Written evidence submitted by Smart DCC (EVP0090)

Introduction

The Data Communications Company (DCC) greatly appreciates the efforts the Transport Select Committee has made in its inquiry into accelerating the shift to zero emission vehicles, and welcomes the opportunity to respond to the ongoing inquiry -- particularly with regards to the actions required by Government and private operators to encourage greater uptake of electric vehicles and the infrastructure required to support them.

The DCC is a licensed private sector company, regulated by Ofgem, which was established in 2013 to operate the central, standardised data and communications infrastructure for smart metering in Great Britain. In effect, the DCC is the secure digital spine of Britain's energy system connected to all energy retailers, national grid and regional grid.

The DCC supports the roll-out of second-generation (SMETS2) meters, as well as the migration of c.17 million existing first-generation (SMETS1) meters onto our system, upgrading these devices over the air and enabling them to be fully interoperable meaning consumers can switch with no loss of functionality. We provide the central role and platform to support Ofgem's programme to deliver a faster, simpler central switching service for energy consumers and will play an integral role in the delivery of domestic half-hourly settlement should this go ahead.

You may be aware that the Department for Business, Energy & Industrial Strategy (BEIS) has consulted on the use of the DCC infrastructure to facilitate nationwide EV charging. Consequently, we have invested significant time in considering the functionality which would be of benefit to end-consumers, as well as other market participants such as the Distribution Network Operators (DNOs). Some of that thinking has already been turned into practical functionality as, in response to a BEIS mandate, DCC has implemented a proportional load control capability to enable authorised parties to control the charging of EVs remotely, via the DCC network.

As we articulate through this response, the DCC believes that in order to encourage greater uptake of electric vehicles, Britain's EV charging network needs to be:

1. **A genuinely competitive market** underpinned by standards that work on behalf of consumers to avoid people or businesses becoming "locked in" to poor deals.
2. **Secure by design** – end-to-end cyber security designed in to defend against manipulation or disruption, and to build consumer confidence.
3. Recognised as being part of an **integrated energy system** with asset visibility and load control built in from day 1, together with the appropriate controls.
4. **Open, yet secure and privacy protected, data** to facilitate new market entry with innovative solutions and insights.

5. A **platform for innovation** – offering a consistent and high-quality experience to consumers wherever they are in Britain, but also providing an environment through which new and innovative services can be developed and deployed.

The problems currently facing the roll-out of EV charging infrastructure

There are now almost 400,000 EVs registered in the UK. The Government continues to support the growth of this market through incentives for the purchase of EVs and home chargepoints, whilst also funding bodies such as local authorities through a range of competitive schemes and grant funding. At first sight, one might say that the market has developed well; however, given that road traffic accounts for around 20% of carbon emissions and EVs are still very much the minority choice, there is still a long way to go.

The UK needs to rapidly roll out EV charging infrastructure across the nation to meet the Government's deadline of 2035 to end the sale of all petrol and diesel cars. This roll-out needs to ensure that the industry is not only delivering the right infrastructure in the right locations but that it is delivering an EV charging network that is ubiquitous for all motorists regardless of chargepoint operator, car model, or energy provider.

We believe there are three key issues which need to be addressed as a priority by Government and private operators to encourage greater uptake of electric vehicles and the infrastructure required to support them.

1. *Consumer issues*

Unhealthy features to the market are already starting to appear, such as the proliferation of proprietary solutions locking in consumers, which need to be addressed before they become truly embedded. For example, per kilowatt-hour pricing for private driveways versus public chargepoints will yet again see digital divides and penalise those least able to pay higher costs. Whilst EV chargepoint suppliers and retailers need to make a return and should be able to charge a premium for faster charging, for example, consumers must be able to choose which supplier to use and not be artificially locked in.

Currently, local authorities are working with a variety of car manufacturers, such as Tesla, and chargepoint operators, such as bp pulse, to roll out EV charging infrastructure in their local area. However, the industry does not currently have any design, interoperability or security in place, which may result in motorists being locked into using one type of car model or chargepoint service due to the lack of competition in their area. For example, non-Tesla EVs can use a Tesla charging station, but they will have to purchase an adapter first. While if you want to charge your EV, you have a choice of over 40 charging networks, most of which operate in different ways and require you to set up an annual or monthly subscription.

2. *Security issues*

Without any industry security standards in place, chargepoint security is currently left to each operator to apply as they see fit, leaving chargers and the grid vulnerable to cyber-attacks. As demonstrated through a simulated hack by a group of engineers from the Southwest Research Institute (SwRI) in Texas, hacking an EV while it is charging is remarkably easy and can be done using low-cost hardware and software. If this issue is not addressed as a priority, the UK's future energy infrastructure would be vulnerable to cyber threat just as the number of EVs on Britain's street increases.

A lack of standards also runs the risk of each individual chargepoint operator developing their own level of cyber security to protect their individual customers resulting in some consumers potentially being left vulnerable to hackers due to a low level of security in their chosen EV charging network.

