POWER TO THE PEOPLE!

SMART METERING as one of the cornerstones of a sustainable 21st century infrastructure

By

ANDREW HENDERSON,

CONSERVATIVE TECHNOLOGY FORUM

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Contents

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Foreword by Ian Taylor

First I would like to thank the Conservative Technology Forum for the work that it has done to produce this paper. In doing so they have highlighted the shortcomings of the previous policy approach and presented a pragmatic and intelligent way forward for smart metering.

Secondly it has highlighted that smart metering is but one aspect of the UK's energy policy. Smart metering alone does not cut the mustard. I look forward to further policy documents on the smart grid and smart infrastructures which will complement this policy. Moreover the work that is being done by the CTF on broadband completes the infrastructure policies that will help to keep the lights on in the United Kingdom. It also shows the importance of cross-departmental efforts as our broadband policy sits with the Department of Culture, Media and Sport under its Minister, Maria Miller. Smart meters are only smart if they empower the property owner to regulate usage of energy and control equipment. The energy companies initially thought all that was needed was their ability to read usage remotely. Fortunately many new innovative applications are becoming available to owners through wider integration of meters and sensors in buildings.

Thirdly, we have a golden opportunity to lay solid foundations for the next phase of the UK's energy market now. Demand for energy is both a bellwether for the economy as a whole and is also linked to our economic security. Thomas Hicks, Deputy Assistant Secretary of the US Navy for Energy, stated earlier this year that "energy security **is** national security". That statement is just as valid for the United Kingdom as it is for the USA. Predictable and affordable energy is also good for both the consumer and for business, smart metering has a crucial role to play in achieving this. For many years energy policy has been a top-down one which allowed the producers and suppliers to control the market. The consumer has been passive and, unless they happen to be a large industrial user of power, unable to monitor closely what they use and buy from different sources. Energy in that sense is a commodity that could be bought from different supply sources as well as suppliers. It could also potentially be traded not just by a small group of large suppliers but also, through micro-generation, by individuals. This would secure our supplies by making the sources so diverse and it would also bring into the market a healthy dose of both choice and competition.

I would thus like to see smart meters help us avoid a vicious circle of increasing reliance on primary fuels sourced from unstable suppliers and ever increasing energy prices. Instead I would like to see smart meters help to create a virtuous circle whereby through the exploitation of Britain's indigenous renewable resources our energy security and supply are decoupled from the global market, and a shift to low carbon technologies in our homes provides the ability to match demand to the available supply – creating a virtuous circle that delivers energy security, affordability and helps us to meet our climate change commitments.

Ian Taylor

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Ian Taylor was Science and Technology Minister in the mid 1990s and later chaired the Parliamentary & Scientific Committee. He has now left the House and is Chairman of Living PlanIT SA and on the Science & Technology Facilities Council.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Introduction

"Owing to past neglect, in the face of the plainest warnings, we have entered upon a period of danger. The era of procrastination, of half measures, of soothing and baffling expedience of delays, is coming to its close. In its place we are entering a period of consequences." Winston Churchill.

The UK faces multiple crises after a decade of failure to invest in maintaining our existing national infrastructure let alone re-building it for the 21st century. In the immortal words of Liam Byrne in the note he left behind in 2010 "there's no money left".

The current smart meter programme came about because the Labour Government rejected the proposal put forward in 2006 by Sustainability First : http://www.sustainabilityfirst.org.uk/docs/2006/smart%20meters%20pdf%20version.pdf

for deregulation to permit a major industry-led trial to test the benefits and business case for smart metering. Their priority for those suffering "fuel poverty", who were perceived to be unlikely to benefit from a purely market-led solution may have been admirable. The consequences have been the opposite to what was intended. Had that trial gone ahead we would almost certainly have been well into an incremental roll-out prioritising those who stood to benefit most (whether business or consumer) and would have been in a leadership position in the smart meter sector. That would almost certainly have also put us in a position to deliver real benefits (not just "priority") to those least able to pay rising energy costs.

Instead the DTI, later BERR and DECC set about planning an exercise to provide theoretical benefits to all. When the "business case" was found to be missing the numbers were re-worked and linked to the centralised, top-down, command and control approach to energy supply envisaged in Ed Miliband's 2009 Energy White Paper http://webarchive.nationalarchives.gov.uk/+/http://www.berr.gov.uk/files/file10719.pdf

The result was a policy with a built in "off switch" in every smart meter. Some might say that this exists to enforce energy rationing for all, (unless we see mandatory exemptions for those on benefits) because of the failure of the last government to encourage investment in generating capacity to replace that coming to the end of its life. However others would point out that this functionality was built in and lobbied for by consumer groups and industry as a step to help remove barriers to competition in the prepay energy market, improve customer service and choice of payment methods for all customers and drive down prepaid energy costs at a time when increasing numbers of consumers are switching to prepayment[1]. The current policy gives guaranteed roles for incumbent suppliers and regulators but fails to reward them for investing in improved efficiency in meeting customer needs, as opposed to meeting regulatory targets.

[1] (Consumer Focus/Accenture research - *Smart Metering Prepayment in Great Britain – Making prepaid energy work in a smart world* October 2012)

Whilst good work has been done looking at standards, investment is stalled because the "business case", whether for suppliers or consumers, remains uncertain. The CTF therefore seeks to address the failings of the current policy in a timely manner. We believe that a more market-led approach to deployment, with those segments where the benefits are highest and those customers who will save the most will be able to receive the meters first, must be at the heart of Conservative policy towards smart meters. That approach should also include, through appropriate fiscal incentives and obligations, those groups who would also benefit but might otherwise be excluded on grounds of cost.

The potential benefits identified back in 2006 probably remain good. Smart meters can be a means of giving choice and control back to customers rather than suppliers. Consumers should be able to cut their demand or to pay extra, dependent on their priorities, not those of their suppliers Market forces should be allowed to reward those who invest in meeting the needs of the future.

However it is recognised that market forces will not necessarily deliver energy savings for all consumers. Thus prepayment customers are less likely to see significant energy saving benefits from smart meters because they already have visibility over their energy use and tend to be more energy efficient due to budgetary constraints. Some customers have little discretionary load that they can reduce or shift to off peak times. Ofgem has recognised the challenges faced by particular customer segments to engage in the competitive market and select the right tariff for them. Unlike network-led rollouts, there are limited commercial incentives in place for suppliers to encourage **all** consumers to use smart meters to reduce their energy use and without reforms to settlement processes inadequate incentive to expand demand side response and management offers.

On the other hand smart meters (and their open inter-operability standards) are said to be one of the cornerstones of the 21st century infrastructures that will support smart homes, offices, shops, cities and inter-connected on-line services in a world of ubiquitous computing and the "Internet of Things". The others are smart grids, smart infrastructure, standards and ubiquitous broadband. They are, however, only cornerstones. They are not, by themselves, sufficient.

The central pillars of any infrastructure investment policy must be predictable fiscal and regulatory regimes which encourage and reward market-led investment. Open standards for sustainable inter-operability and competition, which enable failed operations to be readily transferred as well as customer mobility, are also essential to give investor confidence and preserve customer choice. So too are equitable market rules to give a fair return to those who took the initial investment risk if customers exercise that choice and change suppliers

The standards need to include not just those for technical components but for catalogues of physical assets (e.g. ducts and poles), operational processes (e.g. performance measurement) and business processes (e.g. service level agreement, monitoring and response) as well as security. One of the opportunities where government has a genuine role is to build on the

work to date on “smart meter standards” and to use this to help establish UK leadership in the setting of global standards.

Finally our policy will address the creation of jobs and how the smart metering policy can feed into an export led recovery. Not only will the implementation of this policy feed into UK-based jobs installing, servicing and maintaining the network of smart meters but it will also assist in creating employment in the exporting of UK-made smart meters. We also recommend a certification scheme for installers in the same way that gas fitters or electricians are now certified.

However, beyond the above roles, the challenge for the Coalition Government is to make it possible for failure of the all-regulatory approach used thus far to be compensated by a mix of market forces and targeted regulatory pressure such as the Operational Licence Condition to compensate for failure of the approach so far before we have to make use of the compulsory rationing system planned by Ed Miliband, turning off the lights and heating of those in most need because we put “priority” before “action”.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Proposed Conservative Party Policy on Smart Metering

This policy document has been written by the Conservative Technology Forum (www.conservative-technology.org/) and stems from a meeting on Smart Metering on April 24th 2012. It was also informed by the report of a meeting on the policy implications of "The Internet of Things" on 26th March.

The last Conservative Energy Policy document was entitled: "Rebuilding security: Conservative Energy policy for an uncertain world". That document, published before the 2010 General Election, had a number of comments on smart metering. It defined it as:

The smart grid *– Smart grid technology has the potential to cut energy bills, enable the electrification of transport and banish black-outs to the history books. Yet, once again, Britain is falling behind our competitors – many of which are already running large-scale demonstrations or have even begun nationwide deployment1*[2]*In Britain, the Government has announced plans to deploy smart meters by the end of 2020, a timescale of over a decade that is widely regarded as unambitious.*[3]

It then went onto state:
The deployment of smart grid technology will provide new ways of using energy more efficiently. For instance, smart meters will give consumers the information and monitoring tools to identify and act on energy saving opportunities. As well as cutting overall energy use, smart meters would make it easier for consumers to benefit from off-peak tariffs, thereby helping to smooth-out consumption patterns which would reduce the cost of peak supply across the network and generate additional savings[4].

Action point 9 of that document dealt with Conservative proposals for the rolling out of a smart grid which would do for energy what the internet did for information. In other words, the smart grid would enable consumer interests in the purchase of and use of energy to come to the fore. This would be done by setting a deadline for roll-out to most homes and businesses of 2016. Importantly there was a commitment to work with industry to ensure common standards *that enable smart meter support for microgeneration, electric vehicles and consumer-controlled automation of appliances and heating systems*[5] Standards have an important role to play in driving down the costs of technology by enabling competition in sourcing as well as creating resilience in the supply chain.

Moreover, this market is to be open through interoperability and to allow for cross-border trading. But above all, the aim is to ensure that the consumer has choice about what the options are for sourcing energy supplies and for accurate billing. One outcome of this is that, subject to appropriate supplier incentives being put in place, the consumer will be able to take advantage of new kinds of demand response tariffs including multiple rate Time of Use tariffs, critical peak pricing, and automation of appliances. As a consequence, peaks and troughs will be smoothed out and this will help to reduce the need to add extra capacity for

[2] The Economist, 'Building the smart grid', 4 June 2009

[3] Confederation of British Industry, Decision time: driving the UK towards a sustainable energy future, July 2009, page 14

[4] Page 26 Rebuilding security Conservative Energy Policy for an uncertain world.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

peaks as they are reduced, as well as overcoming the inflexibility of supply from some greener sources such as wind. This reduces the scale of the challenge of securing the required investment in our energy infrastructure

In 2009 the Conservative Party published a document in March of that year entitled "The Green Technology Recovery 2009". This called for the roll-out of smart meters as the third of 10 items requested for action from the then Labour government.

This document now seeks to take these policy statements further, taking into account market and legislative developments since the election in 2010. Roll-out has already begun of smart meters and engagement with industry is now advancing. In the background the economic crisis rumbles on which alters the investment requirements both of the Government and companies involved in this sector. This new policy document therefore seeks to set policy for the future, taking into account the lessons learnt so far, the economic situation and the fundamental requirements of the Energy Policy to protect supply and the give more choice to the consumer.

Definition:

What are Smart Meters? Smart meters are components or modules within a system (Smart Grid) that feeds data out from the consumer to the supplier. It is both part of the supply network and part of a business or home energy control system. There are a number of standards in place or being created to support Smart Meters. Examples of these are SMETS, DLMS or M441.

