Smart Security Governance

The implementation of Smart Meters is complex due to the wide range of new technologies required to manage and maintain new computer-based infrastructure, monitoring systems and reporting applications. We need to ensure a high level of security is in place to protect against malicious parties wanting to compromise or disrupt energy supplies. The Department of Energy and Climate Change (DECC) has mobilised programmes to address cyber security which include input from UK Government intelligence agencies, energy suppliers, smart meter manufacturers, large systems integrators and security consulting organisations.

The key security challenge the energy industry faces is the adoption and implementation of best practice standards and frameworks for security, including skills vetting and resourcing, governance, technical build testing, controls and awareness to ensure threats to the UK CNI (Critical National Infrastructure) are appropriately managed. The creation of the Smart Energy Code (SEC) and the Data Comms Company (the DCC) can further enhance the integrity of settlement between Balancing and Settlement Code (BSC) parties.

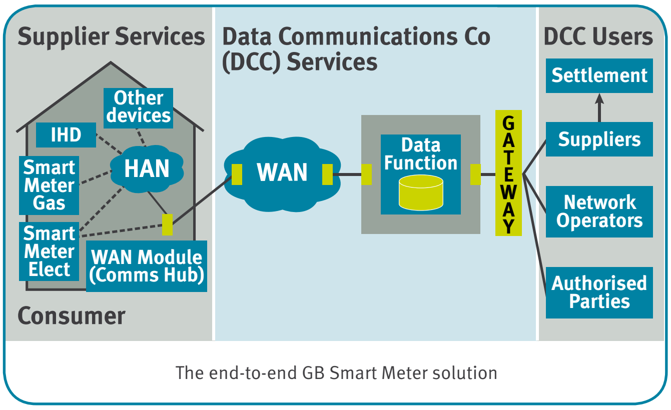
> The SEC and the DCC also provide vehicles to drive a culture of best practice security across the GB smart solution and this is an approach ELEXON fully supports going forward.

The need for clear definition of roles and responsibilities

In the new smart metering world, there are numerous participants that have a keen interest in knowing that the central systems are secure – not least consumers, DECC and Ofgem. However, ensuring that the end-to-end system is secure involves co-ordination across a number of industry parties as the DCC is not responsible for all the potential points of threat to the central system. The SEC is central to defining the roles and responsibilities for DCC and users as part of the wider security governance arrangements.

The DCC Licensee will have overall responsibility for security of the central systems that provide connectivity, data carriage and translation between the customer premise and the DCC user. However the DCC is not directly responsible for the equipment at the customer premises which will be the source of the data needed by the DCC user. Suppliers are responsible for installing smart meters, in-home displays, the home area network (HAN) and the Wide Area Network (WAN) module – although the WAN modules will be provided by DCC.

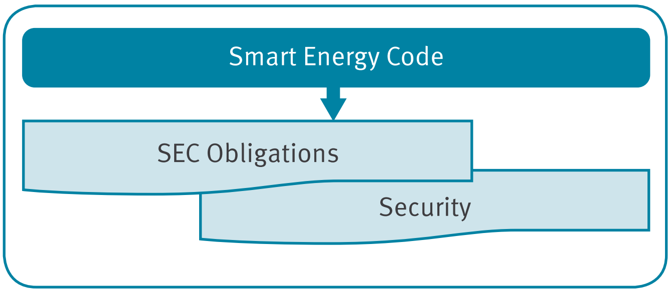
The SEC therefore needs to set out an assurance regime for DCC users to ensure that they and their systems are robust to mitigate against potential threats to the security of the end-to-end smart metering systems.



The end-to-end GB Smart Meter solution

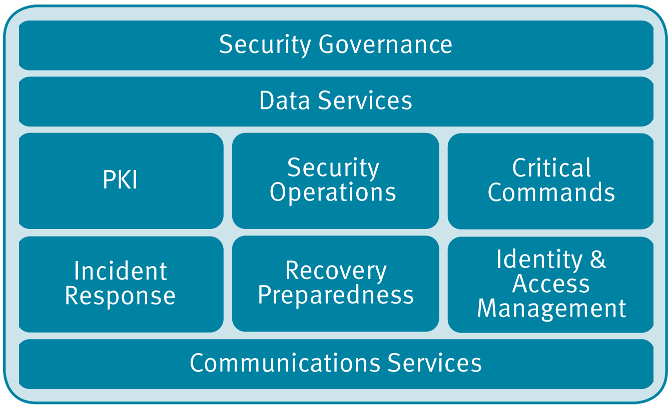
Who manages this regime?

