# The Foundation for Information Policy Research

## Consultation response on license conditions and technical specifications for the rollout of smart meters

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We have a number of comments to make on the consultations on rollout obligations and on privacy and data access[1]. Our overall analysis and concerns are described succinctly in the attached paper[2]. Here we tease out the specific implications for the consultation on the rollout of smart meters.

1. It is probably not feasible to complete the rollout by 2019.

2–7. The most likely reason for failure is that the DCC project cannot be completed on time or at all. However, even so, managing the evolution of smart meters over time will be a complex task and will need appropriate incentives as well as a regulatory framework.

8–10. Interoperability has to be done in the right way. One approach might be for the UK to be a late adopter; let the smart metering technology package be refined in other member states and then set hard standards in, say, 2015. Given ministers' desire to start the rollout before the next election, that is probably not viable – especially in respect of communications with the HAN. We reckon the best way forward is for an Open Home Controller to be developed as described in the attached paper. The controller will act as the gateway between meters, appliances and the head-end; it will be developed as an open project along Apache lines; and dispute resolution will become a matter for the governance mechanisms of this project.

11–12. No comment.

13–14. We believe that the UK decision to be the only EU Member State to include gas meters in the smart metering programme was an error, of which ministers should recant.

[1] See our consultation response on Smart Meter data access and privacy, http://www.cl.cam.ac.uk/~rja14/Papers/fipr-sm-privacy2011.pdf

[2] http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf

15–16. No comment.

17–19. Both the reliance on an In-Home Display, and the requirement to provide one, are misguided. Most households will want to interact with their meters, appliances and energy suppliers via the web, and thus the critical questions are how the web server will be maintained, and where it will be hosted. An Open Home Controller project is required to build and maintain the critical software for the web server. Once this exists it might be hosted in a home appliance (such as a router or communications hub), at an ESCO, at the retailer or even at the DCC. The idea that this server could be hosted at the IHD is naïve, as the IHD will be a low-cost battery-operated device that will not have sufficient compute power, or connectivity, or upgradeability.

20–23. No comment.

24–25. See above: the critical missing piece of architecture is how the meter, the HAN and the back end talk to each other and to the customer. We refer to this (following CEER) as the Open Home Controller. If DECC cannot get the architecture right, the whole project is likely to founder; architecture is policy. What the architecture must deliver is a platform for innovation, so that ESCOs, appliance vendors and others can build and participate in a vibrant market for demand-response devices and services, without this being crushed by retailers or other incumbents.

26. The fundamental problem is that the security mechanisms must mitigate real threats (such as abuse by strategic adversaries of the remote disconnect facility) but must not be capable of being abused by incumbents so as to exclude new market entrants. For example, it will not be acceptable to adopt the BSI Protection Profile for metering gateways as this specifies that meter communications are not merely signed but encrypted, rendering them inaccessible to the Open Home Gateway.

27–28. As noted above, the governance arrangements will have to foster innovation as well as preventing malicious disruption. We're not convinced that DECC is following a sustainable path.

29. No comment.

30. There must be a hub for the meters to talk to the HAN, the head-end and the customer, as noted already. However if this is simply made a regulatory requirement we can expect a minimally-compliant piece of equipment that will be used by incumbents to exclude new market entrants and stifle innovation. If this happens, the smart metering programme will not meet its objectives; rather than fostering energy saving by making consumption salient and creating a market in demand-reduction and demand-response technology, the program will be captured by the retailers who will operate the meters and used to continue the business-as-usual of confusion pricing.

31–33. The smart metering infrastructure must not be used for outage detection, voltage measurement or anything else to do with the DNO's responsibilities. Abusing it for this secondary purpose would be provide little of value while increasing project complexity, making failure and delay more likely. This functionality (if the DNO wants it) should be provided by feeder meters in the substation. There may however be a much stronger argument for having the smart meters provided and maintained by the DNO as this would make switching easier and also reduce the cost of capital, as DNOs are heavily regulated bodies and largely financed by debt.

34–35. The communications hub may be the best place to host the Open Home Controller. In that case (in fact in any case) it should not be in the meter, or intimately bonded with it; it will need to be upgraded frequently to deal with ever more appliances on the HAN, and ever more complex requirements for user interaction.

36–40. This is wildly unrealistic, for several reasons. First, the international standardisation process doesn't move that quickly. Second, this is not just about physical-layer interoperability or even messaging protocols, but about application-layer issues including APIs and command languages – in short, syntax and semantics. Third, all this is going to develop constantly as markets for demand-response appliances and services do. Fourth, the major appliance vendors have their own proprietary protocols and interfaces; while one of them might win out in the end, that won't be decided by ISO or IEC, or even by HM Government. That is why the Open Home Controller will have to be able to interact with multiple types of equipment. It's also why it has to be an open project. Else if (for example) the OHC is software running on a Cisco router in my front room, and I buy a new freezer from Samsung, how can I expect Cisco to write the software to talk to it, without risking being sued by Samsung for some IP infringement? To make this work, there has to be an arrangement whereby (in this case) Samsung contributes to necessary drivers and communications modules to a shared codebase, along with the necessary IP licenses, so that Cisco can ship this with its next upgrade. This kind of mechanism is fairly well understood in the software world, and the appliance and meter vendors are going to have to learn it.

