for many global and cross border M2M applications / solutions is access to consistent network and service coverage in all the respective territories, along with the appropriate technical support and troubleshooting tools to analyze and resolve particular situations where coverage issues occur.

Although network coverage may seem like a given with GSM/UMTS roaming this is not always the case. Roaming has its technical challenges like: preferred operator selection, intervening steering mechanisms, and local coverage and registration issues. It is more difficult to troubleshoot an issue while roaming and to access information from the roaming partner network and consequently the incident resolution cycle is longer. Sometimes m2m applications / solutions were developed under home network connectivity conditions. Therefore application handling of certain roaming issues like longer first time registration are overlooked and this can cause major issues during deployment. As a result it will be extremely difficult to analyze in the absence of effective technical support and troubleshooting.

## 5. Technical Support and Troubleshooting

---

The network connectivity provider's technical support and troubleshooting capabilities are often a key factor for successful m2m application / solution deployments and their importance is usually underestimated and played down by application / solution providers.

Statistically when deploying an application / solution, especially a fledgling one without a proven track record, there is almost always a certain percentage of units that do not operate as expected and that behave quite differently than they did "in the lab" or even in field testing. There are multiple reasons and points of failure that cause this: for example, unit installation, software bugs in both the unit and server components of the application / solution, faulty design of network access implementation on the unit side, faulty design of network topology on the server side and also real mobile network connectivity issues (both local and roaming) like registration, coverage, packet data communications setup etc.

When the m2m units are being deployed, and even when they are already in the field and operational, if a problem occurs it is often the sophistication of the network connectivity provider's technical support and troubleshooting capabilities, ranging from Over The Air diagnostic solutions to professional services, that can deliver a Root Cause Analysis (RCA) and sometimes even a resolution of a crippling technical fault.

## 6. Security

---

Security is always a challenge in every type of computing solution that includes components that need to communicate with each other. The challenge in the case of m2m applications / solutions has several dimensions, some of them are unique to m2m since often there is nobody who can control a specific unit, notify a call center that something is wrong with it, alert about theft or misuse, or simply shut the unit down or restart it.

First of all there are the "usual" security dimensions related to connectivity, like authentication, encryption and privacy that require a certain IT infrastructure to be in place. The second dimension is a whole layer of defensive services and solutions that need to be put in place against malevolent misuse of the m2m unit or connectivity assets.

Examples include fraudulent usage patterns detection, SIM theft detection, asset geo-fence violation detection, unit location awareness, alerting, etc. Following detection damage limitations solutions need to be in place to quickly deactivate the subscription of a stolen unit or SIM card in order to prevent rampant network usage that would compromise a deployment's profitability.

If these security solutions do not come from the managed connectivity provider, then the M2M application / solution providers have to custom build them into their application. This requires considerable R&D effort, integration, maintenance, hardware, hosting and software licensing costs that are not related to the core m2m application / solution.

## 7. Immature m2m Applications

---

Many applications are developed almost from scratch and are not based upon robust, proven platforms. Although the underlying communications hardware is a hardened, industrial grade component, developers in most cases, and especially in new applications, write most if not all the application code themselves. This may mean that they do not take all the applicative aspects of connectivity into complete and thorough consideration. There are many examples of this ranging from incorrect handling of end case problems in device registration, incorrect connection retry mechanisms, incorrect implementation of recovery scenarios from momentary out of coverage through to asynchronous PDP context drops and so on.

Some issues are not easily reproducible in laboratory conditions and are triggered by specific real life conditions in the field. In cases like this, application certification by an experienced partner with broad horizontal use case experience and the right environment to simulate potential error scenarios may prove very valuable when starting to deploy the application.

---

## 4. m2mAIR GLOBAL SERVICES

As indicated in section 3, scalable, wide area m2m connectivity entails many challenges. So, how can m2mAIR help deal with those challenges and enable application / solution providers to focus on their core business applications?

m2mAIR offers a multi-tiered managed services solution built on:

- Global SIM and network connectivity by Telefonica;
- Industry leading Service Delivery Platform;
- Advanced Telit Value Added Services.
- Customer Support and Professional Services.

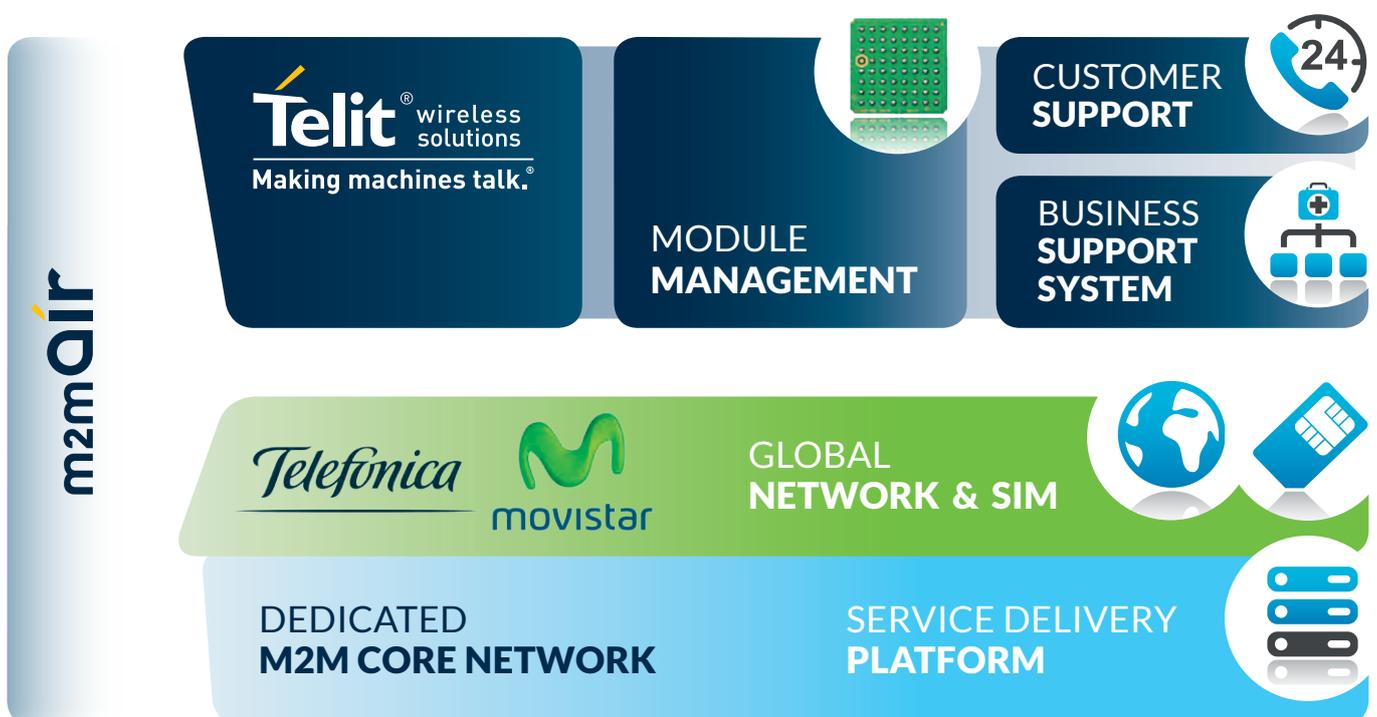


Figure 1: m2mAIR Offering Building Blocks

Telit's contribution to this offering is enhanced by its expertise and control as the module manufacturer, including control of module software and enabling managed value added services that interact with the module.

## 4.1. GLOBAL CONNECTIVITY PARTNERSHIP

---

An important element of m2mAIR's offering is a strategic partnership with Telefónica. Telefónica is one of the top three tier-1 global mobile network operators. It has wide service coverage including Europe, Latin America and China. Moreover Telefónica has made huge investments in m2m including dedicated service components, the industry leading service delivery platform and value added services.



Figure 2: Global Service Coverage

Through its partnership with Telefónica m2mAIR is offering its customers, ranging from those using only hundreds of modules to those using many thousands of modules or more, enhanced functionality and lower cost connectivity, i.e. rates that would normally be restricted to the kind of large scale projects that obtain the direct attention of tier-1 MNOs.

Moreover it is combined with the connectivity footprint and backing of a tier-1 MNO and a set of services that MNOs do not usually provide to small and mid-range customers. In addition to the above, m2mAIR provides its customers with subscription lifecycle management, Value Added Services, technical support and professional services.

Some of this additional functionality goes beyond what even tier-1 MNOs currently offer, for example, services that provide accurate of usage control plus network and module related monitoring.

## 4.2. MANAGED SERVICES

Let's take a look at the services that m2mAIR is offering along with connectivity. They allow m2mAIR to function as a one stop shop for m2m application / solution providers, thereby helping them overcome scalable, wide area connectivity challenges and allowing them to focus on their core business functionality.