A SEC Panel will be established to manage the SEC. This Panel will have an interest in the performance and security of the services provided by DCC, but also of the equipment installed by suppliers. It will also need to ensure there are no threats arising from third parties wishing to connect to smart meters via the DCC or use DCC services. However, the DCC must be certain that users and their equipment pose no threats to the central services. It therefore is essential that DCC has visibility and contributes to the SEC assurance regime which deals with DCC users and user equipment.



We expect the SEC Panel to make use of committees comprised of relevant experts to determine matters of security. Such a committee could advise on the risks and mitigation required for potential changes proposed under the SEC. The security group could also advise on the costs and impacts of different solutions on any proposed changes.

However, how changes are implemented to DCC systems and managing the ongoing security of the central systems must remain the decision of DCC as it holds ultimate responsibility for those systems. A further role for the security group may be to determine the mechanism and timing for applying emergency fixes to smart metering equipment.



What are the key DCC security services?

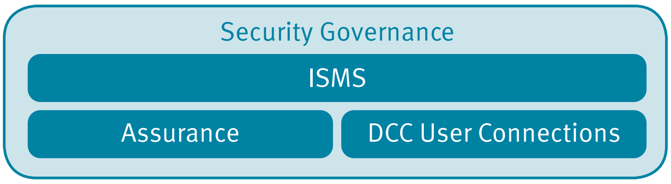
The DCC will be a highly trusted security entity responsible for delivery of key security services to the industry, a number of which do not exist within the industry today. The model above identifies key security process areas.

This is not a comprehensive list. However it is what we see as being integral to a successful DCC;

Security Governance	Information Security Management System, Assurance & User connections
Data Services	Meter data storage and translation services
Public Key Infrastructure [encryption services]	The security trust hierarchy between DCC users and smart meters in the home
Security Operations	Meter and systems alert logging, triage and categorisation, threat intelligence and technical test coordination
Critical Commands	Source validation and signature checking to ensure critical commands (remote disconnect, firmware upgrade etc.) come from legitimate sources and have not been altered prior to being pushed to meter devices
Incident Response	Meter and systems alert response and escalation
Recovery Preparedness	Crisis Management, Business Continuity, IT Disaster Recovery
Identity & Access Management	Provisioning users and ensuring access is granted based on need-to-know
Communications Services	Meter data transmission

What is the scope of security governance for the DCC Licensee?

We support the current approach that the DCC Licence entity must be separate from the Data Services Provider (DSP) & Communications Service Provider (CSP) to ensure a degree of independent governance and assurance for security. All DCC entities must work closely together in defining and delivering the DCC security strategy. The following high-level model should be used by the DCC Licence entity going forward;

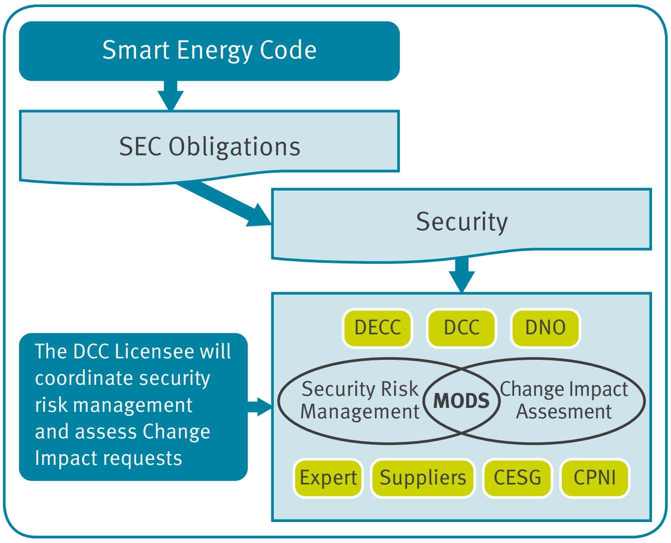


Information Security Management System (ISMS): the ISMS for the DCC Licence entity must be scoped and implemented to manage the governance aspects of DCC security and to coordinate the management of risks for key security services and business processes across DCC entities and licensed users.

Assurance: a key process within DCC security governance will be to regularly review and audit its service providers and Licensed users for certification against the relevant International Standards Organisation (ISO) standards and the DECC security requirements.

