Privacy technology options for smart metering

A white paper by Dr George Danezis (Microsoft Research, Cambridge)

Overview

Electricity suppliers have traditionally held personal data about their customers: from personal details, payment details to quarterly consumption and bills. Proposed smart metering architectures in the UK mandate the next generation of meters to support fine-grained half-hourly electricity usage measurements. This level of detail represents a qualitative leap in the kind of information that could be made available to enhance electricity provision, improve billing and settlement processes, and provide added-value services to customers. It also could represent an unprecedented invasion into people's privacy and in extremis a customer resistance associated with privacy concerns could jeopardise or slow down smart meter deployments.

This white paper explores options to maximise the benefits all parties can draw from smart metering, while minimising the potential for privacy infringement. Our focus is on building strong privacy protections into the technology to support the data minimisation principle: only the necessary personal data should be made available to third parties. Terms of use, privacy charters, and trusted third parties have a role to play to ensure that the minimal data disclosed is further processed lawfully.

Implementing privacy technologies benefits all parties, compared with alternative approaches, such relying on customer opt-in / opt-out. The objective of privacy technologies is to provide functionality and benefits comparable with traditional solutions, where in which personal data is available to third-parties, without disclosing this data. In contrast, a privacy strategy based only on customers opting out of smart metering or collection of half-hourly readings impairs key functionality: time-of-use billing is not possible, settlement is less accurate, profiling for forecasting is difficult, third-party services are unavailable, and fraud cannot be easily detected. Privacy technologies enable these functions while at the same time providing strong privacy guarantees. An opt-in / opt-out option can complement them, but the incentives to opt-out due to privacy concerns are minimised (other issues such as sensitivity to metering or wireless equipment may still be a concern).

Architectures

Smart meter architectures require meters containing processors, local and wide area communication facilities. Furthermore support for security and cryptography is necessary to ensure the security of the meters and infrastructure. Privacy technologies make use of the facilities of smart meters to implement functionality without allowing detailed meter readings to leave a user's home.

