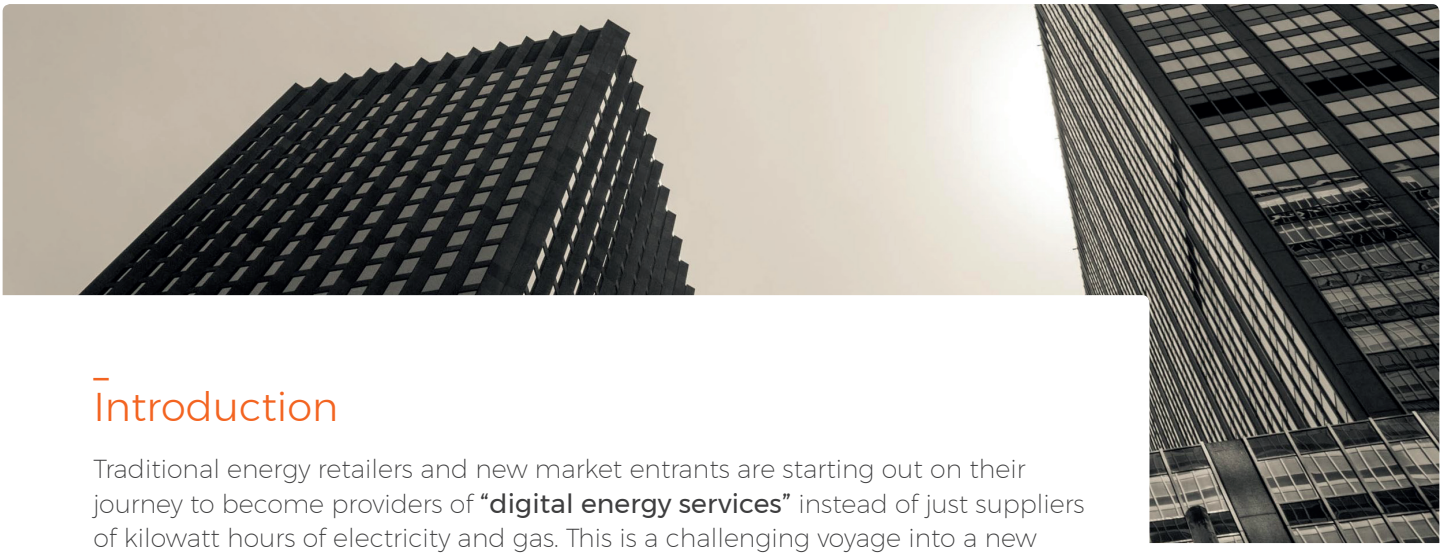
geo
smarter energy

Choosing the right technology platform for your journey into the digital energy services world



Introduction

Traditional energy retailers and new market entrants are starting out on their journey to become providers of **"digital energy services"** instead of just suppliers of kilowatt hours of electricity and gas. This is a challenging voyage into a new digital world of changing consumer habits and expectations along with rapidly evolving technologies at a time when the competitive environment in the energy industry is undergoing fundamental changes.

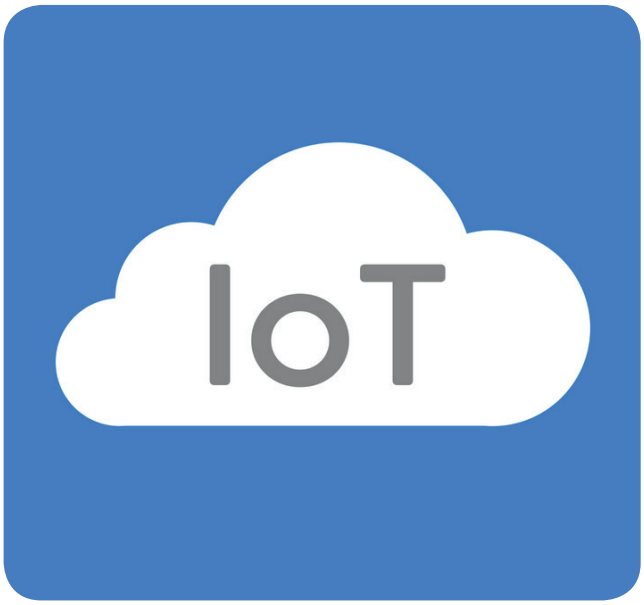
Choosing the right technology platform is a critical step in reducing business risk and maximising the chances of success through this transition. Digital energy services require a capable end-to-end solution which consist of in-home devices, cloud services and apps to capture data from electricity and gas meters as well as other sensors in the home. It also needs to transfer data to the cloud, transform it into useful information and feed the results into engaging consumer applications.