Future generations of Smart Meters should also enable the customer to control remotely sources and use of energy and should enable connection via sensors to electrical appliances and temperature controls within buildings.

The context for smart metering

Smart metering needs to be considered against the background of the current political and economic situation. Demand for energy is set to rise as illustrated by the graph published by DECC in 2010[(5)]. There are very real fears of power demand outstripping supply within the next few years leading to a need for centrally controlled rationing. The challenge is to abate the rise in power demand – through improved efficiency (using less energy), changing when energy is used (reducing or spreading peaks and aligning these with supply (e.g. when the wind is blowing). The ability to handle peaks in demand drives most investment in generation, transmission and distribution infrastructure. Spreading demand should enable a reduction in the capacity needed and improve the return on capital under traditional investment models. This is what Prof Goran Strbac of the Centre for Sustainable Electricity and Distributed Generation calls the "Predict and Provide" model of energy generation[(6)] . This leads to large differences in capacity and utilisation between peak, minimum and normal usage rates. This difference enables, for example, the Swiss to run highly profitable operations, buying off-peak electricity from France to pump water uphill to flow back downhill at times of peak load, generating power to sell back to France at several times the price. The value of fine tuning such operations and making better use of hot standby (e.g. gas) generation capacity by deploying smart meters feeding timely information via the distribution networks (so called 'smart grids') is a large part of the business case for the proposals inherited from the last government.

The run down of Nuclear power and depletion of North Sea Gas means that the UK is no longer self-reliant with regard to energy supplies. The "dash for gas", both in the 70s and later 90s, fed by supplies from the North Sea gas and oil fields, has led us to be dependent on imports. Government policy may be to encourage the use of renewable sources of energy but until these come on stream (with unreliable sources such as wind and time dependent sources such as tide, linked to large scale pumped storage), that dependence will remain. Demand side reduction and management, which smart metering technology can facilitate could help to lessen that dependency.

But will the lessening be the result of customer choice, using less power at peak times when it costs more, or supplier imposed rationing (to optimise revenue from limited capacity within regulatory constraints)? And which type of regime will do more to encourage investment in additional capacity, whether innovative or traditional (counting hydro capacity linked to pumped storage as traditional, albeit little used in the UK for a variety of environmental, as well as financial, reasons)? The policy challenge is:

[5] Page 21 Rebuilding security Conservative Energy Policy for an uncertain world.

[6] What is the budget for being smart about energy? 10th November 2009, presentation to Intellect

- to establish a market where consumers will benefit from products and services that allow them to benefit from more affordable overall energy bills by allowing control of when non critical demand is taken.

- to deliver positive and meaningful choices for the consumer rather than a threatening vision of energy austerity.

- to create an energy services market which creates jobs and the technology innovations that would make the UK a world leader in this sector.

Technology changes affecting the scale and nature of both demand and supply

Technological developments in society, principally based around the rise in computing as both a business as well as a domestic activity have led to an explosion of electrical gadgets with consequent results on demand for power, estimated to double demand by 2050. Our economy has become increasingly dependent on computer power to operate which puts up demand for electrical power to run the machines that are necessary to modern life. There are many allegations in this space but little analysis as to whether the net effect (including of investment in standby generating capacity for the data centres and server farms to support on-line networks, centralised services and cloud computing) is to reduce volatility while increasing base demand. We are also seeing marked changes in the price / performance of micro-generation technologies which may change the cost of servicing rural communities that are currently seen as in need of cross subsidy. For all the talk of smart grids, most current thinking assumes a "norm" of distributing power from centralised sources as opposed to collecting it, other than from "contractors" who are to be compensated in the event of lack of demand.

The economic pressures on suppliers and customers, both public and private

The switch (under the Labour Government) from focussing regulating on price, competition and consumer protection to regulating return on investment has led to the problems anticipated when that approach was rejected by the Conservatives after the original privatisation. Most of the distributors were subsequently bought by EU utilities operators who are reluctant to undertake risk investment without political and regulatory certainties or guaranties which the UK government can no longer afford to give. That reluctance has been increased by the effects of the euro-crisis and of domestic policies on their parent operations.

Investment is therefore more likely from the residual UK-owned operations and new consortia backed by sovereign wealth and pension funds looking for secure, predictable, low risk utility returns, e.g. those underpinned by long-term customer contracts with business customers whose operations are critically dependent on resilient (as well as cost competitive) power supplies. These might well include social housing owners (seeking to better meet the needs of low income tenants) and the public sector (having to make cuts of 20 – 30% in overhead costs) as well as those building or operating on-line services, server farms, shopping malls and entertainment complexes.

Meanwhile we have entered an age of austerity with personal disposable incomes dropping by 10% p.a. and more. Underlying energy costs are rising on what seems to be a sustained

trajectory. Demand is inelastic with price and this has a disproportionate impact on people's disposable incomes, a vicious circle.

A smart metering programme which provides rapid payback to both customers and suppliers and the same time as reducing the need for imported oil and gas should be a win-win opportunity. It should also provide the opportunity, assuming we help take a lead in developing and working to world standards, to create large numbers of private sector jobs across the UK (not just in the South East) in the smart infrastructure businesses of the future. If we fail to act then increased population will lead inexorably to increased demand. In August 2009, the BBC reported a "perfect storm" of increased population combined with scarce resources leading to shortages in 2030.[7]

Smart metering policy under the Labour and Coalition Governments

As yet smart metering policy under the Coalition has been built on the assumptions made when Labour was in power. Whilst this document concentrates on the technological aspects of the policy, there are serious issues with regard to the accuracy of the figures put forward by Ed Miliband when he was Secretary of State for Energy and on which all subsequent calculations have been based.

The first three economic assessments of residential smart metering found that it would not pay for itself.
1. The Carbon Trust smart meter trial in 2004 found net disbenefit to smaller SMEs, and by implication to most residential customers. Government is still struggling to understand how it will deliver cost benefits to micro-businesses.
2. In April 2007 Mott Macdonald for BERR reported that smart metering is "heavily burdened by the high costs associated with replacing legacy meters and developing the comms infrastructure. Therefore it is not favoured in terms of overall NPVs". Their figures showed a net benefit of - £700m for BEAMA minimum spec over 40 years.
3. The April 2008 Impact Assessment (IA) Option 2a, for a mandated 10 year roll-out with in-home displays, estimated the net benefit at -£4.3bn.

In order to demonstrate that their figures made economic sense the previous Government held a review in May 2009, IA Policy Option 2, for a mandated roll-out by the end of 2019 under a centralized communications model, which predicted a net benefit of £3.6bn. In 2011 the Coalition conducted Assessments in March and August which were still more favourable with the latter predicting a net benefit of £7.2bn. One commentator on this process claimed that "the successive reworkings involved a reduction in costs, an increase in benefits, and stretch credulity given some of the assumptions".

The CTF does not believe the markets of today and tomorrow will support such a slow and uncertain return on investment. However, we also believe that they will support much cheaper, and simpler alternatives, which are not only more likely to succeed but will also delver greater benefits, much more quickly, which will also benefit low income consumers.

[7] http://news.bbc.co.uk/1/hi/sci/tech/8213884.stm

We are where we are because the last Labour government would not sanction a market-led solution.

The inherited policy introduced three areas of specific concern to the CTF. These also lead to potentially high (and uncontrolled) costs:

- The decision to require suppliers rather than DNOs to roll out smart meters. This runs counter to the way most EU countries have rolled out smart meters and has added costs and complexity. Frontier Economics' research implies that a network led rollout could result in a £1billion of savings.[8]
- A recent Which? commissioned report showed that the suppliers are largely distrusted; If the supplier community can re-build consumer trust then this will not be a show-stopper. Consumer Focus research[9] reported that only 24% of bill payers trusted their energy supplier to give them help and advice on cutting their energy bill and going green,[10]. However it also showed that consumer trust overall is low and suppliers were not far behind consumer groups in terms of trust.
- The proposal to include gas meters and an in-home display (IHD). It is vital to include gas metering as gas (for those homes that have it) makes up the majority of the home energy supply, and about half our cost and carbon. IHD units are more problematic. On the one hand New Zealand has demonstrated that the IHD is not economical Yet an ESMIG[11] study showed that Smart Meter rollout or pilots which included an IHD sustained an 8% saving over 2 years, on average.. IHDs should be seen as a great first step in the necessary journey of educating consumers about how energy bills are made up. Consumers who have experienced IHDs become more open to taking other steps.

  Consideration should therefore be given to the use of ancillary devices to display the smart meter such as smart phones or domestic computers. IHDs should be viewed as the first step along the road to smarter devices, just as there is a very varied market for mobile handsets ranging from smart phones to simpler devices aimed at target markets.
- The proposal to turn the communications and data collection operations into a large centralized and separately procured system. The UK market has a multiplicity of actors when compared with other EU markets. Where you have a multiplicity of actors, they usually favour shared infrastructure models. Sharing communications using, for example, the PSN standards and frameworks, could improve security and resilience and save most of the cost. Moreover a centralised database should make it easier for consumers to switch suppliers.

This policy document will present new policies that meet the above concerns and answer them.

---

[8] Less is more? How to Optimise the Smart meter Roll-out. Frontier Economics. January 2008. http://www.frontier-economics.com/_library/publications/Frontier%20bulletin%20-%20less%20is%20more%20stp.pdf

[9] Consumer Focus face to face survey 1460 UK bill payers between 29th March – 3rd April 2012.

[10] This was a face to face survey 1460 UK bill payers between 29th March – 3rd April 2012.

[11] http://www.esmig.eu/ also see Consumer benefits of smart metering - Results of the Empower Demand study, phase II by Dr Howard Porter 10/10/2012

Policy objectives and cornerstones

Policy objectives

This policy document builds on four key areas. Listed below as policy cornerstones. However, underpinning these policy cornerstones are five policy objectives. These are:

1. VALUE FOR THE CONSUMER. Conservative policy must ensure that smart metering maximises the benefit to consumers and that both monetised and non monetised benefits are realised. Fundamentally, smart metering should end estimated and inaccurate bills – a major source of consumer complaints; promote improved competition through faster and easier switching; enable more cost efficient and effective delivery of support to low income and vulnerable consumers; facilitate competition in new and existing markets such as smart homes, remote healthcare and pay as you go energy. It should enable consumers, both business and private, to control their own usage and obtain competitive tariffs and options so that they can make better use of the funds available for gas and electricity to the home or workplace. This is against a backdrop of increasing fuel supply costs due to higher levels of global demand and political / economic uncertainties in many countries that supply traditional fossil fuels. Government targets for replacing power generated by fossil fuels by renewables (wind, nuclear, tidal etc) should not be at the expense of consumers' ability to feed and cloth themselves or their children or of UK-based businesses to remain globally competitive.

2. VALUE FOR THE INVESTOR. Conservative policy must encourage those who have a choice between investing in the UK or elsewhere to choose the UK. It must also encourage those looking for a better home for their personal savings to invest in building the infrastructures of the future, instead of buying index-linked stock with a nominal interest rate, if any. That will in turn make the UK an attractive location for the businesses of the future, whether home-grown or attracted by political stability, workforce skills, reliable energy supplies and predictable costs and taxes. The Number One objective for the Government though is to bring predictability. The Solar PV debacle is an example of how a Government flip-flopping on policy can destroy trust in a very short space of time.

3. KEEPING THE LIGHTS ON. Conservative policy must ensure that smart metering assists us all to keep our lights on in the short and medium term. Smart metering is just one area of energy policy and must complement overall Conservative energy policy. One outcome of the successful implementation of smart metering should be that consumers can choose not only which tariff to use but when to consume and from what energy source. It should help them do their own time-shifting and (where practical) install their own alternative energy supplies. Thus, a consumer could chose to run their washing machine when demand is low or the wind is blowing or to install their own energy "storage" systems.