3. *Load control issues*

With the acceleration of the ban of the sale of new petrol and diesel vehicles to 2030, demand for EVs will continue to grow exponentially in the coming decade. Government projections forecast that EVs could account for up to 10.6 million vehicles on UK roads by 2030. As EV demand increases, so will demand for electricity to charge the vehicles. This means significant pressure will grow on the electricity grid to balance the energy demand and ensure it does not lead to local power outages. Currently, the fragmented roll-out of EV charging infrastructure means load control can only be done locally and in an isolated manner.

As it is likely to become one of the leading drivers of electricity usage, the EV charging network must be recognised as being part of an integrated energy system with asset visibility and load control built in from the outset, together with the appropriate controls. An electrification project of this scale requires a grid that can not only balance load control effectively, but importantly one that is protected from any cyber-security threats. This is why finding a way to secure load control will be a key component in accelerating a futureproof shift to zero emissions vehicles.

Why a secure centralised network is key for accelerating the shift to zero emission vehicles

In order to address the concerns stated above, we believe EV charging infrastructure should operate on a universal and centralised ultra-secure network. Utilising a pre-built highly secure network, with a reach greater than superfast broadband, will enable faster deployment of chargepoints, act as a platform for innovation and create greater consumer choice. It will also reduce the skills required to install EV chargepoint telemetry with a plug-and-play communications approach to installations.

1. **How a secure centralised network helps to create greater consumer choice**

We can already see the emergence of poor customer service in relation to EV charging through, for example, the numbers of chargepoints which are found to be routinely out of commission, 'landgrabs' by operators, and use of proprietary systems and contracts which lack mutual interoperability and therefore risk locking in consumers to a single provider. These practices must not be allowed to develop in the EV charging market: having to unwind them later would be time-consuming, difficult and expensive.

A secure centralised network for EV charging seeks to address those concerns by focusing on:

- Ease of use which, as far as possible, enables any consumer to turn up and use any chargepoint.
- The option that electricity supply and billing can form an extension of a domestic contract, with the electricity being billed at a known price and presented through one household bill for a consumer, when so desired.
- Interoperability – for consumers, there needs to be simple and rapid switching between electricity providers without loss of core functionality. Ideally, a consumer should never have to contemplate a change in charging hardware in order to switch between suppliers.
- Tie-in agreements that are fair to both the provider and consumer - for example, to subsidise the cost of a home chargepoint.

2. How a secure centralised network helps to protect the security of the system

As we reach 2030 and beyond, the UK will come to rely heavily on the multitude of charging networks, which will have access to consumer's payment details and direct access to motorists' EVs when connected. It is therefore paramount that Britain's EV charging infrastructure has the right security in place to protect consumers who use these networks.

The UK's EV charging infrastructure needs to be considered, if not designated, as "Critical National Infrastructure" and recognised as an integral part of the wider energy system. The security of the EV charging infrastructure will need to meet the requirements set down by the NCSC, ensuring its capability to defend against a range of current and future cyber threats and threat actor sophistications and motivations. Any requirement to retrofit the security of a heterogeneous EV charging infrastructure at scale would be costly and time-consuming which, given the 2030 target, could undermine the Government's policy intentions.

It is crucial to remember that this not just about EV charging – it extends into the District Network Operators or the System Operator's ability to mobilise demand-side response through smart grids. Over time it will become part of wider domestic energy management systems including vehicle-to-grid, storage and home generation. So, EV charging infrastructure must not be allowed to become a weak link which enables criminals or hostile forces/states to attack our energy and payment systems.

3. How a secure centralised network manages load control

It is well understood that the adoption of EVs has the potential to put considerable strain on both the electricity networks and generation capacity. Reinforcing the local distribution networks and building new generation will come at a significant cost which will need to be picked up by the consumer: minimising any such investment should therefore be an important consideration when designing a nationwide EV charging infrastructure and its regulation.

The logical solution to this would be to introduce central asset registration – as currently deployed by the DCC within the installation of SMETS2 meters – which is automated during the commissioning process. This will assist the DNOs in managing the additional load on their networks as EVs are rolled out, both in terms of pro-active planning but also in making use of load control capability to ensure day-to-day balancing of the grid. In addition, a central asset register will provide key data for consumer services, such as mapping of available chargepoints.

Recommendations

The issues highlighted in this response can be summarised as:

- ensuring every user can use and access any charger across the country
- enabling demand to be managed, to prevent outages and protect the grid
- ensuring security across the network

The most effective way to address these is to create an EV backbone that both connects every charger to a single network and enables communication to and from every public and private charger. Such a backbone underpinning the charging system would allow Britain to achieve the necessary EV adoption rate and pace of transition required to enable the Government to meet its Net Zero targets. Visibility of usage across many suppliers and across the country is also key to smoothing user adoption and protecting the nation's grid.

Rather than inventing – and building – a new network from scratch, the easiest option would be to use the DCC's existing network. Already there are more than 10 million meters in homes and small businesses connected to this network and, by 2025, the aim is to have 30 million homes connected. Using the DCC secure platform as a backbone to underpin the charging system nationwide would avoid much of the cost and complexity of developing and installing a new network to connect EV chargers.

February 2021