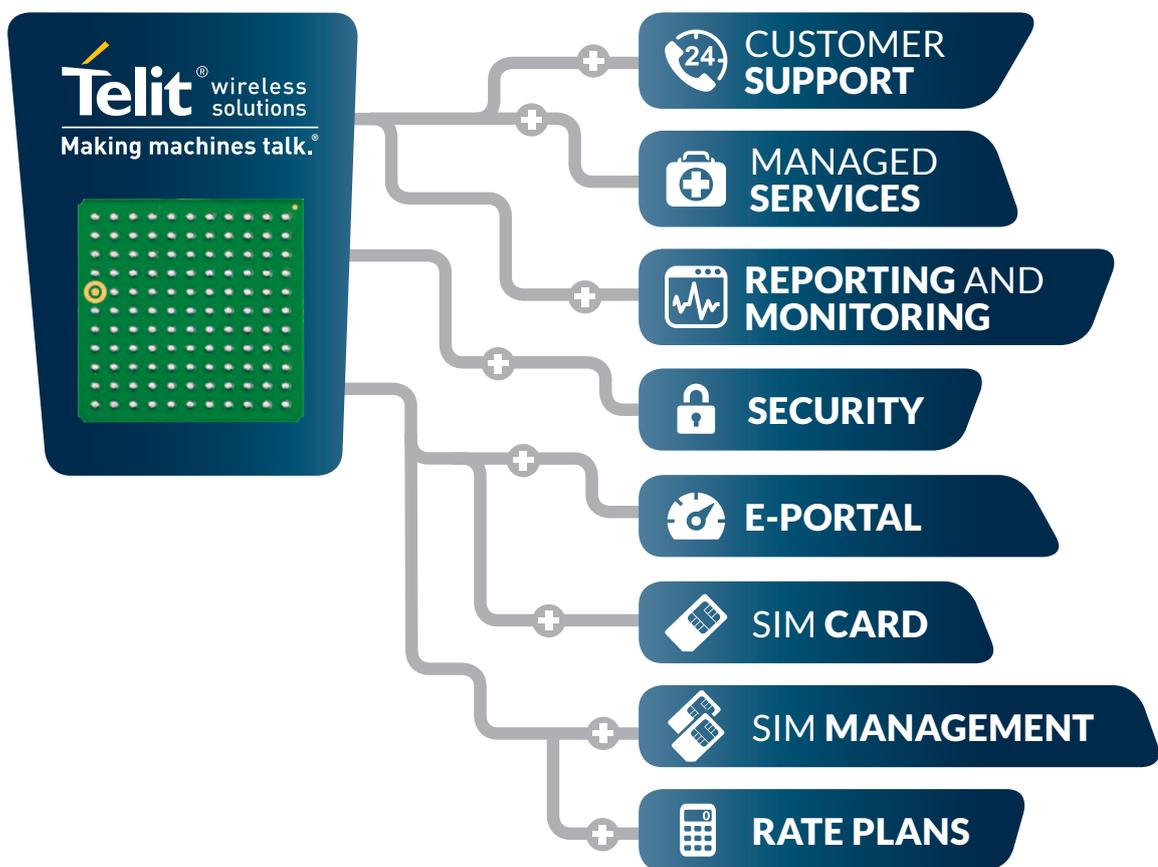


Figure 3: The m2mAIR One Stop Shop

## 4.2.1. SUBSCRIPTION (SIM) LIFECYCLE MANAGEMENT – SERVICE DELIVERY PLATFORM

Effective mobile connectivity and subscription lifecycle service delivery starts with a Connected Device Service Delivery Platform (SDP) that is tightly integrated into the MNO's core components. This allows both the managed connectivity provider and the user to access and manage a subscription

deployment down to the single subscription level. The platform exposes its functionality using a Web portal for human interaction and a set of Web Service APIs for integrating 3rd party solutions such as Business Support Systems that can implement custom automated batch processing procedures.

The SDP allows the managed services provider (m2mAIR in this case) to control the subscription life cycle and to manage when and under which business rules and conditions the subscription should transition between activation and billing states (e.g. from "test ready" to "active").