DCC User Connections: Processing DCC User Licences requests and the associated vetting of organisations wanting to become DCC Users is a key business and security process. DCC Users will need to be compliant with the DECC security requirements and ISO 27001 for information security.

Wider security governance



Security governance for the wider smart solution needs to be driven from the DCC Licensee entity as an advisory group under authority from the SEC. All three parts of the DCC organisation (Licensee, DSP and CSP) must work as a cohesive security team to deliver the overall DCC security strategy. Additionally, the DCC will be responsible for security risk management and impact assessments for Modification requests to the SEC on an ongoing basis. This will require the creation of a forum for security with representation and input from key organisations across the industry. For security governance to be effective, this group must be authorised to make decisions on risks and proposed changes to the SEC which may impact the security of the end-to-end smart meter solution.

How can we ensure the DCC is built securely?

Establishing the DCC before the end of 2014 is an ambitious time frame and risks to the security of the solution during design and implementation must be seriously considered. In order to do this effectively, security governance for the DCC must begin being established prior to the initial phases of the DCC solution design and build phases. Metrics for security controls implementation and maturity must be in place, monitored and form part of DCC ISMS scoping activities. There will be challenges around establishing this security governance prior to the initial design and build phases of the DCC due to current DCC procurement timelines. However this should not detract from the need for these activities to be prioritised along with development of the SMETS (Smart Meter Equipment Technical Specification).

What does ISO27001 certification & compliance mean?

Alignment to ISO27001 for Information Security will create a level playing field across the industry. We are only as good as the weakest link so the industry needs to mature collectively. This will give the Government and the public comfort that the security of the CNI is implemented to an acceptable standard. The level of implementation will be different for various organisations depending on what role they play within the industry and specifically the end-to-end smart meter network. Currently, there are two main “security programme state” categories identified within the DECC security requirements;

Certified: currently, DCC entities are the only organisations within the end-to-end smart meter solution which **must hold a valid ISO27001 standard** certification. The scope of certifications must be applicable to all smart meter processes and supporting applications, databases and infrastructure. Other certifications also apply to the DCC for staff vetting, incident response, IT recovery readiness and business continuity.

Compliant: any non-DCC organisations which are directly connected to the GB Smart solution **do not need to certify their systems and processes**, however they must be able to prove their end-to end solution is compliant with ISO27001.

The DCC must be ***Certified*** and have a very high level of controls assurance though a formal certification and audit programme. This is because it will control connections between smart meters in the home and the energy suppliers. ***Compliant*** organisations are also required to assess the risk their third-party connections may present to them and therefore the smart meter network. It is possible potential threats could be introduced via the supply chain and is traditionally an area of assurance which is not closely monitored.

Security governance under the BSC today

The many systems and processes managed by ELEXON are integral to operation of the electricity trading arrangements. Whether, for example, we are registering parties, processing and reporting against energy trades, or processing balancing actions taken by National Grid on our Balancing Mechanism Reporting website, our systems and processes require high levels of confidentiality, integrity and availability. ELEXON achieves this through alignment and compliance with ISO standard 27001 for Information Security and strong, commercial-level controls. A robust security policy is in place and is regularly reviewed along with skilled information security resource responsible for the ELEXON ISMS and reviewing risks to existing processes and supporting infrastructure.

How is ELEXON adopting its security posture to support the UK smart meter rollout?

The security environment within ELEXON will continue to mature and evolve as threats to the energy industry emerge and evolve. Alignment and compliance with ISO27001 ensures ELEXON has an acceptable level of security in place for delivering the BSC today and to support the industry smart meter roll out going forward. This work also includes having engagement with industry around development of the SEC in relation to security and how this might be successfully managed via the DCC. We are keen to talk with our stakeholders and organisations across industry to get any views on Security governance for the DCC. Please contact smart@elexon.co.uk for more information.

For more information visit our website: www.elexon.co.uk

Contact us: 4th Floor, 350 Euston Road London NW1 3AW

T: 020 7380 4100

F: 020 7380 0407

E: communications@elexon.co.uk

ELEXON delivers a range of balancing and settlement services that are critical to the successful operation of Great Britain's electricity trading arrangements. As part of our role in ensuring that residential and business electricity settlement takes place, we have expertise in procuring and managing large industry leading contracts for systems and processes, we provide assurance services that the system works and that our customers are complying. We also managed the implementation and development of one of Great Britain's largest energy industry codes, as well as dealing with the ongoing day to day governance.