THE CASE FOR M2M DEVICE MANAGEMENT

HOW NETWORK OPERATORS CAN HELP BRING M2M TO THE MASS MARKET

STRATEGIC WHITE PAPER

The machine-to-machine (M2M) industry is focused on extending its reach beyond niche verticals. Key players across the industry want to gain access to verticals where there are opportunities to support mainstream consumer-scale deployments involving tens of millions of endpoints. But progress toward the mainstream is being slowed by technology fragmentation, a lack of industry-wide standards and complex device onboarding processes. Progress is also being hindered by the fact that consumers do not yet fully trust M2M solutions with their devices and data.

Network operators are well positioned to help the M2M industry address these challenges and move forward. With platforms that allow them to merge their trusted remote device management and onboarding expertise with standardized M2M functions, network operators can reach more devices and verticals, deliver more value to customers and secure a stronger role in the M2M market.

TABLE OF CONTENTS

Introduction / 1

Coping with complexity / 1

M2M device management: The network operator opportunity / 2

Extending M2M to new verticals / 3

Why remote device management is essential for M2M / 4

Developing standards for M2M device management / 5

Easing onboarding with interoperability testing / 6

Conclusion / 7

Abbreviations / 7

INTRODUCTION

The machine-to-machine (M2M) industry is in transition. Buoyed by growing consumer interest, M2M-friendly policies, strong wireless networks and inexpensive sensor technologies, the industry is shifting its focus from niche verticals to broad mainstream adoption. The emergence of cloud and big data technologies is helping to fuel this shift by bringing large, scalable and economically viable software and analytics solutions within reach.

Key M2M players want to capitalize on these trends and technologies and seize the opportunity to move beyond typical equipment monitoring use cases involving hundreds or thousands of endpoints. They have their sights set on creating applications that can work in different verticals and process data from tens of millions of devices.

A growing segment of the industry recognizes that new thinking and solutions are needed to move M2M beyond niche verticals. The first widely successful telematics, smart energy and smart grid applications have shown that M2M technology can serve the needs of the mass market. However, fragmentation and complex device onboarding processes still present formidable challenges. In many cases, they make it too costly, inefficient and difficult to roll out M2M on a broad scale.

The need to build consumer trust presents another obstacle to mass adoption. Consumers will not fully embrace M2M use cases and deployments until they are certain that they can trust the underlying infrastructure with their data. For example, consumers want and need to be sure that GPS location data from their smartphones or cars cannot be compromised. Their trust must be earned with solutions that can remotely manage, monitor and safeguard their devices, device software and data.

While formidable, these challenges open up opportunities for network operators to claim a bigger role in the M2M market. Operators already use their networks to provide connectivity services for M2M applications. But they have something even more important to offer — the ability to efficiently and securely onboard and manage devices on a broad scale. In building their consumer offers, network operators have shown that they can be trusted to support many protocols, ensure interoperability and security, and manage devices remotely. With solutions that bring their remote device management and onboarding capabilities together with common M2M functions, network operators can create a trusted M2M environment that reaches more devices and verticals, delivers more value to enterprises and generates more revenue.

COPING WITH COMPLEXITY

The introduction of smartphones brought new levels of complexity to mobile device onboarding, troubleshooting and management processes. The mobile industry reacted by developing stronger remote device management capabilities and turning a small number of technologies — most notably the iOS and Android operating systems — into de facto industry standards. These proved to be successful mechanisms for coping with complexity and bringing smartphones into the mainstream. The industry continues to refine and apply these mechanisms as it develops more advanced smartphones and consumer applications.

The M2M industry can learn from the mobile industry's experience and success with smartphones. It faces a comparable challenge: the need to overcome inefficiencies associated with technology fragmentation, device onboarding and platform profusion. These inefficiencies drive up costs and make it difficult for the industry to move beyond niche verticals and monitoring-based applications.

Divergent protocols and custom applications have fragmented the legacy M2M market. Fragmentation makes it difficult to handle devices consistently and develop solutions that can apply to more than one vertical market. What's more, it adds complexity, time and cost to integration processes. To achieve broader success with M2M, the industry must continue to develop standards that can harmonize device interactions, simplify integration and create economies of scale.