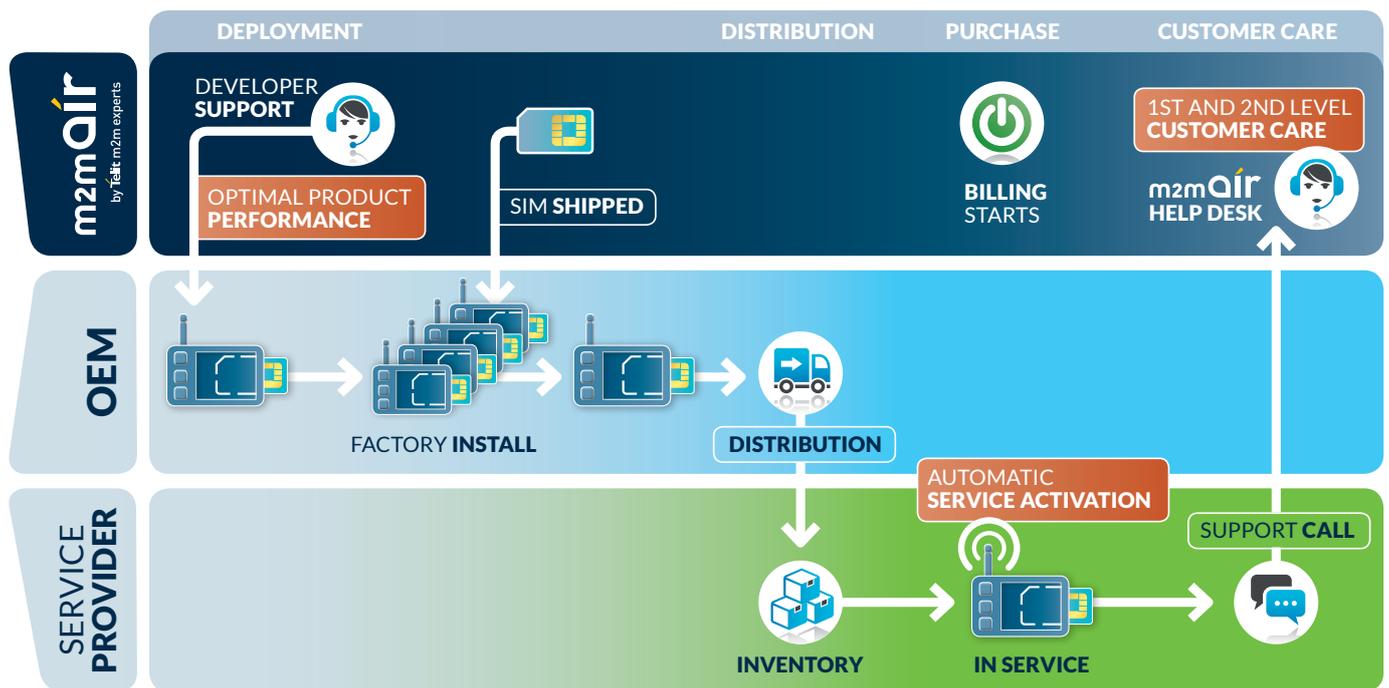


Figure 4: Flexible subscription Lifecycle

An important feature of subscription lifecycle management is automatic service activation that allows setting and implementing a threshold based rule (e.g. first use of X KB of data) for subscription and billing state transitions (e.g. transition from "test ready" to "active"). This way it is possible for an m2m application / solution provider to hold batches of SIM cards in stock, waiting for deployment. The SIM cards can also be used to perform product unit testing without being billed for the traffic. Only when a SIM card is commercially deployed in the field and the subscription consumption goes beyond the predefined threshold will the subscription move to the "active" state and the agreed billing cycle will start.

The advanced, state of the art SDP used by m2mAIR exposes a set of APIs that can be used to implement custom business rules that are not offered out of the box by the platform. These rules can be implemented by a backend application such as m2mAIR's Business Support System (BSS). Using this functionality, customized billing rules can be implemented in order to tailor fit the unique business needs of some m2m application / solution providers.

For example an advanced billing plan can be implemented based on a rule that triggers subscriptions to automatically transition to a non-billable state when they do not generate any traffic after X days and then move back to a billable state when data traffic has resumed and has crossed

a certain threshold. This way it is possible to allow an application / solution provider to ensure the subscriptions are in a billable state only when the end consumer actually consumes the service and is paying for the subscription.

The SDP used by m2mAIR also enables the delivery of advanced capabilities and support to smaller customers. A key feature of the SDP is that it is easy to provision new small to medium sized customer accounts. Each customer added by m2mAIR can then add further sub-accounts for their own customers. Using this approach, it is possible to provide smaller companies with the level of service that is usually provided only by much larger application / solution providers.

### 4.2.2. POST PRODUCTION FEATURE ACCESS (REMOTE AT)

Telit's rich API comprises hundreds of AT commands that are implemented in the modules. Through m2mAIR Managed Services, Telit enables application / solution providers to use module APIs and features, over the air, for which their terminal based applications were not initially designed.

This capability is the foundation of Telit's Over The Air (OTA) service capabilities

Through managed services it is possible to access module features and services after the modules have been shipped and installed (post-production). This enables

solution and application providers to utilize value added services that are not directly linked to the terminal application. All this can be done easily and seamlessly, post production, through a modern SaaS web platform.

### 4.2.3. MODULE MANAGEMENT

Built upon Telit's post production feature access framework, remote module management is an Over the Air (OTA) service that m2mAIR intends to switch on in early 2013. It will enable seven initial remote module management features with more to come going forward. The seven initial module management features are:

- Network Diagnostics;
- Remote Reset;
- Module Inventory Properties;
- Remote IP Testing;
- Preferred MNO Selection.
- Remote Hardware Testing;
- Usage Policy Management;

The focus of the initial release is on features related to diagnostics, service level monitoring and cost control.