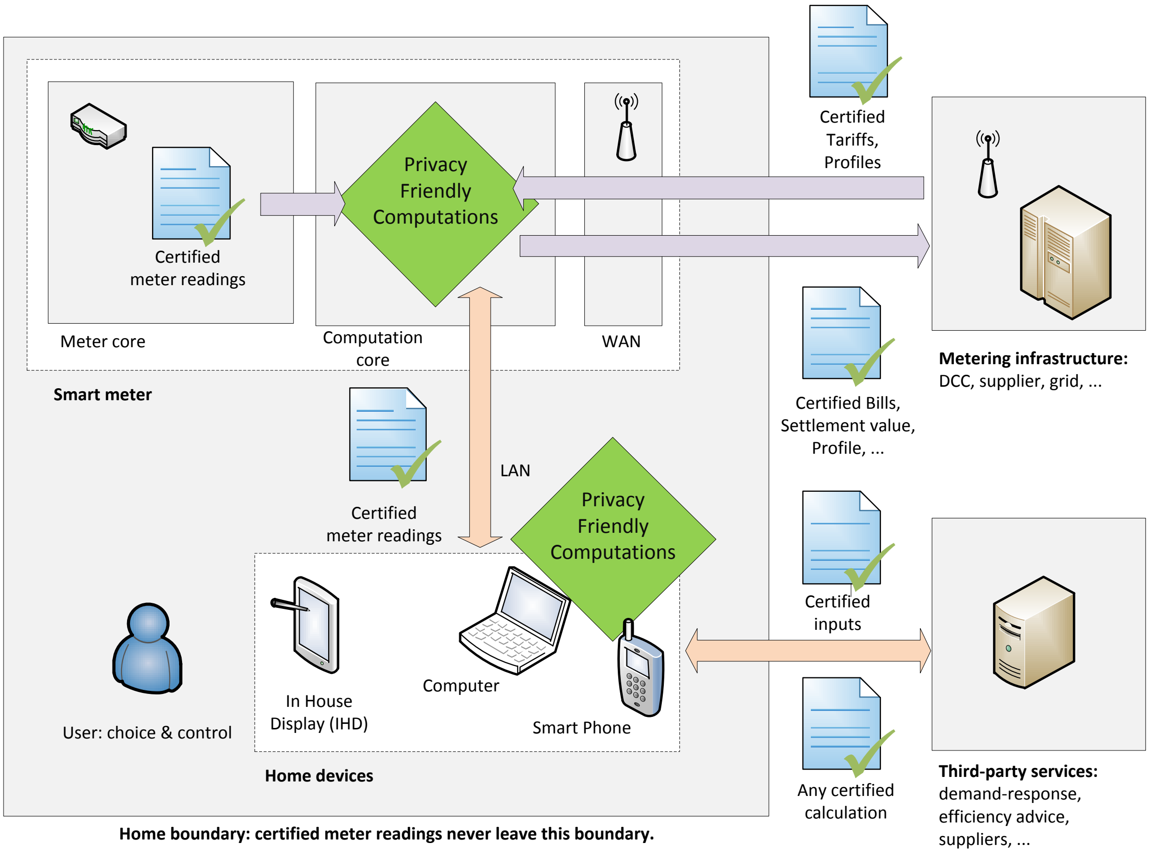

Figure 1. A schematic of a privacy preserving metering infrastructure

Figure 1 illustrates a sample privacy friendly infrastructure, for privacy friendly billing, accurate resolution of settlements, user profiling for forecasting, and third-party services.

- The **meter core** measures detailed consumption and other quantities of interest, and cryptographically certifies them. Cryptographic certification is similar to signing the meter readings with a meter key. Once readings are certified they cannot be forged, and they can be used as inputs for privacy preserving computations.
- The **metering infrastructure** facilitates communications between the meter and information customers, such as suppliers or the grid. It can also provide the meter with inputs for privacy preserving computations, such as tariffs for billing, the value of energy for settlement computations, or a list of profiles for forecasting computations.
- **Privacy friendly computations** are at the heart of a privacy friendly metering infrastructure. They allow certified readings and other information to be combined to compute arbitrary functions. These computations can be performed in the meter itself, or any other device (home computer, web browser, smart phone). The cryptographic nature of the computation ensures that the computed values will be correct. Any computation can in principle be performed, but common computations needed for billing, settlement, and profiling are extremely efficient.
- **Third-party services** rely on accurate meter readings to perform computations and provide services, such as energy efficiency advice, tariff comparisons, etc. They can use platforms such as smart-phone applications, social-networking applications, web-based applications, and traditional computer software to perform those computations on certified readings in a privacy friendly manner.

The privacy friendly architecture based on certified readings offers security advantages over traditional architectures beyond privacy. In particular readings made available to third party services though the local area network are certified, and can be used for operations requiring a high degree of integrity. A reliable and usable interface to output certified readings to the local area network future proofs the smart-metering infrastructure: as smart phones, computers and broadband connections become ubiquitous and cheap, it possible to leverage them to perform critical functions, such as billing. In-meter operations and WAN communications are still available to provide a utility robust backup infrastructure.

There are further security advantages in using certified meter readings for computations. The core of the meter certifying the readings can be very small, and cheaply certified and secured. Further computations based on the readings cannot be forged or manipulated. Thus other parts of the meter do not need to be certified to the same standard of security – tampering with the computations can be cryptographically detected. This provides a meaningful end-to-end cryptographic verifiability of the smart-metering infrastructure, keeping the operational security costs down and providing strong evidence in case of disputes between customers, suppliers or the grid.

In principle any computation can be performed on the certified readings, yielding a result that cannot be forged, while leaking no further private information. Some common families of functions are extremely cheap to implement within meters or other resource constrained devices such as smart phones. Those cheap privacy friendly computations form the core of privacy friendly smart billing, settlements and profiling.

Billing

Time-of-use tariffs are the most complex form of billing proposed relying on smart metering. It consists of different tariffs being applied depending on the time of day, day of week or day of year to the half-hourly customer consumption to determine its contribution to the final bill. All contributions are summed up to calculate a monthly or quarterly bill. Tariff structures – the time periods within which different tariffs apply – can be arbitrarily complex, and different between customers.

We compare different options for performing time-of-use billing, some with procedural control and others using privacy technology:

- An opt-in / opt-out option is a baseline protection: it means customers can choose to not be subject to time-of-use tariffs. It denies to those customers the ability to participate on the basis of privacy concerns.
- A trusted third party can be given the fine-grained readings and the applicable tariffs for the customer and asked to compute the bills. This third party can be integrated with the DCC or even be the supplier of the customer. The data has to be held securely, which represents significant operational costs. That party can still come under compulsion to reveal information. It is not clear users will accept this solution as being privacy-friendly.
- The meter can be entrusted to perform the calculation of the bill. The meter has to be aware of the tariff applying to the customer – this will likely be the case to facilitate energy management and prompt savings. The meter can then multiply the consumption of the user

with each applicable tariff and only send back to the supplier the value of the final bill. The full meter needs to be trusted to perform the computation correctly.

- The meter can output certified readings and allow any device to perform privacy friendly calculations and communicate the bill to the supplier. The meter itself could be entrusted with performing the bill calculations, and any deviation from the correct bill will be detected. Other devices such as smart phones or home computers can also be used to periodically update the supplier with an accurate bill.

The last option, using certified readings, provides most protection and flexibility. Performing computations using the raw readings and the tariffs in the meter is a fine solution from a privacy perspective, but relies on the absolutely correct functioning of the meter and its software, possibly raising their cost. Relying on procedural opt-in / opt-out makes it impossible to implement time-of-use tariffs and the weak protection offered by trusted third parties might be seen as insufficient by many users.

Technically the computation of a certified bill involves the selection of the correct tariff, a multiplication with the reading to determine its contribution to the final bill, and a sum of all contributions to determine the bills. The cryptographic computations required to ensure the correctness of the bill are of a similar complexity: multiplications and sums of large integers. Current meters are computationally capable of performing those operations in seconds.

Certifying a meter reading is equivalent in term of computation cost to applying a digital signature. Meters already are required to provide facilities for digital signatures and the same hardware can be used to certify the readings. The storage and communication requirements on the meters do not increase significantly. Any further computations and communications can be performed on commodity hardware significantly lowering their cost.

Settlement

The settlement process determines the fraction of grid production at any time that corresponds to customers of a particular supplier, and thus the amount a particular supplier should pay for electricity consumed by its customers. Currently, this faction is estimated according to the number of customers of each supplier and their profiles. In the future it will be desirable to enhance the accuracy of this process.

There are two ways to cast the settlement process in order to implement it in a privacy friendly manner. First, increasing the accuracy of the fraction of electricity used by a customer base per-half hour would increase the accuracy of the settlement process. This can be done though aggregation and sampling:

- A third party can be used to aggregate the fine-grained consumption of all customers per supplier, and only provide the aggregates to the suppliers and the settlement process. The key down-side of this approach is the need for a single party to have access to all the data.
- Sampling can be used to get increasingly accurate estimates of user consumption per utility: users are selected either at random or through incentives to provide detailed measurements of their consumption. Those are used to estimate the fraction of electricity used by all utilities for the settlement.

- In order to avoid any bias all users may be required to offer a sample readings at random, for example 1 in 100 readings (equivalent to 1 random reading every 2 days). This would greatly enhance the settlement process without requiring all measurements. Meters can be programmed to only send those readings to the suppliers or DCC.

A second technique considers settlement as a billing problem. Consider the problem of settling what is due by each supplier per month rather than per half hour: this is the sum of the detailed consumption of every customer, multiplied by the cost of electricity at the time of consumption. This is equivalent to the sum of the cost of consumption of all customers if they were billed on a time-per-use tariff corresponding to the cost of electricity.