41–42. DECC must get away from the idea of a single proprietary communications solution. This will lead to massive lock-in whose consequences will range from obsolescence to high costs. (The NHS network should serve as a warning; GPs' surgeries pay much more for network connectivity than neighbouring businesses.) Even at the outset, it's a matter of practical necessity, as GPRS cannot serve all households. Many premises may end up putting smart meters on a general-purpose network, such as a business LAN or domestic wifi. The link between the communications hub, or Open Home Controller, may have to deal with DHCP and firewalls and even traverse a VPN.

43–45. As with 31–33 above, these are gold-plating which must be avoided.

46. As already stated, what's needed is an Open Home Controller that will talk to the meter, the HAN, the headend and the customer. This is the key part of the architecture, not a frill that geeky customers can buy specially. That route won't work

as no-one will have the incentive to develop systems for a platform with less than 1% penetration.

47. Again, this is classic gold plating and must be resisted.

48–49. The translation cannot be done at the DCC. Suppose I invent a new demand-management device – say a washing machine with a red button on the front for “do it now” and a green button for “do it later when it’s cheaper”. Where in the system will the support software for this be run? Will I have to persuade the minister to order the DCC to upgrade their systems? If so, every energy startup will need millions for lobbying costs, and will face a delay or years; the prospect of green innovation by UK industry will be sharply reduced. Much the same goes for doing the translation at a communications hub if it’s integrated with the meter: then I end up having to persuade three meter vendors to roll out an upgrade, possibly across Europe. The metering industry isn’t like the PC industry; it doesn’t do monthly software upgrades. That’s another reason why we need an Open Home Controller.

50. The IHD is pointless. People will not want to go into the hall to look at a widget; they’ll want the data on their laptop, or iPhone, or iPad, or Kinect, or whatever the *device du jour* happens to be. The middle classes (who burn most of the electricity) may be particularly reluctant to even display in their homes a device issued to 28 million households, including most of the nation’s welfare claimants.

51–52. Bear in mind that the energy retailers live by confusion pricing, for the same reason as banks and telcos, so they will have a strong incentive to design credit tariffs that are not compatible with the IDTS tariff table. Making credit balances available to customers is a good thing, of course, but will require direct regulation.

53. We would like to see the development and specification of a standard tariff description language that would have sufficient expressive power that all retailers might be required to express their tariffs in it. It would apply a finite state machine to the meter database and return a tariff; it would be more general than a tariff table. This could solve a number of problems, including the visibility of credit balances referred to in the above answer; it could also solve the fundamental privacy problem, namely whether the customer must be compelled to supply all her meter readings to the utility, or merely a signed statement from the meter of the data that are precisely sufficient for calculating the bill (plus perhaps signed statements to other regulated principals such as the DNO and Ofgem of the data required for their regulated functions).

We would also like to voice the concern that the security work described in the Industry’s Draft Technical Specification is deeply unimpressive. A security engineering exercise on a project of this scale, complexity and criticality cannot be accomplished properly with a few cut-and paste recitals. It should start from a threat model, proceed to a security policy, and then be refined into targets. In the very first requirement, for example (SP.1) we read that ‘Non-security functionality on Core Devices and Systems, if compromised, shall not affect the overall device or system security functionality.' Now consider the following: does the meter tariff count as security functionality? We get the impression the authors don't think it does. Yet if an attacker can set the tariff to an arbitrarily high value, he can deny service, at least to over a million prepayment customers; by any stretch of the imagination that's a security failure. Before designers can start to reason about issues like these, terms such as 'security functionality' have to be carefully defined. What are we trying to protect, and with what? What's the Trusted Computing Base? Yet the authors of this document rush ahead and write down all sorts of requirements without thinking what they're trying to protect, and against whom. The quality of the drafting is also extremely poor – SP.9 has typos while some points are repetitive (e.g. SP.10–12).

54. As stated above, the current framework is not satisfactory as it omits a key part of the architecture – the Open Home Gateway. A device or system like this will be a requirement for interoperability between multiple types of meter, appliance and user client.

55–56. We will need a combination, including

- classical testing and accreditation of critical components such as metrology and communications
- governance arrangements for the Open Home Controller software platform, which might usefully be modelled on those of the Apache Software Foundation
- a market-led approach to the development of dmend-response appliances and services

57. Some positive action will probably be needed by DECC to get all this underway. With luck the Department might nudge industry principals in the right direction by exhortation but that might not be enough.

58–62. The communications between smart meters and the DCC will typically have to be authenticated, and meter readings on which utilities rely for billing will probably have to carry digital signatures. Encryption is probably not necessary for most traffic (and encrypting readings from the meter to the DCC would prevent the Open Home Controller from reading them). Other communications security issues include the API security of the meter interface and the management of keys, particularly if keys that authenticate prepayment commands have to change when customers are handed over from one retailer to another. The design of this cryptosecurity architecture is a highly-skilled job and we have little confidence that it will be done properly if handed to a single contractor, whether in the private or the public sector (organisations that understand cryptography tend not to understand meters, and vice versa). In fact we find it slightly alarming that DECC poses the simplistic consultation questions in 60–62: the architectural issues are much wider, deeper and more subtle than that. As for letting DCC control all the keys, that would introduce a single point of failure; it would be more incentive compatible for meter vendors and energy retailers to manage the keys on which they rely (and we've written about some of the options in our paper

‘Who Controls the Off Switch?’[3]) Above all, it is vital that the design should be open and subjected to rigorous peer review, in the hope that all the critical bugs can be found and fixed in advance of large-scale implementation.

Professor Ross Anderson FRS FREng
Chair, Foundation for Information Policy Research
October 13 2011

[3] http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf