Data Communications Company

Factsheet

Security and privacy

Role of the Data and Communications Company

The Data and Communications Company (DCC) is responsible for establishing and managing the infrastructure necessary to support the main roll out of millions of smart electricity and gas meters to homes and small non-domestic properties across Great Britain. It forms part of the Government's wider Smart Metering Implementation Programme.

Funded by the energy industry, the infrastructure will connect smart meters in people's homes to the business systems of energy suppliers, network operators and other authorised users. It offers a secure, consistent service and avoids the complexity and duplicated costs of energy suppliers installing their own networks.

The network will transform how energy is supplied and give consumers greater control over their energy use.

Security and privacy is at the heart of the DCC network

Private data kept private

We know that end-to-end security and privacy of the smart metering network are critical to gaining public confidence and the widespread adoption of smart meters.

That's why we take these matters seriously and why the government has put in place strict rules to give consumers control over who can access their energy data and for which purposes. We recognise the fact that smart meter consumption data belongs to the consumer and that they should retain control over it.

Smart meters will not connect to the public internet but operate on a secure system, based on national and international security standards. This will ensure a consumer's data is visible only to their energy supplier and authorised parties where the consumer has given consent. Data is stored on a consumer's meter – there is no central database.

Energy suppliers will be allowed to access monthly data for billing purposes but consumers must give their consent to sharing more frequent and detailed data.

Secure data kept secure

To protect against the threat of unauthorised users accessing the network, a sophisticated system has been designed for protecting commands sent to meters. At the heart of the system is a new public key infrastructure which employs technology widely used by, for example, the banking industry.

Messages containing energy consumption data travelling along the DCC network will be encrypted at all times. Energy suppliers encrypt the information using a service called Smart Metering Key Infrastructure. DCC does not store, analyse or have access to consumers' data. Indeed, DCC does not have the ability to decrypt the data – that can only be done by the energy supplier.

Security governance and oversight

Consumers, energy suppliers and government all want assurance that the DCC network is secure and will remain so. To give this, a clear hierarchy of governance and oversight is in place to make sure that there are no single points of potential failure in the system.

Uppermost, the Smart Energy Code (SEC) Panel, the body that oversees industry organisations involved in the end-to-end management of smart metering, receives expert advice from security professionals from the energy industry and government.

DCC must also appoint independent security experts to examine security risks and controls during the development of the network. These experts report directly to the SEC

Panel at key stages of the programme. Security testing is embedded in the wider testing programme before the network goes live and will continue once the network is live.

In November 2015 DCC achieved ISO 27001 certification status. ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. Service Providers will gain their certifications before the go-live of DCC Solution.

An organisation that qualifies as a User of DCC services must first undergo a robust security and privacy assessment and be subject to regular audits.

Finally, Smart DCC Ltd must carry out audits, assurance and testing of its providers to ensure that risk assessments are being carried out and actions implemented.

Securing the future

The DCC system is built on a private network that is securely protected from external threats. However, as these are constantly changing, we conduct regular security audits to identify and mitigate any potential risks.

Moreover, DCC has forged links with government agencies and other bodies, such as the UK Centre for Protection of the National Infrastructure, to review new threats as they emerge and works hard to make sure the network is protected against them.

For more information

Please contact the DCC security team at contact@smartdcc.co.uk

December 2015
www.smartdcc.co.uk