It will also create a market for energy services and innovation in the technologies that enable these services thus creating jobs for the self-same consumer.

4. CONTRIBUTING TO JOBS AND ECONOMIC GROWTH. Conservative policy should help create a market for the supply and installation of equipment and services which supports sustainable UK jobs. In particular this would develop leadership in the green technology sector. The potential market is both high and low tech, in terms of the jobs that it creates. High technology jobs will be created in the design and manufacture of smart meters (albeit many "meters" may be components in more complex "smart building control systems") and the applications that depend on them (whether they run on the "meter" or on the control system of which it is a "part"). Installing and maintaining smart meters and allied control systems in 28 million homes and 2 million smaller business will require rather more skills than current meter reading and create many more jobs. To these should be added those manufacturing, installing and maintaining low carbon technologies such as heat pumps and micro generation as the information given to consumers by their smart meters helps commercially sustainable markets to grow. Finally we should note the Green Alliance's example of £273M of exports of low carbon and environmental goods and services to Germany against imports of the same from Germany to the UK of only £171M.[12]

5. GREENING THE SUPPLY OF ENERGY. Conservative policy is to ensure that we meet our targets for greening the country's energy use and meeting our climate change commitments, thus creating a virtuous circle. In 2009 the Conservatives criticised the then Government because it had "failed to create a low-carbon economy"[13]. Success requires a more holistic approach, bringing policy together across communications and transport as well as energy. The Government should consider encouraging companies to have a certified sustainability person on the staff. This would not only help to assist companies, as consumers, to use smart metering technology but will contribute to spreading the message into the domestic market.

Cornerstones

In order to meet the policy objectives, there are a number of pre-conditions, which we have identified as crucial to the success of the Smart Metering programme. These are:

- Consumer engagement: without the active support of customers and voters the policy will fail, even if it can be sustained politically. The concerns of organisations like the Which? must be answered and turned into support based on genuine customer benefits. The Government can do all the things that we cannot individually do for ourselves and in this regard should be able to help to empower the consumer much more than they have been to date. We should try to get to the point where consumer-

[12] http://www.green-alliance.org.uk/greengrowth_GermanyUK/
[13] Green Technology Recovery 2009, Page 1

oriented service providers get creative and bring all sorts of new offers to the table, a good example is Abundance. The roll-out of smart meters will create a better informed consumer and this should lead to better understanding and therefore discrimination in terms of supply. This is not just good for today's consumers, it is good for today's entrepreneurs, as it creates a game in which many can play rather than just the biggest.

- Investor engagement: industry will need the right investment climate to make the commitments needed not only to install but also produce meters to international standards for installation around the world thus helping to create new jobs and export-led growth. Open technical specifications and operating processes are key. Without inter-operability and international standards across equipment and suppliers, it is not possible to create and maintain an open and competitive market. This includes the standards which enable the device to interface with other domestic equipment as well as to communicate with alternative energy suppliers. Such standards also allow the market to develop products and services that are not only interoperable and therefore able to be swapped out by the customer, but can also be sold into other markets. They make it easier for innovators to develop complimentary applications and equipment. They allow us to build infrastructures that are fit for an unknown and unpredictable future (as did our Victorian ancestors). The market must allow evolving technologies to be adapted and adopted as necessary, such as using smart phones to display meter readings, unforeseen as little as five years ago when current policy was being drafted.

  The need for an integrated policy on open standards (at all levels) was well summarised in the report of a discussion organised by the all–party Information Society Group for the 2011 Parliament and the Internet Conference http://www.eurim.org.uk/activities/ke/111013PandIreport.pdf

  That session was on bringing the Broadband and Green Agendas together and a key point was that a dynamic market, with genuine co-opetition between varied and evolving service offerings, is critically dependent on "open" standards to enable inter-operability and choice. For infrastructure sharing these include the definitions for catalogues of physical assets, network components, operational processes (e.g. performance measurement) and also business processes (e.g. service level agreement, monitoring and response). Hence the need to put the work on "smart meter standards" into context and to use it to help establish UK leadership in the setting of global standards.

- Security and resilience: if the devices themselves are not trusted by customers and consumers this will have a very negative impact on willingness to take up the technology. Rumours about the "off" switch and how it might be used and by whom do not help. Meanwhile meters also need to be secured against abuse by consumers and security attacks.

Security is not just about keeping the system secure but also about security of supply. Whilst these are not specific areas dealt with in this paper, the storage of LNG and the build up of stocks to ensure a supply that can be metered must be an energy objective for the Government. Moreover investment in technology to store electricity would benefit both the industry and the consumer by allowing energy to be created when fuels are more abundant (e.g. wind) and released when demand is high.

This document deals with each of the above policy cornerstones with recommendations for the Conservative Party.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Background

The roll-out of Smart Meters is a priority for the Coalition Government, forming a part of action to cut greenhouse gas emissions, decarbonise the economy and support the creation of new green jobs and technologies. It is thus an important part of the Government's energy policy. In June 2012, DECC published the Smart Metering Implementation Programme, Programme Update April 2012.

The Government's vision is for every home in Great Britain to have smart electricity and gas meters with In-Home Displays. This means that approximately 53 million meters will be installed in Britain, involving visits to 28 million homes and 2 million smaller businesses. The consumer benefit will be: near real time information (e.g. gas updates every half hour) on their energy consumption to help them control energy use, save money and reduce emissions. Smart meters will mean more accurate information and an end to estimated billing. Switching between suppliers will be smoother and faster. We need to be cognisant of the advance in technology since this debate started, particularly where IHD are concerned.

Suppliers will have access to accurate data for billing and to improve their customer service. They will also be able to reduce costs, for example by reducing call centre traffic or removing the need for a site visit to read meters and better manage debt. Energy networks will have better information upon which to manage and plan current activities and smart meters will help enable the move towards smart grids which support sustainable energy supply. Over the next 20 years, smart meters are expected to deliver around £7.2 billion net benefits to the nation.

Energy suppliers will be responsible for installing smart meters to their domestic and smaller non-domestic customers. They will be required to complete the roll-out by 31 December 2019. This is a challenging but achievable timescale.

The role of the Government is defined as:

1. Ensure Industry has the right commercial incentives to support and participate in the smart meter roll-out programme;

2. Ensure Industry has the right regulatory regime to enable it to support and participate in the smart meter roll-out programme;

3. Ensure that enduring benefits and costs savings are delivered to consumers.

Charles Hendry, former Energy and Climate Change Minister summed up the Coalition Government's attitude as: "Consumer benefit is at the heart of the Government's smart meter programme"[14] We agree with this summary.

[14] DECC Press Release

Consumer engagement

If the Government is to roll out smart meters successfully then it will need to win round the consumer. A report[15] for Which? by the Centre for Sustainable Energy published in November 2011 reviewed the public's perception of the smart meter programme. Whilst the report cites some clear benefits, it also raised serious concerns over all aspects of consumer engagement in the programme. In fact none of the areas looked at scored a "green" (meets consumer-led objectives) which demonstrates that there are serious areas of concern amongst the general public. Similarly consecutive surveys carried out on behalf of Consumer Focus highlighted the challenge of domestic consumer engagement.

Who is the consumer? In this case the consumer is both the domestic user and the corporate energy customer. Whilst there are therefore clearly areas of difference both will be interested in the twin benefits of cost savings and ease of use. The adoption of many technologies by domestic consumers in the last twenty years started in the workplace. The spread of GSM is a good example. Mobile telephony started out as a corporate tool and the potential of mobile telephony for the consumer was not foreseen at the start. Consumers quickly saw the advantages of mobile telephony and it spread to being a normal part of life. In the same way we can envisage the use of smart metering spreading from the workplace to the home.

Whilst engagement with the consumer will be done through the supplier, it will start with education and this will be done in conjunction with DECC. Both the Which? and Consumer Focus research reports highlight the problems of trust between consumers and suppliers which need to be addressed.

The Government can support this in terms of consumer protection provisions by trying to create a climate of confidence in the programme, but it will be a supplier-led engagement. If the customer (commercial or domestic) consumer cannot make an informed choice whether to accept and use a meter, the costs will rise as sharply as the benefits will fall.

All sections of consumers need to be engaged. A market-led approach would typically target the early adopters. In the context of energy usage this can be summed up as four types of consumer:

- Active Greens who see smart metering as a lifestyle choice;
- Technophiles who want to have and use the latest technology;
- Those who carefully manage their household finances;
- The vulnerable and those on low incomes who are assisted by those helping them manage their finances .

[15] CSE Study : , The smart metering programme: a consumer review , November 2011

This can be seen as a two pronged approach in that the first two categories would be driven by similar motives and the last two are also driven by the same motive – household finances.

The six key elements of our consumer engagement policy are:

1) Build confidence in the benefits to the consumer

2) Demonstrate and communicate the benefits received by early adopters or recipients of smart meters in terms that are meaningful financially and technically as well as in meeting Green targets.

3) Ensure that vulnerable and low income consumers benefit by working with target groups such as Charities, local authorities, health bodies and Housing Associations.

4) User control (including of choice) ;

5) Making devices easy to use;

6) Coherent Financial incentives (to both user and supplier)

We will not be able to create a viable market unless we begin with the interests of the customer, remembering that most trust their energy supplier little, if at all, more than they trust politicians and government.

POLICY AREAS

1) Build confidence in the benefits

If the adoption of smart meters is to be a voluntary exercise, with opt-in on the customer's side, then customers will need to be confident that the promised benefits are attainable. This remains the major challenge. . As the Which? study, "The smart metering programme: a consumer review", points out, there is "a deep-seated concern that the system functions well.[16]" The study goes on to state that, by concentrating on the technical correctness of the roll-out, sight has been lost of the benefits to the consumer. This has given rise to three key areas of concern:

1. **billing accuracy, fairness and cost;**
2. **security and control of the meter and data;**
3. **environmental health concerns about RF.**

Government policy will need to begin by ensuring that billing is accurate and fair. The consumer should be able to better shop around for the best deal and smart metering should enable this to happen more easily than it does now. The other two areas of concern may well have to be taken on trust by the consumer and we suggest below how this might be achieved – but without confidence in the accuracy and fairness of the billing that will be much harder.

[16] Page 15, The smart metering programme: a consumer review

Billing accuracy, fairness and cost: This will need to be done through clear pricing tariffs that the consumer can easily understand and follow. At the moment consumers receive the usage rates and the corresponding tariffs retrospectively. Kilowatt hours attract different tariff rates the rationale for which is hard for consumers to fathom out. Consumers find it hard to equate price rises / falls with world energy prices and this has helped to fuel distrust between consumer and supplier. It is believed that the benefits of price falls are not passed on whereas price rises are. Moreover the accuracy of bills is believed, by the consumer, to be wanting.

Tariff rates must be simple and information on different rates, timings etc. should be readily available. Actual meter costs should be separate from energy costs. The Web is one obvious source of information but not everyone has or uses Web access and rates should be published in printed format as well as online format. The means of distribution of information about rates should also be a consumer choice. If a consumer wants to receive a printed copy by post (at cost) then that option should be available to them. Information on tariffs should include timings as well as price break points as more, or less, energy is used. Thus a company could decide to move more production to the afternoon shift if, for instance, prices were cheaper between 13.00 and 18.00. Or a householder could time their wash for after 23.00 because rates are cheaper. Consumer take-up will be greatly expedited if early adopters are seen to reap serious benefits from linking meters to timers or the affordable domestic equivalent of pumped storage devices.