We can extend the privacy friendly billing solutions described in the previous section to implement "penny-accurate" settlement mechanisms without any privacy infringement by third parties or even through sampling. Meters not only output the bill due using the tariffs that apply to the customer, but also output a normalised version of the total value of the electricity consumed by the customer in the same period (say per month). This is simply the detailed meter readings multiplied by an indexed value of electricity as determined on the grid. Suppliers can use those values, that are aggregated by customer over a month, and sum them up to determine the fraction of electricity used by those customers in that month.

Again there are advantages to using a privacy friendly scheme using certified readings for settlement. First, since it leaks no information about individual readings it alleviates any privacy concern users may have. Further it provides an extremely accurate settlement mechanism by calculating what is due by each supplier. Furthermore, the certified nature of the computation allows suppliers to convince anyone that the fraction is correct – eliminating the possibility for mistakes or any malicious manipulation. This is particularly important as the grid operator relies on the settlement values to charge suppliers.

As for metering the scheme is computationally simple, involving multiplications and additions of large integers. The certified readings used for billing can be re-used for the settlement calculations, thus incurring no additional cryptographic costs. Settlement calculations require a measure of value of electricity not normally available to meters, but easy to communicate through broadcast as it is global to the UK grid.

Forecasting & Profiling

Current settlement processes are based on profiling users, and using those profiles to estimate the fraction of consumption per supplier. Profiles of users are also useful for the financial forecasts of suppliers.

Two families of methods can be used to extract profiles for a customer population: sampling, and exact matching. They both share a common methodology for extracting profiles, through a group of volunteers, but they diverge in how they use those profiles against fine-grained meter readings.

The first stage of profiling is common to all solutions: a group of volunteers is monitored to extract consumption profiles. The smart metering infrastructure can be used to record and transmit the detailed consumption for extracting profiles, and this does not pose a privacy problem as long as they have actively agreed to being monitored. Procedural controls, such as stripping the names of volunteers before processing the data decrease the likelihood that their information might be compromised as a result of participating in this study. As a result of this initial activity a number of yearly profiles are extracted for different categories of users.

Given a number of profiles it is possible to estimate how well a customer matches a profile through correlation. Assessing the match of all customers to a set of profiles would allow an unprecedented increase in accuracy when it comes to forecasting. The correlation between customers and profiles can be uncovered using sampled data, or again using computations on certified readings.

Matching profiles through sampling is straight forward: meters are instructed to leak a sample of readings (again 1 in 100 would be equivalent to one reading every 2 days). Given those sampled readings users can be classified approximately as belonging to different classes. This is a statistical estimate, and subject to an error that depends on the rate of sampling and the regularity of profiles.

A second approach is to define a privacy friendly computation that takes as an input certified meter readings, and profiles, and outputs the probability or likelihood a customer belongs to each of the profiles. The technical details of these correlation calculations are very similar to billing – they involve mostly multiplications and sums. Thus they can be performed very quickly on meters or any other devices.

Being characterised by a certain profile may in itself be considered sensitive to users, and thus special consideration should be given to opt-in / opt-out even if a privacy friendly mechanism is used to extract those profiles.

Fraud

Fraud detection and prevention techniques can be applied to detailed readings to minimise criminal and dangerous activity. A key privacy friendly computation is available to tackle fraud: totals of energy consumption can be made available for certain periods of time.

Reporting aggregate consumption of the meter over a period of time is a simple but effective measure to prevent fraud. Aggregate consumptions from different customers on the same sub-station can be summed up and computed with the total electricity served in an area. Systematic and serious discrepancies may indicate fraud or a fault in the network.

A further fraud detection technique can be applied in a similar fashion to profiling: specific suspect profiles can be constructed and matched with detailed consumption records using privacy preserving computations. The result indicates the likelihood a user fits a suspicious pattern, and can be used to guide further investigations. Further steps could include an inspection of the premises or requesting more fine grained data from the meters.