Past efforts to unify and simplify M2M processes have sometimes had the opposite effect. Today, the industry uses a variety of platforms to address different activation, billing, monitoring, application development and device management functions. Each platform takes a different approach and covers different aspects of the market. All of them fall short of what the industry truly needs — a scalable platform that adheres to standards and addresses a broad range of common M2M functions.

Device onboarding encompasses several tasks that are essential to M2M solutions, including interoperability testing (IOT), provisioning and firmware upgrades. Today, M2M device onboarding often involves complex manual processes that drive up costs and increase the likelihood of errors. The prevailing practice is to tailor applications to the capabilities of specific devices. This approach ties applications to devices and makes it difficult to mix and match old and new devices.

In the mainstream consumer world, we see increasing standardization and consolidation of device capabilities and applications that can run on a wide range of devices. To bring M2M to the mainstream, the industry must consolidate protocol choices and use this consolidation to create streamlined IOT processes that can characterize devices and their capabilities. These processes must allow consumers and operators to use the devices of their choice without having to engage in custom testing or multiple iterations.

M2M DEVICE MANAGEMENT: THE NETWORK OPERATOR OPPORTUNITY

Network operators have home and mobile device management expertise that can help reduce the complexity associated with M2M fragmentation and device onboarding. Each year, they add and upgrade support for hundreds of consumer devices and activate millions of device instances on their networks in a highly reliable and secure fashion. In doing so, they navigate and manage a diverse set of standards and device-specific protocols. The knowledge they gain in performing these activities is readily applicable to M2M applications.

The path to broader M2M success lies in bringing this device management expertise to M2M-specific functions. Network operators have a clear opportunity to encourage a shift toward a more scalable M2M business model. The addition of support for M2M device management functions such as provisioning, configuration, firmware upgrades and analytics will give operators the means to scale and streamline M2M operations and reduce support costs.

An operator can benefit in several key ways by complementing its network connectivity capabilities with standards-based device management as a service offering. For instance, an operator can gain a better understanding of what types of devices are attached to the network and how these devices use connectivity. This knowledge will enable the operator to manage its network more effectively. A standards-based platform can also support end-to-end service assurance and device diagnostic capabilities, both of which will help the operator troubleshoot problems and provide meaningful service level agreements (SLAs) to customers.

Moreover, standards-based solutions can empower an operator to bring more devices under management. Since unmanaged devices are untrusted by definition, the ability to manage more devices will help the operator secure and retain the trust of more consumers and enterprises. Standards will also allow an operator to adapt the behavior of generic devices to meet the needs of specific verticals. This will reduce the need for customized devices and allow the operator to reach a broader customer base.

Open APIs can add to the benefits offered by standards. By embracing open APIs, an operator will gain the ability to offer ready access to useful data and support common service and application lifecycle management functions. These new capabilities will increase their value to enterprises, governments and the M2M industry as a whole.

EXTENDING M2M TO NEW VERTICALS

Adding M2M device management capabilities will enable network operators to compete for business in new verticals and support consumer-scale deployments with 10 to 100 million endpoints. For example, operators could position themselves as M2M enablers for companies that offer usage-based or “pay as you drive” (PAYD) auto insurance. With PAYD insurance, cost and coverage are based on factors such as driving time, distance, location and behavior. Applications that support PAYD require connectivity to in-car GPS tracking devices and generic device management functions such as provisioning and firmware upgrades. Today, insurance companies pay over-the-top (OTT) suppliers to perform these functions. With solutions that support key M2M device management functions, network operators can wrest this business away from other suppliers and help insurance companies operate more cost effectively.

Network operators will see new M2M opportunities emerge in a variety of verticals and markets. The biggest of these opportunities will come from the automotive, energy and government verticals. In the United States, government policies could soon make M2M connectivity mandatory in all new vehicles. In Europe, energy policy makers are pushing for wider adoption of M2M-based smart grid technologies. Around the world, M2M is being presented as an essential enabling technology for smart city projects. These are promising growth areas for network operators — even more promising if they can extend their M2M offers to include device management.