Linkage of tariffs to certain times is one other clear benefit of a smart meter. In fact this can be extended to covering the energy source. Thus a supplier could offer a wind farm tariff or a nuclear tariff. This tariff would reflect both consumer choice and the availability of energy from the chosen source. Wind farm-based tariffs could be dynamic, during a windy period they would be very low for instance. To engage consumers, suppliers must be free to set up a mix of tariffs based on sources of supply and market preferences.

Ofgem or DECC must have a statutory role to ensure that the costs / benefits are transparent. Government should report annually on the progress of and costs and benefits to consumers of smart meter rollout. This should be broken down by customer segment, including fuel type, location etc. to ensure all customers are able to access the benefits. As in other industries, Ofgem must be able to levy fines for non-compliance etc.

Security and control of the meter and data: this cuts two ways, protecting the supplier from abuse by the consumer as well as protecting the consumer from abuse by suppliers or their staff. : This is covered in a separate, dedicated chapter on security policy recommendations. It does though need clear product certification and testing that is understood easily by the public. A parallel is in the certification of white goods.

Moreover, access to, and presentation of, smart meter data MUST improve dramatically. This coupled with the ability of the consumer to interpret, plan, action and manage energy reduction measures. These 2 issues create a very narrow choke point in terms of achieving significant energy savings. To a large degree increased understanding of smart meter data

will help pull through the measures contained in the non-domestic Green Deal. Until non-domestic consumers are able to make use of Smart Meter data significantly and quickly and lead the way, the DECC savings 2-3% estimate will remain.

Environmental health concerns about RF: the equipment used is already governed by safety standards and the Government needs to ensure that these are followed and adhered to by manufacturers. We believe that this is best achieved by independent testing of meters used and the display of a clearly verifiable and recognisable safety logo by a UK-based testing house. The arguments appear to be identical with those regarding the safety or otherwise of mobile phones and similar devices. If that is correct they should be clearly explained and "proved" to the end-user in the same way.

Consumer Focus research found that a significant minority of consumers could have environmental health concerns with an estimated 5% of customers believing they suffer from some kind of electromagnetic sensitivity.

Key policy points:

- **Separate meter costs from energy costs**
- **Mandate clear tariff structures**
- **Give Ofgem greater power to ensure costs and benefits are transparent**
- **Test smart meters in the UK to international standards, with the results accepted globally (that will entail UK participation and leadership in the relevant standards bodies such as OSSSE)**

2) Demonstrate and communicate the benefits

Policy must be developed both to encourage cost and energy savings and this will be achieved through education and demonstrating that smart metering will deliver on its promises. If I now understand my bill and can work out how to use the smart meter to control that bill then, as a consumer, I can begin to exert a measure of control. This control will mean that I am more able than I am now to take advantage of different rates and source my supply as I wish.

One example might be a consumer choosing to source tidal energy as the primary supply. This may allow for premium pricing at times of high demand. It may allow for green tariffs and non-green tariffs to be offered. Another example might be to keep a running total of the bill with the meter informing the consumer when usage is above or below average . This might indicate items being left on and otherwise provide the information necessary for the user to decide how to change their consumption behaviour. It should also be possible to programme the meter (or an attachment) with a budget and for it to give warnings of

overspend so that appliances can be switched off or heating turned down in favour of warmer clothing. If the aim really is to smooth peaks of demand, we need to be thinking of systems which make it possible for users to arrange for appliances or heating to switch temporarily when charges spike immediately after Downton Abbey or during half time for the Cup Final.

A very clear benefit will be billing accuracy (also see 1). This is a major area of concern for consumers.17 It is clear that DECC must focus on this in its engagement with the consumer. Cost and energy savings will follow as users become more knowledgeable but in order to deliver cost-effective energy savings, users need to be educated and informed to ensure that they are won round. There are likely, judging by experiences in other countries, to be anti-smart metering lobbies who will be following particular lines of real or imagined concern. DECC will need to have worked out a full communication strategy that brings in civic groups and creates a wide network of support. This needs to be in place by the end of 2012.

Experience in the US[18] is 10-15% but this is based on corporate consumers who have higher bills than domestic consumers. This is based upon transferring pure data, to visual actionable information, enhancement of that information and stakeholder engagement. This high level of savings also depends on the management's appetite for action and the internal ability to plan, implement & benchmark energy reduction measures. The 15-30% savings can be achieved, but not just with enhanced Smart Meter interpretation. It has been proven in the US that by using a "combination" of the actions below, the 30% mark can be achieved:

- Smart Metering (Interval Data) followed by,
- Targeted Sub Metering (Itemised Data), then,
- Implementation of set-point changes, and technology/renewable investments.
- Board/Management backed energy reduction programs.

Those supplying and installing smart meters should be encouraged to provide educational material (both on-line and off-line) and via a variety of media for all ages, from schools to the elderly, showing how they can use the smart meters in their homes to best effect. That material will need to be available in the language of the customer and for those unable to read and tailored to the needs and motivations of different customer segments.

Key policy points:

- **DECC to produce a communication strategy (which is underway but late**
- **Communication strategy to involve consumer, civic and business (both small and large) groups**
- **Communication strategy to emphasise** customer (as opposed to supplier) **control as a benefit**

[17] Page 34, The smart metering programme: a consumer review
[18] Melrok software services derived from Smart Meter data

3) Ensure that vulnerable and low income consumers benefit

There are two sections of society which need special consideration. These are:

- Vulnerable
- Low income consumers and the fuel poor

Concerns have been raised by the National Audit Office, Public Accounts Committee and consumer groups about the impact of smart metering on low income and vulnerable consumers. Further work is needed in this area including a distributional impact assessment to understand the likely impacts of rollout on different consumer groups.

Whilst the policy needs are nearly identical we have separated these two groups out because there is a clear difference in that the vulnerable in society should (at least in theory) have a guardian or statutory authority to help them take decisions. Low income consumers are in need of products and services that allow them to budget accordingly. We should also be careful about the definition of fuel poverty as several newspapers (FT, Daily Telegraph) have run stories on the Queen being nearly fuel poor.

Policy towards the vulnerable needs to ensure that additional support is available. A model for this is the digital switchover with recent advertisements for Old Age Pensioners and the help that could be given them to switchover such as the Extra Help Scheme for digital switchover.. The switchover provided additional support, home visits and equipment for free. Moreover, it involved data matching to identify those most in need. A number of consumer groups are pressing for energy companies to establish a dedicated pathway for vulnerable and low income consumers and an Extra Help Scheme and at least one supplier is already doing this The Which? study claimed that energy suppliers load costs disproportionately onto (inter alia) vulnerable customers because they are either a higher credit risk or, using more expensive payment methods or are less likely to switch e.g. because they are unable due to a debt, or unaware that they can switch payment method or supplier. Ofgem will need to ensure that consumers are not penalised when they pay regularly but choose to use non-preferred (by the supplier) payment methods. The ability to switch payment methods is important for all consumers. An example is the current attempt by some suppliers to make it difficult or impossible to pay by cheque or via the local post office, an essential facility for those unable or unwilling to use on-line services. Ofgem must be willing and able to levy fines where such discrimination is evident.

Another example is British Gas, who is on track to be the first GB supplier to offer prepayment smart meters, before the mass rollout begins in 2014. British Gas believe that "there is a significant benefit to our customers in being able to switch from having a 'credit meter' to a 'prepayment meter' without needing to have the meter replaced" British Gas is also looking at the future use of top-up facilities online, remotely or through friends or family which is to be encouraged.

Suppliers of smart meters/ equipment must also offer options for customers with impairments, including those who are both the deaf and the blind to "read" and engage with the meter – perhaps using add-on devices or where cost effective to do so, inclusively designed products which meet the needs of as many consumers as possible. No-one individual should be at a disadvantage because of a physical handicap.

Low-income users also tend to suffer from similar disadvantages as vulnerable ones. Again DECC must ensure that all users are treated equally able to access the benefits of smart metering.

DECC must engage with local authorities, health workers, and Housing Associations as well as other housing charities (e.g. the Peabody Trust) and those supporting vulnerable consumers, the frail and elderly, those with mental health issues, long term sick and families with young children in their own homes . One important question is to what extent should a charity or Housing Association be able to manage energy usage on behalf of their clients or residents if they fall into the vulnerable or low income categories? Moreover British Gas have pointed out the current technical difficulties with installing meters in tall buildings where the meter is in the basement but the IHD needs to be in a flat so many floors up.

Key policy points:

- **Pricing policies must demonstrably be the same for all consumers, no-one should be disadvantaged because of an impairment or low income**
- **DECC needs to engage with a range of community actors, including charities, health bodies, local authorities and Housing Associations to ensure that safeguards are in place and that proper education of consumers takes place.**

4) Information privacy.

Key questions are:

1) Informed choice
2) Who should be responsible for what in the event of a data breach or compromise?
3) How do ensure maximum benefit to customers and businesses from smart data, while protecting customers' personal privacy and their ownership of data?

This is one of the areas of greatest concern to consumers and is being addressed by DECC. It has been used publicly as a stick with which to beat smart metering programmes in other nations. Well-publicised failures in both the private and public sectors with information , leaked, compromised or lost have made it an area of genuine concern to all. Security of the system is dealt with in another section of this policy paper. This section concentrates on putting provisions in place to protect the privacy of data.

The sharing of data between consumers, the electricity providers and generators is needed if the smart grid is to receive, collate and interpret information and manage generation on a dynamic basis. The difference lies in whether that data can be traced back to an individual consumer or not. Data between the consumer and the provider will have to be traceable but it should normally be anonymised as soon as it is passed on to another party in the supply chain. Any exceptions, e.g. to enable those with power of attorney or other guardianship duties to manage the energy supplies of the most vulnerable, must be explicitly ring-fenced. .

The only assurable means of anonymising data such that it cannot subsequently be de-anonymised by mining and correlation, is to aggregate data from multiple similar consumers and average across the aggregate. It needs to be recognised that this also limits the ability to analyse data for predictive purposes. There needs to be an explicit debate as to whether those willing to waive their anonymity should be able to do so in return for benefits. That debate should, however, take place in the context of a wider debate on the meaning of informed choice which is outside the terms of reference of this study.

Given that meters are likely to be in place for many years we must assume that the suppliers of malware will be promoting bypass programmes to send back false data before they are replaced or upgraded. We recommend that usage of such software to alter the reading, except in the case of research on mains-disconnected meters to find and remedy meter security issues, be clearly regarded in the same way as interfering with a physical meter or stealing from a coin in the slot device

In sum the customer must own the information about themselves and their consumption while giving consent for it to use for the purposes of serving their contracted needs. That consent, covering address, post code, meter number, frequency with which the meter is interrogated (e.g. every minute, hour or day) etc. needs to be explicit and linked to incentives (e.g. time of use tariffs).

Key policy points:

- **The information should belong to the consumer and be shared by explicit and informed consent with the supplier**
- **Consumer must be allowed to actively opt in to have attributable data shared with 3rd Parties or other members of the supply chain. They should not be coerced without choice.**
- **There should be routines to allow data to be shared up and down the supply chain *anonymously* and not traceable back to the individual**
- **The amount and frequency of data sharing should be by informed consent, with incentives for added frequency if this is desired by those in the supply chain.**

5) Making devices easier to use

The customer interface needs to be to understand and take into account that consumers may have some kind of impairment.. Customers with impairments should not be penalised because they require additional functions or add-on devices because conventional smart

meters are difficult to read. Whether the additional cost should be met by the supplier or by "social services" needs to be discussed and subject to explicit political choice. Inclusive design approaches have been proven to reduce overall costs of equipment which is rolled out widely, as well as often making them easier to use for everyone.

Consumers must also have a choice in terms of complexity. Thus if they want a simple smart meter which just shows them the rate of usage then this should be available. Like the mobile phone market, if consumers want more functionality then this should be available but at a price. We would expect suppliers to offer a range of options (which may be software based using the same hardware or the result of interfaces with add-on devices).