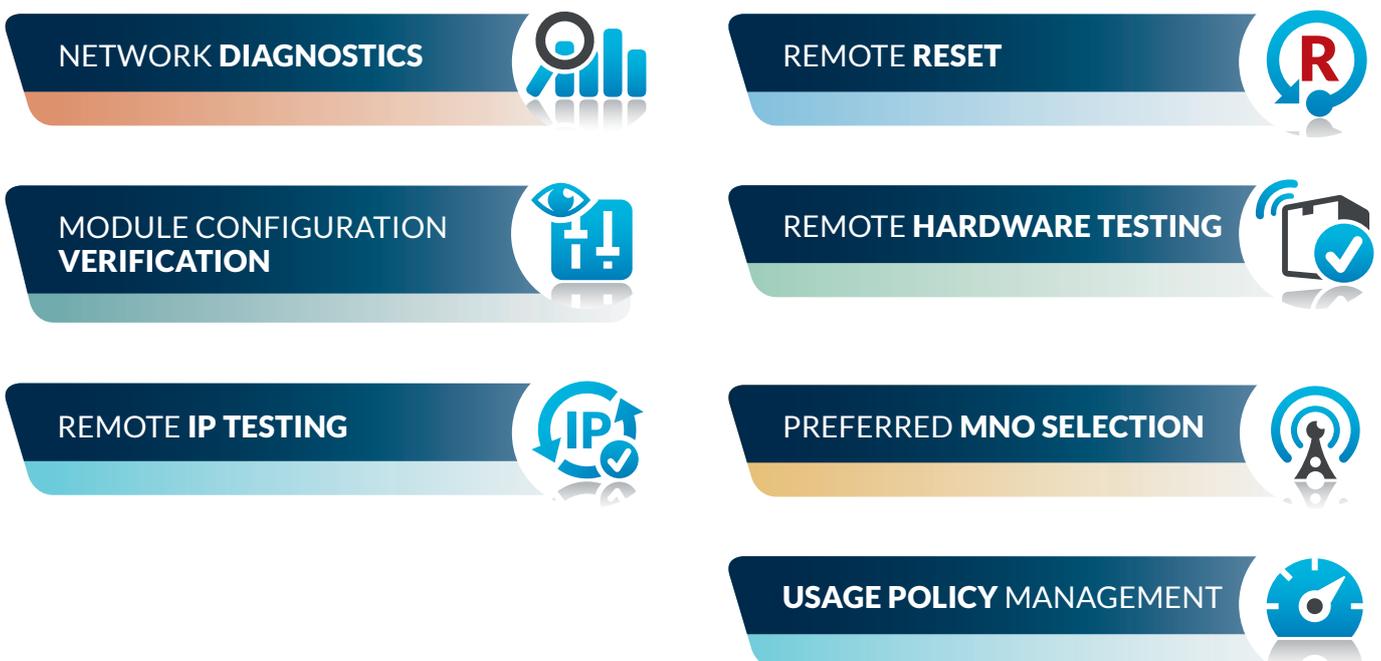


Figure 5: Module Management

## **1. Network Diagnostics**

---

Fundamental network service information such as current reception level, reception quality, network operator and location information, etc., can be checked in real time and accessed by the customer. Mobile operators do not usually provide access to this information, which is very important for technical support, troubleshooting, and managing problematic issues in wide area m2m deployments.

## **2. Remote Reset of a module**

---

A selected module can be remotely reset. This is valuable in cases where a connectivity reboot is required for SIM re-registration to the network.

## **3. Module Inventory Properties**

---

This device inventory feature allows the module to be queried or its exact model, firmware version, IMEI, etc. This is important for troubleshooting an m2m terminal. It allows the correct actions and workarounds for the individual module to be selected, for example, if a software bug is detected in the application interaction with the module. This service provides immediate access to this information, which is often very difficult to obtain in any other way in large m2m deployments.

## **4. Preferred MNO selection**

---

This service enables the user to trigger the module to change the serving mobile operator. Customers can switch between roaming MNO coverage in real time. This can assist in ensuring network access service levels and in controlling operational expenditure.

## **5. Remote IP testing**

---

Enables a module's connectivity to be tested in the field in order to verify that everything is working and that the packet data networking resources are available. Examples include: Ping IP; echo testing; and incoming connection testing.

## **6. Remote hardware testing**

---

This diagnostic feature enables remote hardware tests including: antenna connection; battery charge; temperature of the module; and others. If the m2m unit doesn't work then the cause is often not apparent. This feature can, for example, get a report from the module showing whether there is an antenna installation problem, which is quite common.

## **7. Usage Policy Management (Roadmap)**

---

This cost control service is focused on real time module side consumption monitoring. Usually connectivity providers offer an alerting service if a unit is using too much data in a chosen period. This information is usually gathered from roaming partners, often with considerable latency of around 20 minutes. Such delays are a problem given, for example, a software bug that causes the unit to over consume data. This service allows real time monitoring of module usage. This also means that the service can be used to gain accurate data and voice usage in real time for cost control purposes. .

---

The module management service is based on Telit's remote AT command interface. Because of the flexibility enabled by accessing facilities at the module level, many new services are expected to be switched on in order to extend the richness of the overall service offering. The Module Management

Service can be accessed by the customer using a Web portal (for single device access) or a Web service API for batch access.

These capabilities are additional to those of the Service Delivery Platform. Overall these new services and the rest of the offering can

be seen as a "cycle". The cycle begins with problem detection then with analysis and finally with resolution. The Module Management Services are an important component of problem analysis and resolution within the cycle.



Figure 6: The Resolution Cycle

#### 4.2.4. SECURITY

As discussed in section 3.2 part 6 above, security is a fundamental challenge and requirement in all communications and networking solutions. The m2mAIR approach to security is multi-dimensional. It is based on preventive technologies focused on authentication and encryption, as well as defensive technologies that deal post factum with malevolent events like interception and theft.