Despite years of trials and initial deployments, the market's understanding of the key success criteria for these enabling technology platforms is still limited. The approach of selecting technology for trials and hoping to scale it up for mass deployments is the core of the problem – just as you don't build a sky scraper by stacking storage containers, deploying a high-volume digital services platform is not a case of scaling up a pilot. As major blue-chip companies in other industries have found out at great cost, the challenges of cyber security, compliance with data privacy legislation, service quality, customer retention and building a sustainably profitable digital business are real. **Only by strategically selecting technology platforms that are built to deal with these challenges at "production scale" can companies be confident of success in this new world.**

This white paper aims to help companies entering the digital energy services market with their evaluation of such technology platforms by discussing these criteria, grouped into five main categories: **System Security & Data Protection, Logistics & Support, Meter Ecosystem Coverage, Quality of Service** and **Total Cost of Ownership.**

System Security & Data Protection

A digital energy services platform deployed at scale provides great opportunities in terms of customer engagement and recurring service-based revenue streams. However, unless it is built on a technology foundation that was designed to be secure and compliant with data protection regulations, its risk profile could be intolerably high, not only for the company providing the digital energy services but to the nation's energy infrastructure as a whole.



While most information technology professionals understand the principles of cyber security as they relate to cloud-based SaaS (software as a service) solutions, they cover only a small part of the attack surface of an end-to-end digital energy services platform. In-depth knowledge of the attack vectors associated with IoT (Internet of Things) devices, in this case the in-home device that collects meter information and sends it to the cloud, is much less widespread. However, as the Mirai Botnet incident demonstrated, a large installed base of permanently-connected and often badly secured IoT devices is a very attractive target for cyber criminals because it can be used to create powerful botnets. If a fleet of IoT devices provided by a single blue-chip company was hijacked in this way, the resulting reputational damage could be enormous.

Delivering security for an IoT solution requires an end-to-end secure design philosophy, supported by an information security management system such as **ISO 27001**, and regular penetration testing of key components.

Secure IoT devices will be designed and developed to the latest best practices in the following areas:

- **Operating System (OS)** – Good system design recognises that no OS is 100% secure and that any product vulnerabilities discovered may be exploited unless they are patched using firmware updates. The ability to update the device OS however creates opportunities for cyber-attacks, so validation of firmware updates to prevent malware injection and unauthorised 3rd party software installation is critically important.

- **IO Port, Bus and Physical Access** – Data that is of interest to hackers (including personal data or passwords) may be stored persistently on the device, so it is important that unauthorised users who have physical access to the device cannot obtain this data via hardware interfaces including UARTs, memory interfaces and JTAG interfaces.

- **Data Storage and Transfer** – Data stored persistently on the device should be secured by means of encryption and/or storage in hardened components. Transfer between system components and between the device and the cloud should use encrypted communications interfaces.

- **Security Certificates** – All access to and data transfer from devices should be protected using well-managed security keys and verification certificates with an appropriate cypher strength. Device-specific keys provide much

better overall security as one set of keys being compromised doesn't leave the entire device population open to exploits.

To ensure end-to-end security of the digital energy services solution, these secure design principles need to be mirrored in the cloud platform.

Cloud platforms should use the following security best practices:

- **Secure Perimeter** – The best way to secure virtual machines and other service components is to ensure they are not exposed to the public Internet. For system components that cannot be isolated fully, only essential ports and interfaces should be exposed. Secure IoT cloud platforms tend to use Amazon's Virtual Public Cloud (VPC) or similar approaches to provide advanced security features, such as security groups and network access control lists, to enable inbound and outbound filtering at the instance level and subnet level.

- **Access Control and Proactive Intrusion Detection** – Access to systems should be limited to authorised personnel and their access should be limited strictly to the level required to do their job and logged for forensic analysis in case of an incident. The use of powerful proactive intrusion detection technologies such as Amazon's GuardDuty ensures that any unauthorised access attempts are detected early on and made available for review.

- **Operating System Updates and Security Patches** – Any OS security updates and application patches should be applied in a timely manner to ensure old and newly identified vulnerabilities are not left open for exploitation.

- **Data Protection** – The cloud platform should only store data that is required for the provision of services covered by the contract between the relevant parties and with informed consent from the consumer. Personal data should, where possible, be physically separated from all other data or logically isolated using adequately strong encryption and appropriate key management.

In summary, there are many important system security and data protection aspects which all need consideration during the technology evaluation and selection stages, as well as on an ongoing basis while the digital energy services are operational. Security is a moving target, requiring continuous improvement through upgrading product designs with new, more secure technologies and approaches as they become available.

Logistics and Support

Rolling out any technology solution at scale requires an efficient logistics and support process. While this sounds obvious, these areas tend to get little focus during pilots and trials, introducing the risk that technologies are selected on functional requirements without proper evaluation of the accompanying logistics and support processes.

In terms of logistics, important aspects include not only the ability to manufacture products in volume with stringent quality controls but to have full traceability by production batch, device serial number and even components. This, coupled with a good reverse logistics process (product returns under warranty or for defect analysis), is critically important in the event of a quality issue – being able to narrow down any issue to affected units only significantly reduces the risk of a stoppage of all shipments or large-scale recalls.

For Internet-connected devices, the manufacturing and logistics process should also extend to the provisioning of devices for cloud access. This is best done using

"manifests" that not only track which devices have been despatched to which customer but also determine what a device should do when first connected to the cloud. A manifest-based provisioning approach provides the opportunity for significant cost savings and shorter delivery times through larger volume manufacturing and "late customisation" (e.g. delivering a device with generic firmware which is updated with the latest firmware approved by the customer upon first connection to the cloud) and has clear security benefits as only those devices that are explicitly white-listed can connect to the cloud platform.

Considering that digital energy services are usually aimed at improving customer engagement, satisfaction and retention, providing a great customer service experience should be a priority, not an afterthought. Providing quality customer support can quickly become prohibitively expensive for large projects unless the chosen technology platform was designed with quality, cost-effective customer support in mind. This is why **evaluators and buyers of digital services platforms should understand both the factors that drive the need for customer support** (such as the ease of use and reliability of the solution) **and the tools available to aid support agents in solving customer problems.** Digital energy services platforms should also help customers monitor and manage large numbers of devices in the field, through "fleet management" tools that offer operational analytics such as the number of devices that are actively connected, the firmware versions they run and any error codes generated. Without such tools, the company operating the services is flying blind and not able to proactively address issues or maximise its return on investment.

Meter Ecosystem Coverage

At the core of any digital energy service is the ability to access data provided by the home's energy meters. Given the wide range of electricity and gas meters deployed in the field, support for all the relevant meters cannot be taken for granted. While some smart meter specifications appear straightforward, there are often variations in meter behaviour due to inconsistent interpretations of the standards. Most smart meter specifications also allow for firmware updates, which means support for a specific smart meter is no longer a one-time validation exercise but a moving target requiring continuous maintenance and testing.

Full and reliable meter ecosystem coverage is especially challenging in Great Britain due to the sophistication and complexities of the GB Smart Metering Equipment Technical Specification (SMETS). Unlike most smart meter approaches, SMETS includes a smart energy Home Area Network based on the ZigBee Smart Energy Profile (SEP), designed to meet "the diverse needs of a global ecosystem of utilities, product manufacturers and regulators as they plan to meet future energy, water and gas needs". **With these technical opportunities comes a significant interoperability and testing burden, which only a small handful of providers have shouldered so far** (and even fewer will be able to maintain).

While it is fair to assume that smart meter ecosystems become more consistent and stable as the technology matures, there will be opposing forces such as the increased adoption of micro-generation, in-home batteries, electric vehicles and smart appliances and the emergence of residential demand management services that add new interoperability challenges in the home and in the cloud. With this in mind, it is important to take a strategic approach and look to the future when selecting a digital technology partner – simply focusing on meeting today's challenges without considering a partner's ability to evolve and thrive in this future world could turn out to be an expensive mistake.

Quality of Service

As digital energy services become the main interface between an energy company and its customers, the quality of the service provided becomes critically important. A high-quality service, delivered with consistency and a high level of accuracy provides a competitive advantage as it builds deeper relationships with consumers and discourages churn, while a low-quality service is likely to have the opposite effect.

Delivering a high quality of service starts with the basics of using a high-availability cloud platform designed for redundancy and scalability. The platform also needs to be monitored **24 hours** a day, **7 days** a week, **365 days** a year, with resources available to identify and fix any issues very quickly.

Mature digital services platforms are typically offered with a clear Service Level Agreement that spells out the provider's quality of service commitment. This usually includes a monthly service availability target of between **99.9%** ("three nines") and **99.99%** ("four nines"), with financial compensation offered in the form of service credits in case of under-achievement. While this high level of availability sounds attractive from a buyer's point of view, it generally comes at a cost and is hard to deliver in practice, so unless it comes with credible evidence of a supplier's ability to deliver, **actual consistent achievement of the Service Level Agreement goal should not be taken for granted**.

It is also important to bear in mind that quality of service is not purely a matter of IT operations delivery – managing hardware failures, handling software upgrades and generally running a cloud platform in a controlled and professional manner. Platform security is intrinsically linked to quality of service. A good example is a platform's ability to withstand denial of service (DoS) attacks. Unlike a typical website where only the user interface (or APIs used by the user interface) can be targeted by a denial of service, IoT solutions provide another attack surface: the interface used by in-home devices to send data to the cloud platform. **While the approaches that can be used to deal with a DoS attack on the former are generally well-understood, not all platform providers have a credible plan to deal with the latter.** Solutions that are based on devices that are programmed to send data to a hardcoded IP addressed data concentrator will fail in cases where that IP address is flooded by a DoS attack, and unless there is fast and reliable way for these devices to switch to a different IP address location that isn't under attack, the resulting impact on service availability could be severe and long-lasting. Even systems that make use of DNS entries are susceptible to this type of exploit, unless a public DNS resolver capable of resolving a large number of names to IP addresses is used.

Similarly, the ability for a digital energy services platform to block attempts at "device spoofing" is critical in delivering quality of service. If a rogue operator were able to trick the platform into accepting incorrect data, either from devices pretending to be legitimate ("spoofing") or by taking control of legitimate devices, the service provided is compromised, leading to huge potential reputational damage to the energy company providing the service.

24/7

platform monitoring

monthly service availability target of between

99.9

% ("three nines") and

99.99

% ("four nines")

Total Cost of Ownership

As IoT product suppliers and their customers are beginning to realise, the true cost of ownership of connected devices and services is much more than the initial purchase cost of the in-home device. In fact, there are clear indications that the lifetime "cost to serve" of a connected device is forcing some IoT companies, in particular those in low-cost product categories such as fitness trackers or data-intensive product categories including smart security cameras, to review their pricing or service offerings.

Total Cost of Ownership (TCO) is a critical success factor for the first wave of digital energy services which are focused mainly on helping consumers understand and optimise their energy use. The only proven route to market for high-volume adoption is a free-to-consumer model, typically funded by energy utilities. While most companies can justify the initial roll-out cost as a one-off marketing investment, they often struggle to justify the ongoing cost to serve unless it is reasonable and predictable. Too many promising projects have been cut short as a result of unbudgeted or increasing ongoing costs, and as a result haven't delivered the improved customer engagement they set out to realise.

Companies considering digital services technologies should consider two types of ongoing costs as part of their TCO due diligence, in addition to the cost implications of factors discussed above such as System Security & Data Privacy and Logistics.

The first cost type is cloud operational cost, which can vary substantially from vendor to vendor. Suppliers that designed their platforms for cost-effective operation at scale will have carefully considered how much data needs to be sent and how this can be sent most efficiently from the in-home to the cloud, simply because data volumes directly impact the data transfer, ingestion and storage costs which form a significant part of the overall cost of operating a cloud platform. For example, sending electricity readings once every **3 seconds 24 hours** per day is inefficient (each packet sent is mostly overhead with only a small payload) and unnecessary (the likelihood of a consumers wanting the see how much energy they are using in real-time at **2:00 am** is very low). The more considered approach of sending real-time data only when requested for an individual device and sending it in compressed periodic batches in all other cases can reduce the data volumes sent by as much as **5000%.** Other ways to reduce data volumes include using lightweight data protocols such as UDP instead of verbose alternatives such as HTTP, and compressing and packing data before transferring it from the home to the cloud. Economies of scale also play a major role in cloud operational cost, so providers that already have large numbers of devices on their platform will have a cost advantage over new entrants or competitors with less market traction.

The second type is the cost of providing customer support. Contrary to the assumptions of many companies evaluating digital energy solutions, this cost is influenced by many factors other than simply the reliability and quality of the technology. Smart in-home product design (such as including a display for showing diagnostic messages instead of just some LED status indicators which typical users won't understand without reading a manual) means fewer support requests, which is the best way to reduce support costs. When a support call is unavoidable, the ability for a support agent to diagnose and remedy the problem quickly is important – time is money, and the quicker the problem is solved, the better the customer experience. Leading digital energy services platforms therefore provide customer support teams with tools that aid with problem diagnosis and resolution.

TCO

Total Cost of Ownership

5000

% reduction in data volumes when sent in compressed periodic batches

Conclusion

Evaluating and selecting the right technology platform is a critical and multi-faceted task for any company considering an entry in the new world of digital energy services.

In our experience, companies approach this task with a narrow focus on technology and functionality, and end up making choices that are, at best, suitable for initial trials and pilots. We hope that this white paper highlights some of the common pitfalls and how to avoid them.

An early and comprehensive focus on **system security and data protection** is critical, as is the understanding that keeping any system secure and compliant requires ongoing attention and effort.

Successful digital energy services will be used by hundreds of thousands or even millions of consumers, and will typically include hardware devices, so it is important to consider the challenges of **logistics** (fulfilment, provisioning, etc.) as well as customer support. Great efficiency in this domain can make a solution, poor efficiency will almost definitely break it through poor customer satisfaction and unsustainable costs.

Because energy meter data is at the core of any digital energy service, the extent and quality of **meter ecosystem coverage** is a key success factor. It is important to bear in mind that existing smart meters are regularly updated and that new models are introduced regularly, so it's important to also consider whether the meter support provided by a technology platform is likely to be maintained into the future.

Consumer expectations with regards to **quality of service** are high, so consistently high availability of cloud service and app functionality is a must. In this area, the main pitfall to avoid is focusing only on the vendor's availability metric in the Service Level Agreement and not considering "worst case scenarios" such as a DDoS attack and how the platform would deal with that.

Finally, as with any mass market product or service, **Total Cost of Ownership (TCO)** has to be one of the main considerations, given that it will be a major determining factor in the return on investment assessment. Understanding the "T" in TCO is the key to success in this area – the total cost of providing a digital energy service ranges from the cloud operations cost (data storage, data transfer, etc.) to the delivery of hardware devices and providing customer support.

About the authors

This white paper was written by Rik Temmink (Chief Data Services Officer) and Adrian van den Heever (Chief Technology Officer) of geo, the UK's leading smart energy technology company. If you would like to explore the topics discussed in this white paper in more detail, please contact geo by phone on **+44 (0)1223 850 210** or by email at **marketing@geotogether.com.**