Suppliers of smart meters should also allow for the development of smartphone and PC applications that consumers can use to both read the meter remotely and to manage it. Thus I should be able to check whether the heating is off or be able to control devices remotely (as is already available with some video recording devices). It is important that appliances are interoperable and interchangeable so that the customer is not locked into purchasing equipment from the supplier that installed their smart metering system, and so that the appliance will work if they move home. Key functions that consumers may wish to extract from their smart meters are old bills (for proof of residence), an end to estimated bills and the ability to control the switching on and off or items so the consumer understands what is efficient or not. However, while home automation systems are sensible and desirable adjuncts to smart meters, their functions - including monitoring and turning specific appliances on and off remotely - must remain explicitly outside the scope of this study, and these functions should be implemented by equipment explicitly outside the meter's security perimeter.

Key policy points:

- **Smart meter interfaces must be legible by all consumers and cater for the needs of different customers including those with impairments**
- **Smart meters should have interfaces that are accessible by application designers so that they can be managed remotely and by other devices under customer control (from mobile phones to "smart" heating systems or domestic appliances).**
- **Consumers must be able to use the interfaces to extract energy consumption information that enables them to become more empowered consumers. This includes: suitable billing information; consumers also need be able to access data they need to compare deals in the market and identify the best deal one for them; hold suppliers to account for poor customer service; share with third parties, who may be offering services like energy efficiency or switching services; become effective consumers, where they generate their own energy they need to know how much they are generating – so how much they are owed, price getting; budget more easily etc**

6) Financial incentives

The suppliers should be obliged to offer smart meters to all who want them within a given timeframe but should be able to discharge that obligation via 3rd parties who own the meter,

install and maintain meters that meet the standards agreed by the regulator. Obliging customers to accept and use smart meters is not, however, practical politics because of the current level of mistrust. .

The consumer experience with savings from changing energy tariffs so far has been largely negative. Which? published (http://www.which.co.uk/switch/energy-suppliers/energy-companies-rated) its 2012 review of customer satisfaction based on a survey of consumers in November 2011. This gave an average satisfaction rate of 47% (weighted to the market share of each energy company). Consumers do not believe savings can be made by switching amongst suppliers because today's cheaper supplier is tomorrow's more expensive one. If smart meters are not seen to deliver cost savings for the early adopters then the bulk of consumers are unlikely to follow them. Conversely if early adopters can receive demonstrable cost savings then voluntary take-up will follow . DECC as part of its consumer information policy will need to make clear that it recognises this. Given that Government and Regulators are trusted little, if at all, more than the suppliers, we suggest that an engagement with a neutral consumer group such as Which? to publish results will go a long way to convincing the sceptical consumer.

Attitudes may also change given upfront financial benefits. The incentives the work for early adopters may well be different for "followers" who are more likely to want "ease of change" and "guaranteed savings".

As a policy decision, the CTF believes in incentives that are tailored to help meet policy objectives. These might should be limited in time in order to help get the programme going and have a particular focus on the needs of the vulnerable and of low income groups (e.g. free installation and guaranteed savings). We would expect the cost of smart meters to drop as the technology becomes more accepted anyway and this expectation is borne out by other technology sectors. Thus, whilst "early adopters" might willingly pay more in the expectation of greater (but uncertain) benefits, the bulk of consumers would pay less as the costs of manufacture and installation come down. By organising subsidised installation programmes for low income earners, prepaid users and the vulnerable at the start of the programme, the policy will also help to add volume to the initial number of smart meters installed which in turn will help to drive down costs and accelerate take-up.

Assistance to these target groups can be realised in a number of ways. DECC may introduce a targeted scheme that either defrays the cost for the consumer or subsidises it directly. However as a Conservative policy we would not advocate giving something for nothing. If the consumer has had to pay even a token amount (in return for a "guaranteed" benefit) we believe that this will be more of an incentive for them to make use of the meter and avoid it becoming a free hand out that just sits in the corner doing nothing.

A simple incentive scheme that offers a rebate against your energy bill or Council tax, could work well. This would have to be limited in scope but could significantly alter behaviour. An important target audience for initial roll-out, that would benefit those on low income or who are classed as vulnerable, is landlords. These might be Housing Associations, Charities or

private individuals. The installation of the smart meter would be classed as a property improvement and be used as part of the selective licensing requirement by a local authority.

Those unable to afford the cost of a new meter due to low income should also be able to obtain a subsidy, perhaps as an extension of the Green Deal. If so, this might be in the form initially of a longer payback plan rather than a subsidy. Suppliers should, in any case, be obliged to offer long-term payment plans for low income consumers if these are necessary to deliver genuine cost savings.

Key policy points:

- **DECC should support the provision of time-limited subsidies for early adopters**
- **Low income consumers should be offered long-term, affordable payback schemes to ensure they receive genuine cost-savings.**

Conclusion:

DECC will need to work hard to educate the consumer in the benefits of Smart Metering and ensure that these are delivered in practice. The Energy market thus far has not offered open competition or control to the consumer who is therefore reluctant to believe in further change. It is therefore incumbent on DECC to ensure that the market is transparent and consumers both understand what smart meters offer and have the tools and knowledge to best to take advantage of this.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Investment: market rules and business case

Generally speaking the UK is seen as a good place for start-up businesses and a leader in some energy-generating technologies: "Britannia really could rule the waves when it comes to marine renewable energy," said Tim Yeo.[19]

However, a more coherent business case is needed to attract and reward the pension and sovereign wealth funds whose support is necessary to enable suppliers to invest in the roll-out of smart meters as a step toward smart grids and a more energy efficient future. Investors need confidence that they will see continuity of political and regulatory support and to be able to test the likelihood of mass market with low risk, scalable, pilots that are seen to give the payback predicted.

We should also ask how citizens can be brought into the investment model, How can we enable and encourage the ordinary citizens to "buy into" the smart meter roll-out other than simply paying for their own? How can we enable and encourage individuals to put money into the shared infrastructure build? Might there be a Big Society option that is also better than putting your savings in the building society such as a co-operative model to install meters in a given area?

Part of the investment case rests in the ability of the market to drive down the costs of installation. The cost of installing a meter may remain roughly the same but the cost of the actual meters is expected to fall over time. This is because economies of scale are expected to come into play as certain volume thresholds are reached. One way of helping to reach this threshold more quickly is to bring in smart meters for low income or fuel poor consumers. This would not only benefit those who can least afford energy and therefore be a social good which also drives down production costs by boosting initial roll-out volumes.

Our policy areas are therefore:

Review the overall UK Communications (including fixed and mobile broadband, 4G and PSN) strategy in the light of the evolving needs for shared infrastructure investment for the world of ubiquitous computing and intelligent cities whilst encouraging early investors.

Dealing with churn

A viable market will only be created if it is clear that the investment will pay off.

POLICY AREAS

Investment in Smart Metering

1) Review the Communications Strategy in the light of the evolving Communications scene and changing investment opportunities and priorities

[19] The Guardian 20 February 2012

Current smart metering plans include communication plans are at arms-length from those for fixed and mobile broadband let alone the new generation of public service, health and education networks being procured via a variety of frameworks, including those for PSN.

Moreover it has been said that officials have been forbidden to communicate with their peers in other departments because they may be negotiating with the same suppliers.

However, infrastructure sharing across much of the world goes well beyond merely sharing communications networks. It is commonly driven by the needs of local authorities to save costs by bringing together currently separate networks serving, for example, street lighting and traffic controls, surveillance cameras, welfare services and schools. In some cases the targeted savings already include those from better monitoring and controlling energy costs,

Meanwhile mobile operators are merging their infrastructure networks, piggybacking on council and utility networks in order to cope with soaring demand for mobile communications. It is apparent that there a variety of competing models are now developing which are capable of delivering the connectivity required for smart metering and that the value of polling budget budgets to reduce both start up and maintenance costs and improve resilience and security is considerable.

Key policy points:

- **Improve policy co-ordination between Government Departments, (DECC, DCMS, DEFRA, DCLGe etc.) perhaps using the Cabinet Office PSN team or those organising regional PSNs via the LGA REIPs as brokers so that communications infrastructure and operations costs can be shared across applications.**
- **Improve information exchange between Ofgem and OfCom at all levels pending the creation of a merged Infrastructure Regulator, as in Germany.**

2) Encouraging early investors: Policy has been written based on a 100% roll-out with aggregate savings per year of on average 2 – 3% per consumer. This is unlikely to "float anyone's boat" in terms of encouraging adoption. Alone, this is unlikely to encourage Experience in the US is between 15 and 30% savings. This is based on the ability of the consumer to understand and interpret the data so that action can be taken to save costs.

Instead by concentrating on the early adopters with savings of between 15 – 30% in reasonable prospect the market can build on success stories. Many other technologies have followed this model such as set top boxes, mobile telephony etc. Although the initial costs are higher, these come down over time. This illustrates the importance of open standards and creating a competitive market. One early adopter group could be businesses who may create their own "micro-climates" on business parks or industrial estates. In addition early adopters would reduce costs as they will want to give access to their property to install the meter. Installation into properties where people do not see the benefit is far more costly.

Key policy points:

- **Market-led roll-out that targets certain groups who are more likely to reap the benefit.**
- **Consumer understanding around how to use the data and turn it into information**

3) Dealing with churn

This is a disincentive for industry in that it is a brake on investment. Market rules say that the energy supplier is responsible for installing the meters. Installation and the meter costs are roughly £300. If the consumer changes the meter during its lifetime then the original supplier runs the risk of losing money on the installation. This needs to be addressed with rules and regulations (e.g. for investment write-downs and transfer costs) in the Codes that are agreed along with the licence obligations which the supplier has. We would not want to create a barrier for early adopters who wish to switch at a later stage.

One critical issue to address is transference of energy supplier by the consumer and who then owns the meter. The new supplier is not obliged to use it. The issue is whether or not the new supplier should be responsible for paying a residual value for the meter or the consumer who chooses to change. There is a danger that the brake will be put on consumers changing unless there are clear rules which do not disadvantage either the supplier or the consumer. These must be set by a 3rd Party such as DECC.

Conclusion:

Due to the high roll-out costs of smart metering, a stable market needs to be created so that suppliers can raise the capital necessary to fund those costs. This depends on an assured long-term vision from the Government (of whatever political stripe) that smart metering will be supported whosoever is in charge.

Moreover the investment case will need to demonstrate a clear return on investment both for consumers and for suppliers. We believe that this is best done by a targeted roll-out, stage by stage which will benefit those in society who are more likely to want or make use of what the meter can offer them in terms of information. This will provide a momentum and acceleration that will ensure a profitable roll-out for all parties and is more likely to achieve the desired 100% coverage .more rapidly and at less cost than a “big bang”, centrally planned imposition.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Standards, Data and Communications and the Smart Grid

The Conservative Technology Forum wants to ensure that standards are both open and international as this will benefit an export led recovery. The UK must not go down a standards blind alley which limits the market to the UK and effectively prohibits export of British made smart meters to other countries because the standards do not match. Similarly the UK government must work to ensure that our Standards bodies are aligned with those in the EU and further afield. We must not fall into the trap of using local standards as a way of protecting our home market.

The importance of open standards to a successful system not only impacts on the ability to export but also on the consumer. An easily recognisable open standards programme will give surety to the market that products for sale are tested and can be safely installed. It also makes it easier to change suppliers, meters or smart products without having to update whole networks. Moreover the CTF envisages the development of application software and related hardware to complement smart meters. This will be simple and more straightforward if smart meters conform to set open standards.

The security of data and what can or should be done with it and how it is to be handled is dealt with in other sections of this document. However, it should be carefully noted that data and communications are an essential backbone of this system. Together they form part of the Smart Grid, which DECC defines as:

"Smart grid" generally refers to a class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries.[20]

The Smart Grid is a separate topic and whilst we touch on this in this policy paper, our aim is to produce a specific paper on Smart Grid / Infrastructures paper.

POLICY AREAS

1) Standards

Standards should be open and international. The Government must ensure that the UK plays its full role in international standardisation bodies (a role formerly well fulfilled by the National Physical Laboratory). There is an initiative to develop standards for the European Technology Platform for smart grids[21].

The meters themselves should be as simple as possible, M441 is an example of a standard that makes the metrology simple. The basic function of the meter is to measure supply and

[20] http://energy.gov/oe/technology-development/smart-grid
[21] European Tech Platform for SG: http://www.smartgrids.eu/node/28

relay that data back to the consumer / supplier. This should be kept as simple and uncomplicated as possible. Furthermore the meters should have their own connections to the network and not go through the consumer's network. This means resilience and ubiquity rather than capacity. As yet there is no definitive framework for the Smart Grid standards. UK should take a lead and pull together its own inputs on this topic so as to have a coherent approach on this topic.

Standards should also be viewed as a cross departmental and industry effort. As an example smart meters and the standards used will have an impact upon the construction industry which has standards of its own. These are regulated by a different Government department, BIS, and need co-ordination.

Key policy points:

- **Standards are key to the success of the programme and the UK Government should be active in supporting UK inputs to the relvant bodies, national and internationally.**
- **Standards cut across industries and must therefore be handled on a cross-Government departmental basis.**

2) Data and communications

The secure exchange of data between the smart meter, the supplier and the consumer are the crux of the smart metering policy. Whilst the supplier can clearly make use of data to measure and ensure sufficient capacity is available, the consumer can be given incentives to use energy at times that smooth out the peaks and troughs for the supplier. This is particularly true of the gas suppliers who have traditionally see large fluctuations in demand in the winter when millions of households put the kettle on at the same time after a popular TV programme

Moreover the consumer should be able to benefit from this data and communications infrastructure. One example could be the ability to take advantage of specific tariffs. Another example could be dynamic discounts for large or small consumers. Thus if the Met Office is forecasting high winds over a given period, the electricity generated from wind turbines could be sold at a discount. Though it is recognised that not all consumers will be able to benefit from new smart tariffs.

An advanced data and communications network will allow for much more sophisticated tariffs and offers, the CTF would particularly like to encourage the use of dynamic tariffing to demonstrate the benefits of renewable sources such as wind where it is proven to deliver consumer benefits and one in a way that safeguards consumers.

We also need to consider the premises (address) and why it is needed.

Many of the new energy initiatives, (Green Deal, Feed In Tariffs (Fits)) as well as Smart Metering refer to customer premises. Smart Meters which are installed at a customer's

premises will comprise of multiple devices which will include but are not limited to a home communications hub, an electricity meter, a gas meter and an In Home Display. The details of the smart metering devices installed will need to be associated with the customer's premises as some of the devices (e.g. Communications Hub and IHD) are shared assets between multiple suppliers. The question should then be asked how do you identify which smart metering devices are installed at a premises as there is no existing standard definition of a premises within the Utility industry and therefore the current proxy for a premises is an address.

The Smart Meter Implementation Programme (SMIPS) is a standardising process within the existing Electricity and Gas Markets for the installation and operation of smart metering. The Electricity and Gas industries use different identifiers to distinguish between customers, The Gas industry uses MPRNs and the Electricity industry uses MPANs, there is no current link between the two references, the only way within the existing arrangements to link MPANs and MPRNs is by matching associated postcodes. This presents 'challenges' because different definitions of an address exist in each sub sector, There is no fixed format between industries and these different approaches create address data quality issues which mean problems arise when trying to identify premises and match addresses across different systems and organisations, which is one of the key planks of the Smart agenda.

The aim should be to create a common premises standard which delivers a single property reference within the utility industry which both Electricity and Gas companies use. The communications hub network address will provide a link between all devices on the same Home Area Network (HAN). The Data Communications company (DCC) will need a spatial reference per customer premises to tie together the Electricity MPAN and Gas MPRN. A Unique Property Reference Number (UPRN) could provide the spatial reference key and it is a Government created addressing reference approach for over 34 million GB address premises. The UPRN is not required for access control purposes but the DCC and its users (DNO and Suppliers) would benefit from having this information within the 'inventory management' database. For example, suppliers may request information from DCC to identify all smart metering equipment at a customers premise (e.g. to assist with rollout planning or asset management)

The UPRN has also been identified as a means of recognising the existence of 'single fuel' meters on the same site (Address).

DECC have proposed that the UPRN is added as a new data item to be included in the Electricity and Gas Industry registration data sets within the SMIP Legacy System Changes (Enduring) paper. That proposal suggests that the data item should be maintained by the Electricity Network Operators or Gas Transporters who are responsible for the existing MPxN registers. As it stands today the UPRN could be added to registration systems now, although registration will be transferred to the DCC 2-3 years post DCC go-live, Network operators are best-placed to manage new connections / decommissioning and the UPRN would be passed from registration systems to DCC as part of the data set required for access

control purposes. The UPRN can then be stored as part of the DCC smart metering device inventory to deliver a common premise address underpinned by a single common spatial referencing framework.

Key policy points:

- **The data and communications network must be recognised as two way customer to supplier and vice versa.**
- **Data and communications must be secured and access to the data strictly controlled to ensure consumer privacy.**
- **Subject to a positive business case and consumer protections in place, suppliers should be encouraged to make use of the data to offer dynamic tariffs to both commercial and household consumers.**
- **The issue of registering premises must be addressed in a cross-supplier (Gas and Electricity) manner.**

3) Smart Grid

This policy paper will not touch on the Smart Grid in depth as it is our intention to produce a separate paper on this topic. The importance of the Smart Grid will be felt by the consumer as part of a wider, smart infrastructure programme which will be backed up by smart metering and broadband communications. Without foreshadowing our views on the Smart Grid too much, the CTF can envisage a UK in the near future in which buildings will become auto or self-managing against set parameters and fit into a larger urban design which will support intelligent systems for traffic control and guidance.

The Smart Grid will also enable micro-generators to produce and sell their product into an open market for energy. We also need to ask ourselves whether micro-generation and local storage are likely to grow exponentially and, if so, what effect will this have on the Grid? Could micro-generators be isolated so that they do not overload the Grid for instance? Understanding the latent demand is key. Suppliers need to understand what this might be.

Key policy points:

- **The Smart Grid is so important that it needs a specific policy review**
- **in conjunction with smart infrastructures such as building management systems.**
-

Conclusion

Standards must not be underestimated as these are key to the successful roll-out of smart meters and also to the establishment of an export-led market for UK manufacturers.

Moreover, standards will help to stimulate the creation of applications and other services over the data and communications network which will in turn make the Grid truly smart.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Security and resilience (Smart Meter / Smart Grid Security)

The objective is to ensure that the end-to-end smart metering systems that suppliers manage and operate, along with the equipment they install, enable a secure and reliable infrastructure for energy supply, protecting consumers' interests and industry investment, and realising data privacy commitments. These are all key to securing consumer confidence in the system. We recommend that the system be part of the CNI and thus afforded the support of the National agencies (CPNI and CESG).

It is imperative that security is embedded into the design process for smart meters and their communication systems from the start, to create a framework that allows systems and processes to be fit for purpose as risks, technology and requirements evolve.

All smart metering systems need to address security threats to data privacy and confidentiality and from unauthorised access to smart metering functions. The existing DECC programme correctly recognises the need to place specific obligations on suppliers in relation to the security of their end-to-end smart metering systems, through a new licence condition to reflect and underpin their responsibilities These will need to evolve over time and the risks evolve.

POLICY AREAS

1) Risk assessment

The process of carrying out a comprehensive risk assessment is an important step in managing security risks. It requires an appreciation within the organisation of the level of risk that can be accepted and the potential impacts should an incident occur.

Requiring suppliers to conduct ongoing risk assessments is key to identifying whether there are changes to the threat environment. It is recognised that what is secure today may not always be secure, and an important element of a risk assessment is to have a thorough understanding of the threats to the smart metering systems. Equally critical to a risk assessment is to have an appropriate scope which allows risks to be identified in the first instance.

The risk assessment should drive a set of measures to mitigate identified risks in line with the Appropriate Standard it has set. This should be set in the context of an Information Security Management System (ISMS). This is a framework that enables organisations to continually design, implement and maintain their desired set of security policies, to leverage industry good practice, and provide a holistic security approach. To that end, it has been suggested that suppliers should seek to align their security operations with ISO27001: Information technology – Security techniques – Information security management systems, although with ***no*** explicit requirement to become certified against this standard.

However, not all suppliers are in a position to certify themselves against this standard and while there is an expectation that suppliers will use this period to work towards attaining this

standard and be able to demonstrate steps they are taking in this regard, that may not be practical. The licence condition has been drafted to capture this intention but there is a need for further discussion on whether this is a suitable approach.

In addition to a robust ISMS, there are a number of disciplines that it is expected all suppliers to have in place, which include:

- A security policy, to govern the supplier's approach to risk assessment and treatment.
- Incident management procedures, that enable suppliers to identify and respond to a security incident in a coordinated manner, minimising the impact to those that may be affected.
- Business continuity and disaster recovery procedures.
- Access to appropriately qualified security staff who can advise on matters related to security.
- Physical security controls to protect equipment that interacts with the smart metering system.

Risk profiling will differ between suppliers, given the importance of maintaining secure smart metering systems, It is expected that suppliers will adhere to standards in line with good industry practice and that the standards adopted must be capable of being verified by a Competent Independent Organisation (CIO). The CIO is expected to assess whether the supplier's ISMS provides a level of protection in line with good industry practice that is also commensurate with the security risks.

A CIO is an organisation which has certain qualifications or characteristics such as being members of (or contain staff who are members of) CESG schemes (HMG's National Technical Authority for Information Assurance), such as CCP (CESG's Certified Professional Mark), CLAS (CESG's Listed Adviser Scheme), CHECK (CESG's IT Health Check Service Scheme) or CTAS (CESG's Tailored Assurance Service assessment scheme), or a combination thereof. This is achieved in the licence condition by using the term "Appropriate Standard".

We have constructed a structured Threat Model, to show and discuss openly the detailed thinking which leads to the Approaches and Recommendations below. The Threat Model text is included as an Appendix to this document.

The risks to be considered are not limited to those incurred by the system owners but also those pertaining to third parties and to the nation as a whole. For this reason the risk appetite cannot be properly captured by reference to the system owners alone but the guardians of the CNI and of the customers (for example the Regulator) who also have a role.

Key policy points:

- **Smart meters and the associated monitoring networks need to be seen, alongside the rest of the UK communications infrastructure as part of the UK critical national infrastructure.**
- **A full IT Security risk assessment should therefore be carried, covering all aspects of Smart Metering policy, if it has not been conducted already.**
- **Independent risk profiling and monitoring will be needed on an ongoing basis whether by DECC or by those acting on behalf of the CNI team.**

2) Mitigating Approaches

We note that any design to mitigate the issues in the Threat Model has to be durable; the lifetime of a meter and its supporting technology will be a minimum of 10 years whilst some commentators have indicated a half a century of life. If so the meter will see changes in the occupancy of premises, changes in providers, and possibly changes in the nature of the commodity business model. We are already seeing micro-generation of electricity becoming more common, dynamic energy auctions would only involve a streamlining of the current mechanisms for changing energy providers and changes in the attendant legislation - as well as changes in computing and attack methods. Thus, any security approach must be both flexible and pragmatic. While the security ideal would be for each provider to have their own private fibre network for their meters, which is disjoint and air-gapped from other providers' networks and the general domestic or business Internet feed to a premises, this basically is not going to happen due to the cost of installing such a system. Moreover, stand-alone networks have their own vulnerabilities.

To maintain consumer flexibility in choice of providers, all providers will need to share common meter network infrastructures. Purists would like meter networks to physically air-gapped from general-purpose domestic or business Internet feeds but given that the latter may already be carrying safety critical alarm and medical systems over the same channels the added resilience, even in those parts of the UK where this is practical, can be questioned. More-over it is not feasible in many rural areas or many export markets, therefore meters must support QoS protocols as well as cryptography and platform integrity assurance.

Key policy points:

- **Meter installers should share common network infrastructures.**
- **Meters should support Quality of Service protocols.**
-

3) Baseline Protection Recommendations

As a baseline for meter and infrastructure security specification, the following items are recommended:

Most importantly of all, meters must fail back to "dumb" operation in the absence of data network connectivity - network compromise must never deny provision of metered commodity records.

Traffic to and from meters must be encrypted, with bi-directional certificate-based authentication; meters are to include Trusted Platform Module capabilities and use attested boot functionality.

The actual choice of specific encryption or key management architectures or of specific security parameters is best left to a later stage in the design process rather than being a specifi policy point. At the policy level we wish to highlight the need for encryption (and associated key management) and assert that there are technologies available that are suitable for the required job. The specific details should be a matter for the system designers subject to the standards to be set by the National authorities. The recommendation of ECC recognises that smart meters are limited-memory environments. While commentators have mentioned the risk of advancements in quantum cryptography during the lifetime of a meter and the authors recognise this, if quantum cryptography comes to enable the brute-force cracking of RSA 4096 in practical time, the smart meter network will be some way from the top of the list of networks to redesign as a priority.

Meters must have tamper-resistant stored state (NVRAM in the form of Flash, memristor or a suitable successor technology, a Trusted Platform Module acting as a keystore and assured boot vector), and be able to run for a long time on local, guaranteed power such as battery (for gas and water meters especially) and locally log commodity consumption in the event of network outage. FIPS 140 certification should be considered, especially if the US is a target export market. For the UK market, CESG will need to be involved; a CPA profile will need to be generated for smart meters to be tested and approved against. Meters should show some readily visible evidence of their assurance; the BSi Kitemark scheme would be a good base model.

As is usual when cryptography is involved and there are multiple actors, key management becomes a very interesting subject. Our current thoughts are:

It is insufficient to just put keymat from "the big 6" utility providers in the meters; providers may change over the lifetime of the meter, as companies come, go and merge (even though cross-signing would mitigate a technical issue of consumer changing providers).

Root CAs can and will be compromised (cf DigiNotar, Comodo etc); the smart meter network will be too pervasive (CPNI may even decide it should be considered as Critical National Infrastructure (“CNI”)) to have a single point of cryptographic vulnerability such as one CA infrastructure.

This suggests all utility companies and meters would be best served by sharing physical data networks, with each company set up as certificate notaries under an instance of the Convergence system (see http://convergence.io/).

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

This also suggests that a quorum mechanism for keymat update must be created, such that existing utility companies are required as part of their operating licenses to collaborate to refresh keymat, retire old keymat and introduce new keymat into meters for new providers. A k of n scheme seems a likely candidate for such a mechanism.

Key policy points:

- **Meters must continue to function in spite of an attack or outage on the data and communications network.**
- **CESG should be involved in designing tamper-proof standards for meters to avoid the risk of damage to networks resulting from serious abuse by customers, particularly given that what is secure now may well not be in 5 – 10 years).**
- **The plans for the use of encryption , including Key Management to ensure secure communications across the Grid need further clarification and investigation.**

4) Outstanding Issues

A number of issues remain outstanding, particularly where a wholly-shared network infrastructure is required by policy or circumstances:

Enforcing QoS in the meter network becomes difficult, as the QoS protocols have to be understood and honoured by every device in the communication chain between meter and commodity provider. ISPs will have to be involved in the Smart Grid / Smart Meter programme, and there will be impacts and costs for them, too. However, this becomes less important if meters can fail back to "dumb" mode for whatever length of time a network outage may span.

Depending on smart meter roll-out schedules, the need for smart meter deployment may assist in driving pervasive IPv6 adoption. This is a benefit, although ISPs may not initially see it this way.

Where a resource exhaustion attack is launched against the smart meter network, it will be extremely difficult for the ISPs if they are required to identify the source of the attack and report it to the providers or some other authority. However, this may not be required, unless the smart meter network is classed as CNI.

The question as to whether remote update of meter software should be permitted, remains outstanding.

Key policy points:

- **Encryption must be used for all communications across the Grid.**
- **CESG must be involved in ensuring the robustness of both equipment and processes, particularly given the long life of a meter.**
- **The Smart Grid and Smart Meters are considered as parts of the Critical National Infrastructure.**

Conclusion

Smart meter security has been the topic of legitimate concerns, at the same time feeding into a growing anti-smart-meter movement in many countries. Earlier this year, researchers demonstrated serious privacy flaws in a smart meter scheme that allowed attackers to intercept meter data and determine householders' TV viewing habits and whether or not they were at home. As far back as 2010, researchers in the UK were warning that smart meter security was so poor it offered attackers a remote "kill switch" they could use against electricity consumers. As a consequence, all smart metering systems need to address security threats to data privacy and confidentiality and from unauthorised access to smart metering functions. There this report recommends that smart meters:

- **are Secure.**
- **are Reliable.**
- **Protect consumers' interests and industry investment.**
- **meet Data privacy commitments.**
- **remain easy to use by consumers and fit for purpose.**

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Conclusion

The Conservative Party remains committed to the roll-out of smart meters. The principles have remained the same but as this policy document shows the route and the time elapsed to get there have altered. Since Conservative policy was last published as part of the "Rebuilding Security" policy document several important factors have changed. Not least, we went into a Coalition in 2010 and this has skewed many of the policy initiatives from before the 2010 election. It is also important to remember that this policy cannot exist on its own. Its success or failure will also rest on sound policies for ubiquitous broadband, the smart grid and smart infrastructure.

In sum, this policy paper presents a market-led approach which will lead to a full roll-out. This provides a method for ensuring that smart meters reach the population in a way that is most likely to bring the bulk of them with the programme. It copies tried and tested technology roll-outs that have brought positive changes to both consumers and enterprises over the past twenty years, amongst which are the Internet, mobile telephony and email as some examples. It also answers the needs of investors for surety in investing in the technology.

In 2004 a number of UK energy businesses wanted to work together as a consortium to establish global leadership in this field. This would have placed the UK at the centre of the emerging smart meter market and assisted our exports. However that initiative was blocked by Ministers and the Regulator who wanted a "universal" solution that would cover all UK consumers. That solution, which remains the basis of current policy, gave no advantage to those who take a lead in giving smart meters to those of their customers who will get the most benefit (e.g. savings of 15% and more in energy consumption) and are most likely to be able to smooth their consumption (thus giving a return to distributors and generators). Therefore investment will not go ahead unless some-one else (Government or Consumer) pays. We believe that our policy redresses that balance and will give the market confidence to invest which in turn will give the consumer choice (of meters, tariffs, apps etc.) and help in propagating smart meter technology voluntarily.

The UK could still be at the centre of the production of smart meters, related apps and technology that could be exported to the EU and further afield. As the Government is committed to an export-led recovering which is manufacturing based then this policy clearly assists that one in achieving the objective for UK plc. This in turn has a positive effect on employment and creates skilled jobs. The steady, market-led roll-out of smart meters will also create jobs for installers. Instead of rushing through a mandated roll-out within a set timetable, thus creating a jobs bubble and an unemployment burst, the CTF policy offers steady and long-term employment.

The CTF believes that this policy offers a secure and economically sound methodology for turning the UK into the market leader for smart metering and looks forward to developing complementary policies for the Smart Grid, Smart Infrastructures and Broadband to complement this policy on Smart Meters.

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH
Email: secretary@conservative-technology.org www.conservative-technology.org

Acknowledgements

The CTF would like to thank the following:

Laura Sandys, MP for chairing the Group.

Sophie Thompson for her organisational assistance

Philip Virgo and Terry Bowers of the Conservative Technology Forum for their guidance, input and assistance in preparing this document.

Ian Taylor of Living PlanIT S.A.

The authors:

Andrew Henderson, Wychwood Consulting Ltd

Richard Hampshire, Digital Policy Alliance

Duncan Southgate,

Cllr Gary Waller

Andrew Churchill,

Jim Cessford, Marc Hobell,

John Riley, Peter Drake, James Taylor, Simon Honey

Justin Anderson, Dave Walker,

Simon Sabel,

Nick Wood-Dow, Lord Renwick

Stephen Pattison, Zoe McLeod,

Tara Singh, Gary Highton,

And also the three speakers from our first meeting who helped to get us started:

Liam O'Sullivan, UK Power Networks

Charles Hendry MP

Ash Pocock, EDF

For further information please contact:

Andrew Henderson – andrew.henderson@wychwoodconsultingltd.co.uk

Or www.conservative-technology.org/

c/o Conservative European Parliament Office, Europe House, 32 Smith Square, London SW1P 3HH

Email: secretary@conservative-technology.org www.conservative-technology.org

Appendix – Security and resilience

1.1 Bibliography

ISO/IEC 27001:2005 Information technology – Security techniques management systems – Requirements.

ISO/IEC 27002: 2005 Information technology – Security techniques – Code of practice for information security management.

BS 25999-1:2006 Business continuity management – Part 1: Code of Practice

BS 25999-2:2007 Business continuity management – Part 2: Specification

Department of Energy and Climate Change – Smart Metering Implementation Programme – 31 May 2012.

1.2 Appendix: Threat Model

In order to produce a specification from which to then formulate a set of security design requirements, it is first necessary to formulate a threat model based on requirements for and attacks against *confidentiality*, *integrity* and *availability* as viewed by a Consumer, a Provider and any other third parties. There is also a need to include *legislation* (this latter term being a catch-all for privacy requirements etc), although this aspect should be addressed by an author with suitable training and experience in relevant aspects of law.

While a formal methodology such as ISO 27001 or HMG IS1 is not adhered to, elements of these are involved in this approach. Also, it is important not to lose sight of the need for pragmatism; there is little virtue in making an aspect of a digital solution far more secure than the pre-existing analogue one, for the same threat.

It is also noted that smart meters are embedded systems. Therefore, additional requirements are recommended that any security solution be effective for the lifetime of a smart meter (half a century or so) and the technology changes during that lifetime, and flexible in the face of changes in identities of both consumers and providers, while also being buildable to a low cost point. While the expected scale of the solution is large (the 2011 Census indicates 33 million meterable dwellings and other buildings for the UK alone, and there is intention in the Smart Meter programme to address a significant potential export market) and therefore fabrication of specialist parts could be justified, the need to keep the design sufficiently flexible as to deal with different mains voltages, currents and frequencies, and different means of data communication across at least the lowest two levels of the OSI stack, suggests that using current commodity parts would be the conservative approach.

Also, the smart meter system will very probably be a monoculture, from a control and measurement perspective; while smart meters will most likely be deployed to meter all commodity services (electricity, gas and water), the "smart" elements will need to conform to a set of common standards, and owing to matters of commercial economics of scale, will likely contain mostly the same chipsets, no matter which meter vendors are involved.

1.2.1 For the Consumer

1.2.1.1 Threats from other Consumers

(ie, other actors within the same physical network, involving the same provider):

1.2.1.1.1 Confidentiality

In the analogue world, meters are readily accessible; except where a meter box is located within a secondary security perimeter such as a garage, meter boxes are trivially accessible to anyone who visits a property, as any meter box key (or even a pair of long-nosed pliers) opens any meter box.