The core security solutions implemented by m2mAIR are:

- IPsec (SSL) VPN Tunneling all the way from the module to the backend, using Telit modules embedded SSL stack implementation and the m2mAIR IP Core. This provides powerful encryption (on top the standard GPRS/EDGE/HSPA encryption) and removes the possibility of eavesdropping on the data communications.
- Dedicated APN – A dedicated APN association to the subscription prevents a stolen SIM card being misused for unwarranted data communication.
- Secure SIM authentication and PIN code – requires authentication before a data channel is setup, either explicit or implicit based on the hardware identification. This technology prevents unwarranted data usage and misuse of stolen SIM cards.
- Secure SMSC – assures that all SMS communications to the deployment subscriptions is done from a designated secure SMSC. This prevents spoofing and the ability to send false commands to m2m applications / solutions that use SMS as a Mobile Terminated (MT) OTA control and configuration bearer. Using Secure SMSC the possibility of using SMS as an attack vector on an M2M application / solution is greatly reduced.
- Module based policy management – is a real-time, module-based usage hedging solution that protects against unpredicted data usage caused, for example, by application software issues.
- Embedded Jamming Detection (Roadmap) – A diagnostic security feature that can report either in real time or post factum that a jamming attempt, intended to block mobile coverage, was made in the vicinity of the module. This is mainly applicable to applications in the security vertical space.

 <b>IMPERSONATION</b>	 <b>INTERCEPTION</b>	 <b>SIM THEFT</b>
<ul style="list-style-type: none"> <li>• Embedded SSL encryption</li> <li>• IPsec</li> <li>• Network usage alarms &amp; limits</li> <li>• Module-embedded usage policy management</li> <li>• Secure SMSC</li> </ul>	<ul style="list-style-type: none"> <li>• Embedded SSL encryption</li> <li>• IPsec</li> <li>• Embedded jamming detection</li> </ul>	<ul style="list-style-type: none"> <li>• PIN Authentication</li> <li>• Dedicated APN</li> <li>• "Secure SIM"</li> <li>• Network &amp; module based policy management</li> <li>• Low bandwidth tunnel</li> <li>• IMEI verification</li> <li>• VPN IPsec</li> </ul>

Figure 8: Security Solutions and respective use cases

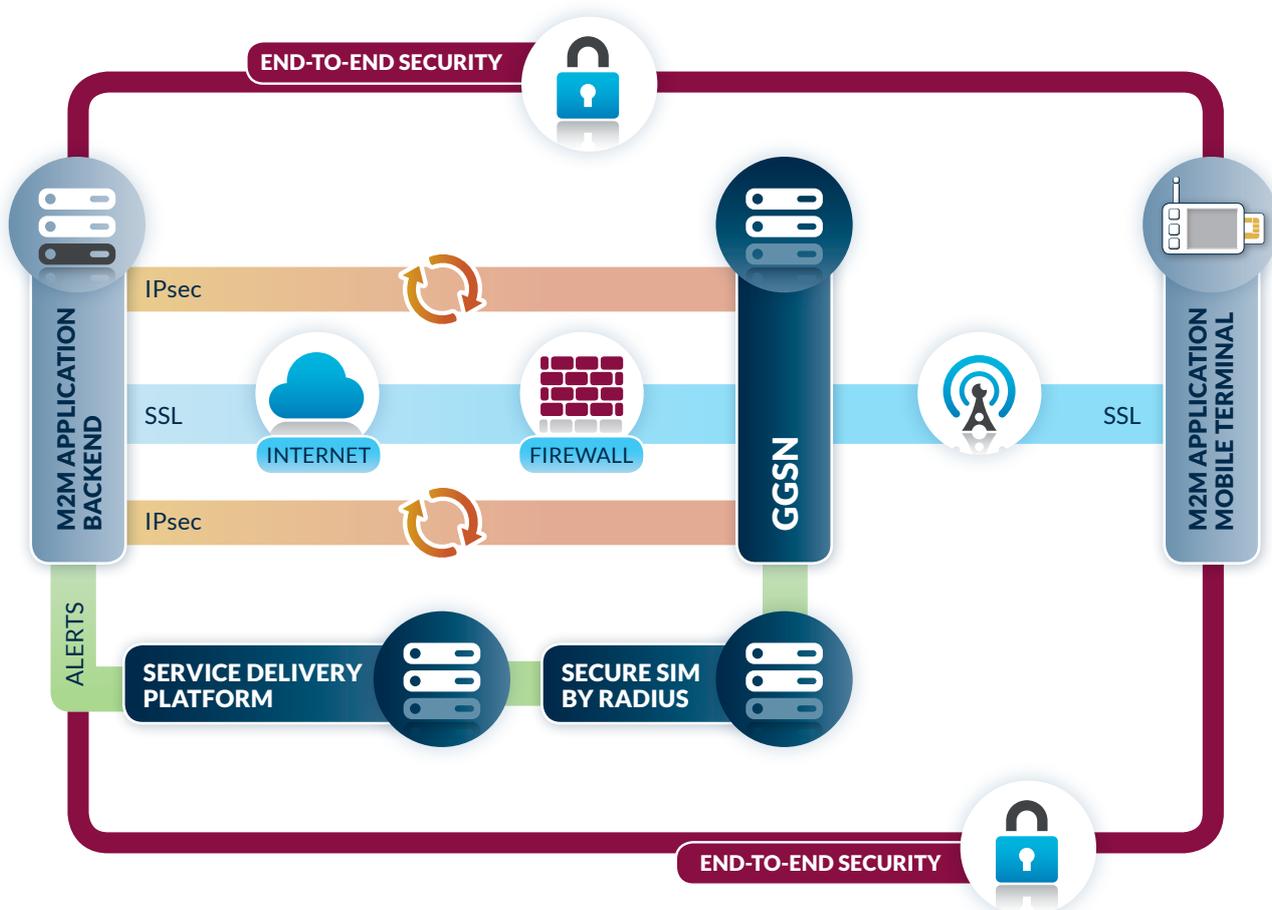


Figure 7: m2mAIR secure managed and value-added services including connectivity

### 4.3. CUSTOMER SUPPORT AND PROFESSIONAL SERVICES

m2mAIR emphasizes effective proactive and reactive customer technical support as a fundamental pillar of its mission of “Making m2m connectivity seamless”. Proactive technical support is focused on application validation and certification in order to minimize occurrences of unpredicted unit behavior in commercial deployments. Reactive technical support is focused on the

analysis and resolution of connectivity issues when they unfold. m2mAIR is well positioned for both types of support through its managed services infrastructure and its partnership with Telefonica. In addition there is Telit’s in-depth acquaintance with its customers’ m2m offering gained over 2-3 years engineering design cycles.

Proactive technical support is offered through the m2m Lab program and access to Telit R&D, which is focused on application certification and correct application implementation practices. Reactive customer support is based on m2mAIR’s Service Delivery Platform, diagnostics and resolution capabilities as detailed earlier.

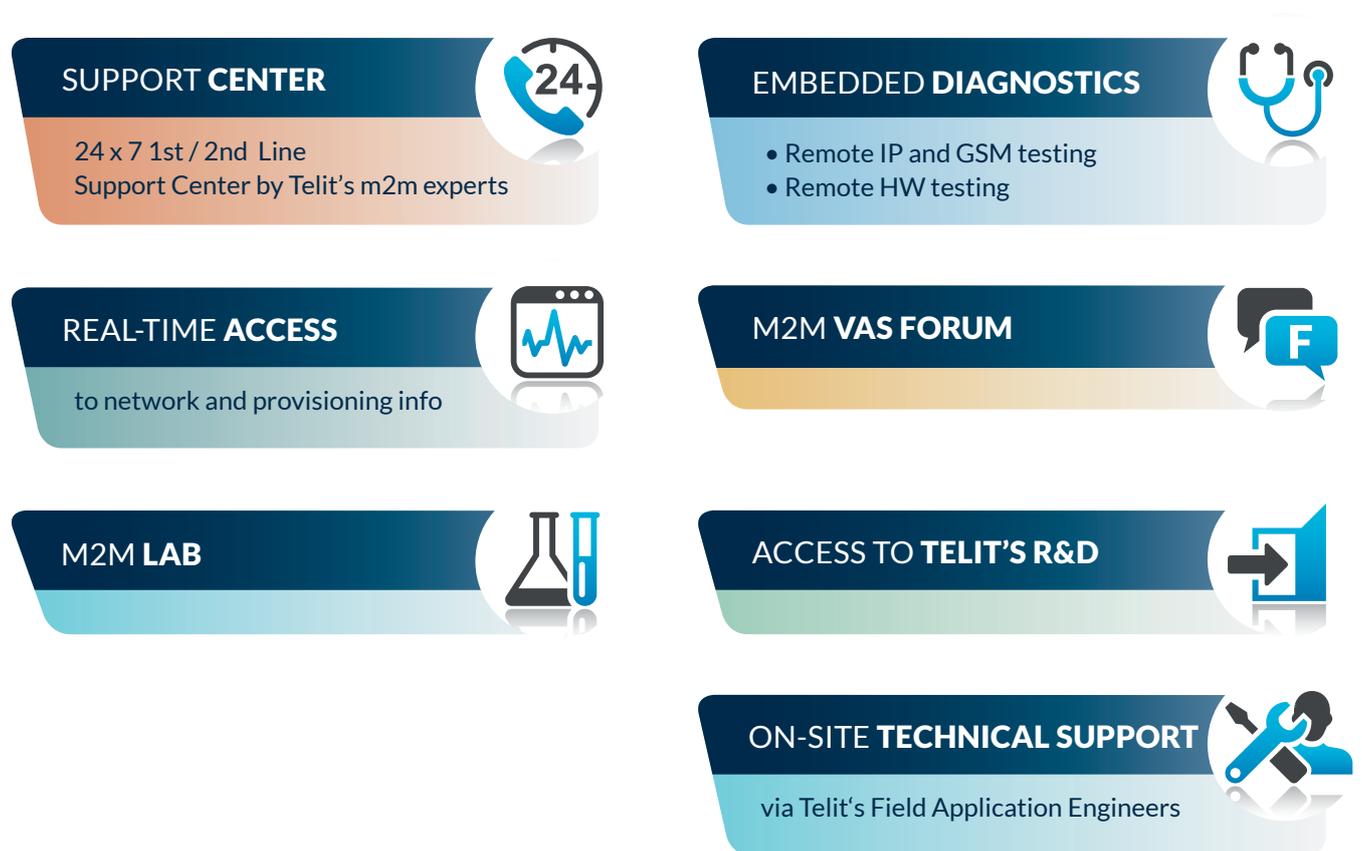


Figure 9: m2mAIR Customer Support

### **1. 24x7x365 1st Line support center**

---

24x7 is a standard that only a handful of connectivity and managed service providers provide.