The eHealth industry represents an immense M2M growth opportunity for network operators, but there are significant barriers to overcome. The industry features a vast ecosystem of stakeholders, a broad collection of use cases and a complex regulatory environment. An intricate system of rules determines how health data must be stored, managed, exchanged, transmitted and secured.

For network operators, the key to winning eHealth business is to earn the trust of all stakeholders. Operators have to prove that they can control the behavior of devices and applications and ensure that sensitive data remains safe at all times. The only effective way to achieve this degree of control is to establish remote management connections to all endpoints involved in collecting information. A standards-based M2M device management platform will help lower barriers to entry. But success in the eHeath market demands highly specialized integration capabilities and a sales force that is well versed in the inner workings of the industry.

WHY REMOTE DEVICE MANAGEMENT IS ESSENTIAL FOR M2M

Both application lifecycle management (ALM) and device management can enhance remote device control capabilities and create trusted endpoints. There are, however, important differences between the two. The primary focus of ALM is to establish a trusted and secure means to customize the behavior of devices. The focus of device management is to streamline onboarding processes and support device-related trouble-shooting. Device management solutions can also be used to perform ALM functions. A look at smartphone management strategies helps illustrate the differing functions of ALM and device management. Trusted application stores perform an ALM-like custom-ization function, while device management systems support firmware upgrades that control the basic core device functions.

Many legacy M2M devices include basic device management functions. These functions allow for configuration in cases where the device does not have a user interface. The creators of legacy M2M solutions argue that these basic functions are sufficient and that there is no need for extensive device management capabilities. They contend that M2M devices are very simple and that there is nothing to gain from adding broad support for scalability, diagnostics or firmware upgrades. Where more advanced device management is required, they create custom point solutions.

This viewpoint is losing credibility as the M2M industry seeks to support a wider range of devices and applications. Mainstream devices are becoming more complex as vendors and developers add processing power and software to bring better experiences to consumers. This trend is evident in devices as diverse as smartphones, Raspberry Pi computers and smart TVs. At the same time, there is a growing need to support devices constrained by low battery and computing power, low memory and low operating bud-gets. For example, companies that offer PAYD insurance may need to update thousands or millions of in-car GPS devices on a regular basis to ensure that these devices always use the latest risk profiling policies. The need for management solutions will only grow as enterprises and governments collect more data from more devices and use it in more advanced ways.

Remote device management has proven its value in consumer-focused markets that involve sophisticated devices like smartphones, residential gateways and set-top boxes. It promises to do the same for the diverse M2M devices and use cases of the future. With remote device management capabilities at its disposal, the M2M industry will have the ability to support functions that are critical to mass-market expansion. These functions include:

- Automated device configuration – Device management can be used to configure important on-device parameters such as server addresses, times when different applications can be used and communication protocols that should be used to connect to different servers.
- Over-the-air firmware upgrades – Device management platforms can upgrade device firmware remotely. This function is critical for M2M because many devices will be deployed at different times with different firmware versions. Once deployed, devices may remain operational for very long periods. For example, smart meters for the energy industry may operate for decades.
- Remote reboots – Device management platforms can reboot M2M devices remotely. M2M devices are typically deployed in a standalone fashion. End users may rely on services supported by M2M devices, but they seldom have direct access to these devices. If an application supported by a given device malfunctions, the device may need to be rebooted remotely.
- Remote diagnostics and troubleshooting – Device management platforms can help eliminate costly truck rolls to M2M device sites. They can provide vital insights into device performance by remotely collecting diagnostic data such as measured signal strength, reboot counts and network connection attempts.
- Security and integrity – Device management platforms can use signatures and security keys to ensure that device software is authentic and not compromised. These security schemes play a vital role in safeguarding the data collected by the M2M device.

Remote device management will soon become critical to any enterprise or government seeking to deploy a large collection of M2M devices. By building device management services into their M2M solutions, network operators will help enterprises and governments to lower operating expenses and avoid having to create customized solutions. These services will be an important enabler for network operators seeking to provide value beyond M2M connectivity.