Demand Response

Demand-response is a mechanism that notifies customers and their appliances of the load on the network or cost of supplying electricity. They may choose to respond by shifting their individual consumption to different times to reduce costs or as part of a contractual obligation. This is an important functionality to spread load and lower energy demand peaks.

Demand response requires information about the tariffs in place or loads on the network. It does not automatically benefit from accurate meter readings, and where it does those can be delivered directly from the local meter. Thus there is no specific need for any third-party, including suppliers, to access this data for this purpose.

A legitimate need for suppliers is to understand the elasticity of electricity demand at different periods for different customers. Profiling and sampling techniques, similar to those described above can be used for those purposes.

More complex demand-response mechanisms can benefit from advanced billing mechanisms. For example customers could be required to prove that their energy consumption did not exceed a certain threshold at specific periods of time. Penalties could then be applied for any unit consumed beyond that limit. Such non-linear billing models can be implemented within the framework of privacy friendly billing without revealing to third parties whether customers did in fact exceed any limits.

High value third-party services

The key environmental benefits of smart metering can only be delivered through customer engagement with their consumption and a radical change in usage patterns, taking into account the real cost of producing and delivering electricity. This involves shifting demand away from peaks, as well as implementing energy saving measures such as installing better insulation and investing in low-energy appliances. Both suppliers and third-parties have a key role to play in providing value-added services that help change energy consumption patterns – often assisted by personalised calculation on fine-grained consumption data.

The core functions required for suppliers to provide high quality provision of electricity rely, as we have seen, on cheap privacy friendly calculations. Any computations involving mostly additions and multiplications can be performed and certified on meter readings with very little effort. Many value-added services can also rely on such calculation, as well as more complex computations.

Added-value services may need to perform more complex calculations to provide service:

- Meter readings of other certified information can be used as keys in lookup tables.
- They can be compared to each other or public values to determine which is larger or smaller.
- Arbitrary non-linear functions can be applied to the readings of aggregates of readings.
- The results of all these functions are certified, and cannot be forged.

A fictitious use-case may illustrate the need for complex function, strong privacy and high integrity:

> *"In 2020 the government decides to create a monetary incentive to consume less electricity. For every KWh a household consumes daily below a threshold, it is eligible to receive a fraction of a penny that grows progressively as the energy savings grow"*

In this example the computation is not linear, as a progressive rebate is proposed (the more is saved the higher the rate of the incentive). Furthermore high integrity is needed to ensure the government is only rewarding for actual savings in energy consumption, and to avoid fraudulent claims. Finally privacy is necessary as citizens may be dissuaded from participating if their detailed energy consumption is necessarily disclosed.

Other high-value third-party services can include incentives to add insulation or change old equipment; or matching reductions of energy savings with monetary rewards. In those cases the third-parties can only provide those services if a high degree of both integrity and privacy can be guaranteed through private computations on certified meter readings.

A privacy infrastructure with simple meters

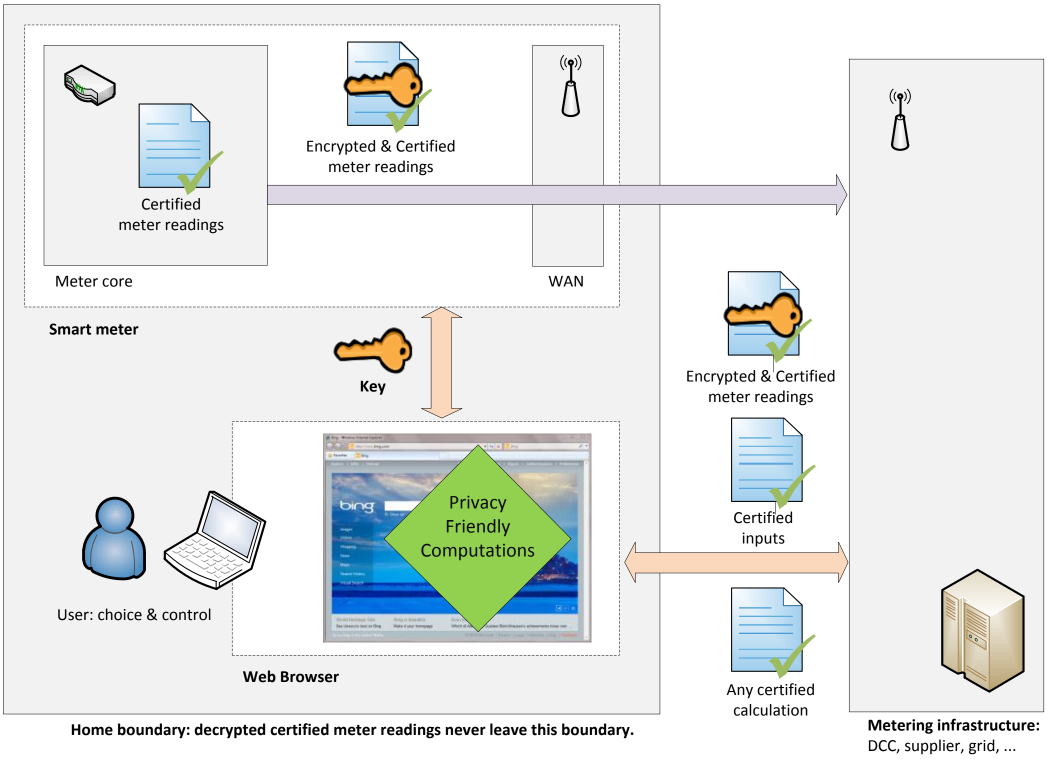

Figure 2. Delivering advanced functionality through reflecting encrypted meter readings.

The UK energy retail industry has indicated that “utility robustness” is a key priority when implementing a smart metering infrastructure. This means that processes necessary for the correct functioning of energy supply should not rely on customer equipment outside the control of utilities such as a broadband connection or computer equipment. In that respect relying on smart meters to perform privacy friendly calculations is necessary.

On the other hand many benefits of smart metering could be achieved for a lower cost by allowing an extremely user friendly and streamlined experience on commodity hardware and software: smart-phones, and common web-browsers. This would allow privacy friendly, thus widely accepted, advanced functionality such as time-of-use tariffs and exact settlement, without any major modification to the meters and the data flows into the meter.

Figure 2 presents such an architecture, where no data has to flow into the meter, but where occasional user engagement is required to benefit from advanced functionality:

- The **meter core** produces certified meter readings. These are signed and cannot be forged. They are suitable input for privacy preserving computations. These certified readings are encrypted and sent to the **metering infrastructure** (the DCC or the supplier). Due to the encryption they are not readily readable.
- A **key** is made available to the user through the documentation of their meter, a label or a display on the meter, or the in home display of the meter. This key can be used to unlock the detailed meter readings. The key is in practice a short string of letters or and digits, like a serial number of a subscriber ID.
- The user, though their **web browser** or any other connected device (such as a smart phone), accesses a service managed by the supplier or another party in the smart-metering infrastructure. The service seamlessly provides the encrypted readings, and any additional information necessary to perform a privacy friendly calculation. The user is required to enter their key, which unlocks access to the data within the application or browser. The privacy friendly computation can be performed within the web-application and its certified results are sent back to the supplier, the grid or any other third party service that relies on it.

Due to the cryptographic protections guaranteed by the privacy friendly computations, no information is revealed beyond the result of the computation, while it is impossible for customers or their equipment to provide incorrect results. The detailed meter readings are decrypted within the web-application ran on the user's equipment, but as before they never leave the devices and premises trusted by customers.

The computations necessary for implementing billing, settlements, profiling as well as a wide range of services in this manner are simple and efficient enough to be performed by technologies readily available within today's browsers or mobile devices (Javascript, Microsoft Silverlight, Oracle Java or Adobe Flash). No modification to browsers is necessary for delivering services in a privacy friendly manner.

The user experience is very similar to the current experience of login into a supplier's web-site to manage their account or to check their billing information. The key can be made short and easy to extract from the meter or the in house display. Instead of a computer generated key, a passphrase can be input into the meter or a security token could be used for high security settings – such as electricity supply for military installations.

The benefit of this architecture is that meters do not need to know any of the additional inputs necessary to perform privacy friendly calculations, such as customer tariff schemes for billing, value of energy for settlements or profiles characteristics to support forecasting. Those can be delivered to users through commodity networks, integrated with appealing value-added services. The downside is the requirement for the minimal user engagement necessary to visit a web-service or download a mobile application, and priming it with the meter key. This can be seamlessly integrated into their user experience of visiting their supplier's site or any third party service advising them on energy consumption.

Careful auditing of applications is also necessary to ensure they do not leak any information about meter readings. A clear statement that storing or misusing these codes is a serious breach of privacy might be necessary. Software verification techniques can readily be used to audit web-applications to ensure raw meter readings are never leaked.

A rich eco-system of web-service providers that compete in terms of added-value, service quality and privacy would be welcome. The integrity guarantees provided by privacy friendly computations enable such a market for application providers even for core services like billing and settlement computations.

Meters, infrastructure & costs

The privacy options discussed require minor software modifications to the current meters, but no additional hardware. Smart meters already implement cryptographic functions for security and privacy: they are required to encrypt data in transit between meters and the infrastructure, and in some cases are required to provide integrity through signatures. The same hardware and software components providing those services can be used to implement privacy friendly computations. Current estimates indicate that both certifying and encrypting readings, as well as performing billing computations should take in the order of magnitude of a few seconds on commodity smart meter hardware (ARM7 or ARM9 processors). The communication overhead for certified readings is minimal.

In case the meter is relied upon for performing the privacy-friendly computations further software and communications modifications are needed to get access to all inputs necessary. For example, to perform billing within the meter the applicable time-of-use tariffs must be available when the billing period ends (not in real-time). Similarly to facilitate accurate settlement processes the value of energy should be made available to meters – this could be done through a broadcast channel as it is common to the whole UK. Other applications, such as profiling, are more data intensive,.

The architecture with simple meters does not necessitate any data to be input into meters. It requires meters to output encrypted certified readings though whatever WAN channels are available. A software modification is necessary to communicate a key to the user, or a procedural method can be used for this purpose such as printing the key on the meter. Key that cannot be changed offer a lesser degree of protection, as changing tenants or home owners might be able to decode previous bills.

The way forward

It has been recognised that privacy concerns are a challenge for smart meter deployments, but current practices do not fully integrated the potential for privacy technologies. Without privacy technologies options are restricted to providing an opt-in or out-out, which denies the benefits of smart metering. Merely relying on trusted third parties holding and processing data is unlikely to convince privacy-sensitive customers to participate. Privacy technology options allow the best of both worlds: equivalent functionality to having access to the full detailed readings for suppliers and the grid, as well as very strong privacy guarantees for the users.

Two architectures have been presented to perform privacy friendly calculations for billing, settlement and profiling. The first relies on meters performing calculations, while the second relies on consumers engaging with the energy process at a minimal level using their networked devices. Both are feasible on current hardware, with simple modifications to the software. Further options, such as sampling and trusted meters, have been discussed to tackle specific information needs, but those offer neither the precision nor the privacy protection offered by privacy friendly calculations on certified meter readings.

Beyond the needs of supplies for high quality data to perform billing, settlement and planning the availability of certified readings opens the door to privacy friendly high value third party services. The fact that calculations on readings can be certified means they can be integrated in third party software and platforms. Thus they can become part of the every-day information fabric of devices and services already used by customers, fostering a deep awareness of energy consumption necessary to reduce energy wastage.

More information

Project webpage:
http://research.microsoft.com/en-us/projects/privacy_in_metering/

Technical Report: Privacy-Preserving Smart Metering
http://research.microsoft.com/apps/pubs/?id=141726

For more information contact Dr George Danezis (gdane@microsoft.com)