### **2. Access to Network and provisioning information**

---

Access to device information through the SDP. m2mAIR believes this is one of the differences between its platform and all of its competitors. m2mAIR has an analytical layer on top of the information received from the operator's network. These features are not readily accessible to MNOs or customers that are not using this SDP.

### **3. Fast Access to Telit's R&D ies**

---

This is another advantage of m2mAIR's Technical Support. Telit developed its own software stack in many module models and access to it provides very strong troubleshooting and problem resolution capabilities.

---

### **4. Built in diagnostic capabilities**

---

Telit modules have built in diagnostics capabilities based on the post production feature access through remote AT commands.

### **5. m2m Lab**

---

m2mAIR invites customers to visit its Labs, where they have infrastructure and facilities for testing their designs. Customers can test their solutions with m2mAIR's internal tools, and can also test and validate their applications, their source code and other parts of their m2m solutions.

### **6. m2m VAS Forum**

---

Telit has a very strong, Web based Forum for its customers. As part of the new services Telit will add "Managed Services" to that Forum.

## **4.4. BILLING AND BUSINESS SUPPORT SYSTEM**

---

Billing is one of the most important features of the m2mAIR mission of "Making m2m connectivity seamless". It is pivotal because in m2m it is even more complex than that in consumer connectivity services. ARPU is usually quite low and very cost sensitive. An inappropriate billing plan can be detrimental to an application / solution's business case and can induce operational expenses that would cripple deployment.

Supporting customers of different size deployments, from different m2m verticals, and with different geographical footprints often requires the ability to rapidly setup a tailored billing plan with customized business rules that are unique for specific customers. The billing plan must take into account all the parameters mentioned above as well as the subscription lifecycle rules that fit that specific customer (see example in section 4.2.1 above). MNOs' legacy billing systems are not designed to support this level of flexibility and customization.

---

m2mAIR's internally-developed Business Support System (BSS) is a multi-layered, flexible and scalable platform that includes end-to-end functionality that allows m2mAIR to perform as a fully-fledged m2m managed service provider to customers of all sizes. This includes the following carrier grade subsystems: customer and product management, provisioning, billing, and integration interfaces towards Telefonica and other relevant third-party Web Services.

## 5. BENEFITS FOR m2mAIR CUSTOMERS

---

m2mAIR offers its customers services, solutions and ways of effectively dealing with all major m2m connectivity challenges, both the business and technical aspects.

### 1.

---

m2mAIR's partnership with Telefónica brings in scale, presence and a wide geographical footprint, which enables customers to purchase managed services and connectivity from a single provider in many countries and reduce logistical complexity and fragmentation.

### 2.

---

Telit, a leading global provider of high-quality machine-to-machine (m2m) modules and value-added services, has in most cases a long-term relationship with the customer and a deep acquaintance with the m2m application / solution. So now a customer can buy communication equipment and managed services including connectivity from the same supplier, thereby reducing supply chain complexity and profiting from the synergies between Telit modules and the current and future m2mAIR service portfolio.

### 3.

---

Telit is the owner of the module software stack and is therefore well positioned to introduce through m2mAIR new, unique services that better handle the technical and business challenges described in this whitepaper. These services are all based on seamless, embedded, runtime services in the module and they do not require integration with the application layer.

### 4.

---

m2mAIR offers real-time cost control solutions that enable verification that the cost of connectivity on some units is not running rampant. This avoids unpredictable bill shocks that might compromise the pricing and business model.

---

### 5.

---

m2mAIR offers real-time cost control solutions that enable verification that the cost of connectivity on some units is not running rampant. This avoids unpredictable bill shocks that might compromise the pricing and business model.

### 6.

---

m2mAIR offers extensive technical support, diagnostics and troubleshooting, key factors to a successful m2m application / solution deployment. m2mAIR also offers on site field support based on Telit's Field Application Engineer task force. This is a first of its kind development.

### 7.

---

m2mAIR offers a set of advance preventive and defensive security solutions as a service to its customers that otherwise need to be implemented at the application level.

### 8.

---

And last but not least, m2mAIR offers m2m application development related professional services and lab certification. This is based both on best practice M2M application / solution development, with a focus on connectivity, as well as addressing problematic application related issues, root cause analysis and resolution.



**m2mAIR**

by Telit Communications PLC

**Phone** +39 04 04 192 555

**Email** [sales@m2mAIR.com](mailto:sales@m2mAIR.com)

***www.m2mAIR.com***

**m2mAIR**

by **Telit** m2m experts