DEVELOPING STANDARDS FOR M2M DEVICE MANAGEMENT

Most device management-related M2M functions are currently performed by OTT suppliers. These functions are usually built from scratch and tailored to specific devices, applications and verticals. Companies that can afford to support M2M will often hire integrators or developers to build these functions into customized solutions. But high customization costs mean that some functions simply aren't covered. These costs also leave smaller M2M players on the sidelines. Those who do invest in building device management capabilities into their M2M solutions often find it difficult to get reasonable returns on their investments.

Suppliers that serve vertical niche markets have little interest in changing this model or embracing open M2M device management standards. These suppliers see standards as a threat to their value proposition. But several industry initiatives — including oneM2M, Open Mobile Alliance Lightweight M2M (LWM2M) and Broadband Forum TR-069 — take a different view. They create standards that drive economies of scale by extending a harmonized approach to M2M device management across all verticals. They are also working to create standardized APIs that can support common M2M device management functions such as provisioning, configuration, firmware updates and troubleshooting.

The work of the standards groups illustrates the industry's desire for broader applicability. For example, the LWM2M standard uses lightweight protocols to simplify the management of low-cost or constrained M2M devices. These protocols minimize overhead to reduce the cost of cloud–device connections. They safeguard data by establishing secure encrypted connections. They ease the integration of constrained devices by supporting clients with small footprints and low resource needs. Finally, they provide device management functionality alongside data connectivity to ensure that M2M service providers can enjoy the benefits of remote device management without having to establish a second connection to each device.

Beyond the standards groups, the industry is taking action to develop solutions that can serve multiple M2M applications. Some industry players are complementing the work of the standards groups by making data available to more applications and stakeholders. Others are working to normalize data and apply common formats to it. Still others are working to create broadly applicable rules engines and realization tools. As described above, network operators are doing their part by seeking to standardize M2M device testing, onboarding and management processes.

Whether pursued by industry groups or individual players, efforts to create M2M device management standards will help the industry build horizontal solutions that can address many different use cases and verticals. Once all devices support the same standards, it will be much easier for M2M solutions to manage and communicate with them. There will be no need to build separate protocol plug-ins for each device type. The end result of standardization will be an overall reduction of device-related costs.

EASING ONBOARDING WITH INTEROPERABILITY TESTING

Continued progress on device management standards will help drive M2M across more verticals and into the mainstream. But the success of a given M2M solution will still depend on how quickly, efficiently and inexpensively devices can be brought on board.

Interoperability testing (IOT) is essential for ensuring that an M2M solution can reliably work with a broad range of devices. The IOT process ensures that devices behave as expected so that device management and business processes will have a consistent effect across all devices. Testing and certification processes must detect and address variances in the way standards are supported by devices from different vendors. Fast and reliable IOT can reduce device deployment and integration costs and allow for second sourcing where required. Moreover, it can allow network operators and device vendors to work together to bring M2M services to market faster and mix and match more devices.

Ineffective or insufficient IOT may create the need for costly point solutions and custom integration. Gaps in IOT may lead to future problems. A device that has not been thoroughly tested may work well for a time, but an undetected incompatibility may eventually cause a malfunction, with significant financial and operational consequences for large-scale deployments. In the auto industry, for example, manufacturers have recalled millions of vehicles to address software issues. Remote device management may have enabled manufacturers to upgrade the software over the air instead of having to pay for manual upgrades.

CONCLUSION

As the M2M industry extends its focus beyond niche verticals, efficient device management, onboarding and IOT functions will become essential. These functions will make more M2M services viable and encourage more consumers, enterprises and governments to trust and embrace M2M. At the same time, M2M device management standards will safeguard and secure M2M devices. These standards will also unlock new service opportunities by making it easier to harmonize, simplify and scale M2M operations to support billions of connected devices.

Network operators are well positioned to capitalize on these new opportunities and help bring M2M to the mass market. With platforms that allow them to apply their trusted remote device management expertise to common M2M functions, network operators will reach more markets, deliver more value to customers and generate more revenue.

ABBREVIATIONS

ALM	application lifecycle management
API	application programming interface
IOT	interoperability testing
LWM2M	Lightweight M2M
M2M	machine-to-machine
OTT	over-the-top
PAYD	pay as you drive
SLA	service level agreement
TR-069	Technical Report 069

Alcatel·Lucent