Meter readings are not secrets, nor do they intrinsically need to be. Information which can rightly be considered sensitive, however, is the rate of change of the meter reading, as it discloses the commodity consumption within the property - especially when commodity consumption is measured on a daily basis over time. This could enable a would-be burglar with remote access to a meter to make a sound estimate of when a property would be likely to be unoccupied based on changes in commodity consumption, and also for electricity meters, whether it would be likely to contain desirable electrical appliances.

Therefore, both meter reading output and requests to a meter for output must be encrypted with bidirectional cryptographic authentication, and metadata (such as the frequency of communication between meter and provider, and the volume of data passed between meter and provider over time) must not reflect changes in rate of commodity consumption.

Where smart meters are designed to use wireless communications to provide some real-time or near real-time energy consumption information to a console within the household or business, measures must be taken to ensure that wireless signals for meters in different properties cannot interfere with each other. This suggests frequency-hopping within a spectrum, rather than division of a spectrum into a small number of channels.

1.2.1.1.2 Integrity

While there is no obvious and mundane good reason for a consumer to attempt to modify the reading of another consumer's meter (although some "movie-plot" reasons exist), the repercussions of such modification would be likely to involve protracted dispute with a provider.

Also, it must be borne in mind that the smart meter network will be both extensive and a technical monoculture. In reality, as many households have separate gas, electricity and water meters, the estimated number of 33 million UK-based meters is likely to be higher. If a meter's operation could be subverted such that it was able to perform functions unrelated to its intended purpose, the resulting "botnet" could be used for various interesting purposes (the set of those purposes being dependent on whether the smart meter network was physically isolated or run over a pre-existing Internet connection as a VPN), such as brute-force cracking of illegitimately-obtained encrypted material such as passwords.

Some meters have environmental factors (such as high electrical currents) which dissuade the casual physical tamperer from attempting to tamper with them; however, the "smarts" of a smart meter must be extremely difficult to access for tampering purposes. Certification to a standard such as FIPS 140-2 is suggested

for the export market; for the domestic market, CESG should be consulted for their recommendations. Cryptographic material should definitely be stored in some kind of hardware security module; a Trusted Platform Module should suffice for this purpose, and it is noted that this also enables meter control software to be written with the integrity verification capabilities afforded by Attested Boot.

1.2.1.1.3 Availability

Loss of data network connectivity to a smart meter, must never result in cessation of supply to the customer of the commodity being metered. In this circumstance, smart meters must fall back to behaving as today's typical ("dumb") meters do.

Smart meter data channels tunnelled over existing physical Internet infrastructure may require support for bandwidth guarantees (to mitigate against flooding attacks against meters, or DoS attacks by compromised meters), but this should probably be a low priority requirement, if meters are designed to continue to operate in the face of complete data connectivity outage.

The question of the nature of the link between meter and provider, in terms of whether it is dedicated or shared bandwidth over a pre-existing domestic or business connection, is important. Current domestic and business Internet infrastructure has quality of service ("QoS") guarantee mechanisms which are limited at best, and the natural requirement for QoS protocols to be understood in all parts of the infrastructure will involve considerable work on the part of ISPs to implement.

1.2.1.2 Threats from Providers

1.2.1.2.1 Confidentiality

While attitudes to personally identifiable information ("PII") mishandling have changed since the HMRC child benefit incident of 2007, large-scale inadvertant publication of millions of customer names and addresses (with or without meter readings) would be damaging not only to the provider involved, but also to some members of its customer base. Therefore, meters must be identified with a unique ID and key pair (without customer metadata) only, with customer details being held by providers in separate databases and mapped in a one-way fashion.

1.2.1.2.2 Integrity

The question of whether smart meters should have the ability to have their software updated remotely, is a subtle one. While the axiom that "a sufficient condition for software triviality is that it be bug-free" is often quoted, the ability to modify smart meter software either remotely or in situ without swapping-out hardware opens opportunities for vendors to inadvertantly compromise the operation of millions of deployed meters by pushing faulty software updates. Requiring updates to be carried out by on-site engineers would have the benefit of issues becoming detectable while relatively small numbers of updates had been made, but the expense associated with this mode of operation would be large. This is a particular example where a formal mathematical risk assessment, inolving the characterisation of the threats, the probabilities of them being

realised, and the consequences of them being realised, is definitely necessary to inform the decision process.

It is noted that smart meter "hacking tools" already exist (http://www.securityweek.com/open-source-smart-meter-hacking-framework-released), however their impact remains limited as local access to the meter is required.

1.2.1.2.3 Availability

Issues of availability associated with activity of other customers are covered in 1.2.1.1.3 above; other availability issues are almost all associated with unrelated parties, and are covered in 1.2.1.3.3 below.

1.2.1.3 Threats from the Rest of the World:

1.2.1.3.1 Confidentiality

The threats of non-customers accessing meter data (and their remediation) are the same as those of customers doing so, as described in 1.2.1.1.1.

1.2.1.3.2 Integrity

The utility (and hence desirability) of perpetrating attacks in this context are highly dependent on whether the meter data network can be routed to, from the Internet at large. If it can, and if a meter can be subverted to connect to the wider Internet, then meters become a very large and attractive monocultural system for criminal activity; effectively, every smart meter could become a participant in a botnet. As with botnets based on conventional computers, meters could be used to perpetrate distributed denial of service attacks ("DDoS"); while their intrinsic computing capability would be very limited, the large number of meters mean they could still be useful in attacking security problems that can be parallelised easily and where the computing requirement for completing a single iteration of a parallelisable operation is small (such as password cracking). We note that PC graphics cards containing large numbers of simple processing units have recently come into vogue for brute-force password cracking; a botnet of smart meters can be thought of in similar terms.

Alternatively, if there was simply a desire to disrupt operations at a commodity provider, successful attempts to modify readings on large numbers of meters would be a very effective method of tying-up a provider's customer support team, and causing considerable inconvenience to their customer base, as well as leading to considerable engineering effort to find and patch the exploit vector.

1.2.1.3.3 Availability

Denial of service ("DoS") attacks could be perpetrated against the meter data network, by splicing equipment onto a connection (at a meter or junction / distribution box). Meters must "fail back to dumb" in the event of loss of data connection, and must be resilient to data flooding attacks.

Construction, renovation or demolition work could result in data cables carrying meter traffic accidentally being severed. Where meter connections are wireless, construction of new buildings could result in loss of line of sight from antenna to,

or creation of radio shadow in, a meter location; planning applications will need to take account of this.

We note that the smart meter data network is not expected to be physically resilient (although a wireless network may prove more resilient than a wired one, in areas with good mobile 'phone coverage); the commodity supply network is itself not physically resilient, so pragmatism takes precedence.

Where buildings which require supply resilience (such as datacentres) have multiple power feeds, we note that the hard requirement for smart meters to fail back to dumb operation in the event of connection outage does not require similar resilience in the data network; meters on different commodity feeds from different suppliers can share the same data network, particularly if they do not share common vulnerabilities.

1.2.2 For the Provider

1.2.2.1 Threats from Consumers

1.2.2.1.1 Confidentiality

Again, events which result in publication of customer data (as per 1.2.1.1.1) are harmful to the provider. Attempts to break into the customer database can be mitigated to some degree by dividing fields across different databases, as well as adding “the usual” protection layers commonly specified by IT security architects.

We recognise that providers will already have protection mechanisms they deem appropriate on their Internet-facing customer account querying and bill payment systems; they must be just as mindful in the protections applied to their smart meter data network connections.

It should not be forgotten that customers are also potential burglars, as in 1.2.1.1.1; information leakage from a meter which informs the committing of a crime may result in some culpability being levelled at the provider.

1.2.2.1.2 Integrity

The smart meter is a communications device, connected to a network in a physical environment under the control of the consumer. A skilled consumer could connect another device (such as a laptop) to the smart meter data network (either inline with the meter, or attempting to impersonate it) and from there, attempt attacks against the smart meter data network.

A consumer could also attempt to impersonate a provider, in terms of pushing non-functional or malicious software updates to meters. If remote software update (by either push or pull) is to be permitted at all, code must be cryptographically signed and verification of keys mandated before the software is copied into active (as opposed to scratch) storage in a meter.

Also, if a consumer is also a micro-generating provider with non-uniform power output (who has solar panels on their roof, a wind turbine on their chimney, etc), they could attempt to modify metering data to defraud the main provider.

1.2.2.1.3 Availability

Attacks as described in 1.2.1.1.1 and 1.2.2.1.2 could also include those aimed at resource exhaustion (“flooding attacks”). Meter data network bandwidth to each meter must be preserved using QoS mechanisms; as well as ring-fencing meter bandwidth, switching infrastructure carrying meter data should be configured to detect and report on anomalous traffic volumes, such that the provider is furnished with information to trace the physical location of such an attack. This is relatively straightforward in the context of a separate, physically isolated meter network, however where meter data traverses a shared infrastructure, it may not be realistically possible (especially the attack tracing element).

1.2.2.2 Threats from Other Providers

1.2.2.2.1 Confidentiality

As another point of data ingress to the provider, the smart meter data network must be protected from snooping and tampering by other providers, from the perspective of industrial espionage. For example, a rival provider who learns the identity of a large consumer along with accurate details of their consumption of a commodity could tailor an offer to that consumer and approach them, with a view to attracting their custom away from the current provider.

1.2.2.2.2 Integrity

Going beyond industrial espionage, if providers share a common network for meter connectivity, a provider could attempt to disrupt the operation of a rival provider's meters or the systems which control and read them, in order to focus their engineers and support desks on addressing the issue, and adversely affect their standing and share value. We recognise that the likelihood of this attack being considered or attempted, is limited, although it must be noted that a provider would be likely to have considerable knowledge which would be useful in executing such an attack, owing to monoculture issues and their ability to maintain their own meter network.

1.2.2.2.3 Availability

The threat here, is the same as in 1.2.2.2.1 above, with the addition of attacks against the meter-to-provider network as well as the meters themselves.

1.2.2.3 Threats from the Rest of the World

1.2.2.3.1 Confidentiality

The threats in this context are covered in 1.2.2.1.1 and 1.2.2.2.1; only the actor changes.

1.2.2.3.2 Integrity

The threats in this context are covered in 1.2.2.1.2 and 1.2.2.2.2; only the actor changes.

1.2.2.3.3 Availability

The threats in this context are covered in 1.2.2.1.3 and 1.2.2.2.3; only the actor changes.

1.2.3 Threats to the Rest of the World

1.2.3.1 From the Consumer

1.2.3.1.1 Confidentiality

If a meter's operation could be subverted such that it was able to perform functions unrelated to its intended purpose, the resulting "botnet" could be used for various interesting purposes (the set of those purposes being dependent on whether the smart meter network was physically isolated or run over a pre-existing Internet connection as a VPN), such as brute-force cracking of illegitimately-obtained encrypted material such as passwords.

1.2.3.1.2 Integrity

No threats have been identified, with this combination of actor and subject.

1.2.3.1.3 Availability

As per meters-as-botnet-nodes and a resulting ability to use them to DDoS other networks, above.

1.2.3.2 From the Provider

1.2.3.2.1 Confidentiality

No threats have been identified, with this combination of actor and subject.

1.2.3.2.2 Integrity

No threats have been identified, with this combination of actor and subject.

1.2.3.2.3 Availability

No threats have been identified, with this combination of actor and subject.

1.2.3.3 From Other Entities

1.2.3.3.1 Confidentiality

As per meters-as-botnets to apply brute-force cracking techniques to encrypted material, above

1.2.3.3.2 Integrity

No threats have been identified, with this combination of actor and subject.

1.2.3.3.3 Availability

As per meters-as-botnet-nodes and a resulting ability to use them to DDoS other networks, above.