



Introduction to the SEC Seminar

September 19th 2018

Welcome!



Booklet Contents

- Agenda
- Slides from each presentation
- A glossary of common SEC terms and acronyms
- A feedback form



Purpose



AIMED AT NEW SEC PARTIES AND NEW STARTERS WITH LIMITED KNOWLEDGE OF THE SMART ENERGY CODE (SEC).



THE DAY WILL PROVIDE AN ENTRY-LEVEL GUIDE TO SMART METERING IN GREAT BRITAIN.



ASK QUESTIONS!

Points of Contact



SECAS Helpdesk Tel: 020 7090 7755



SECAS Helpdesk Email –
SECAS@Gemserv.com



Party Support Contacts:

Courtney O'Connor +44 (0)20 7191 1540 - Courtney.oconnor@gemserv.com

Stephen Blann +44 (0)20 7770 6940 - Stephen.Blann@gemserv.com

Marco Brunone +44 (0)20 7090 1093 -Marco.Brunone@gemserv.com

James Hosen +44 (0)20 3970 2819 - James.Hosen@gemserv.com

BEIS Smart Metering Implementation Programme

Introduction to SEC Seminar

19 September 2018



Department for
Business, Energy
& Industrial Strategy

Programme Overview

- 53 million electricity and gas smart meters – 30 million premises (households and businesses) across GB
- Over 11m smart and advanced meters operating across homes and businesses
- Supplier led rollout to be completed by end 2020
- Total Net Present Value for the rollout of smart meters in GB is estimated to be over £5.7 billion

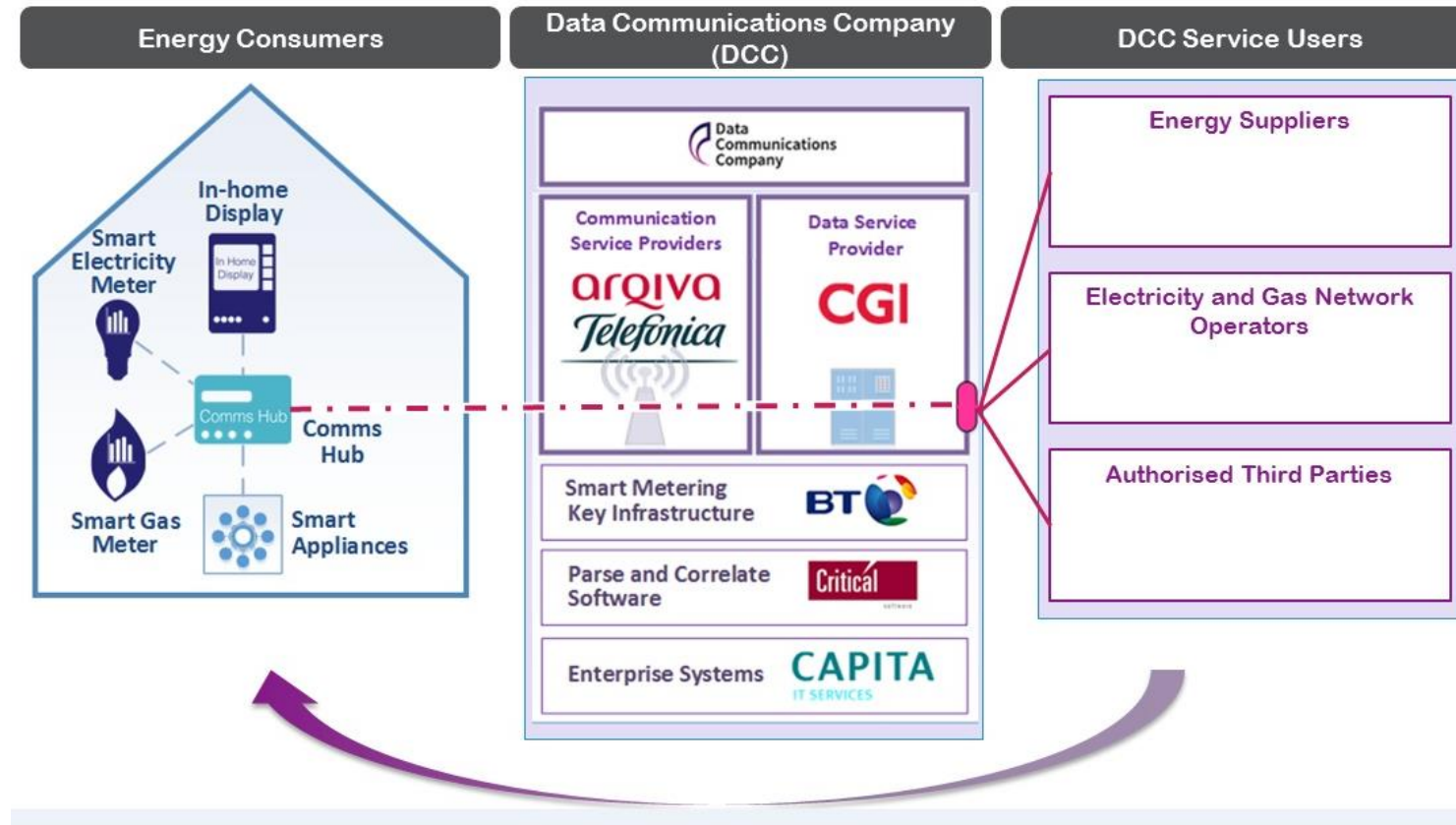


Benefits

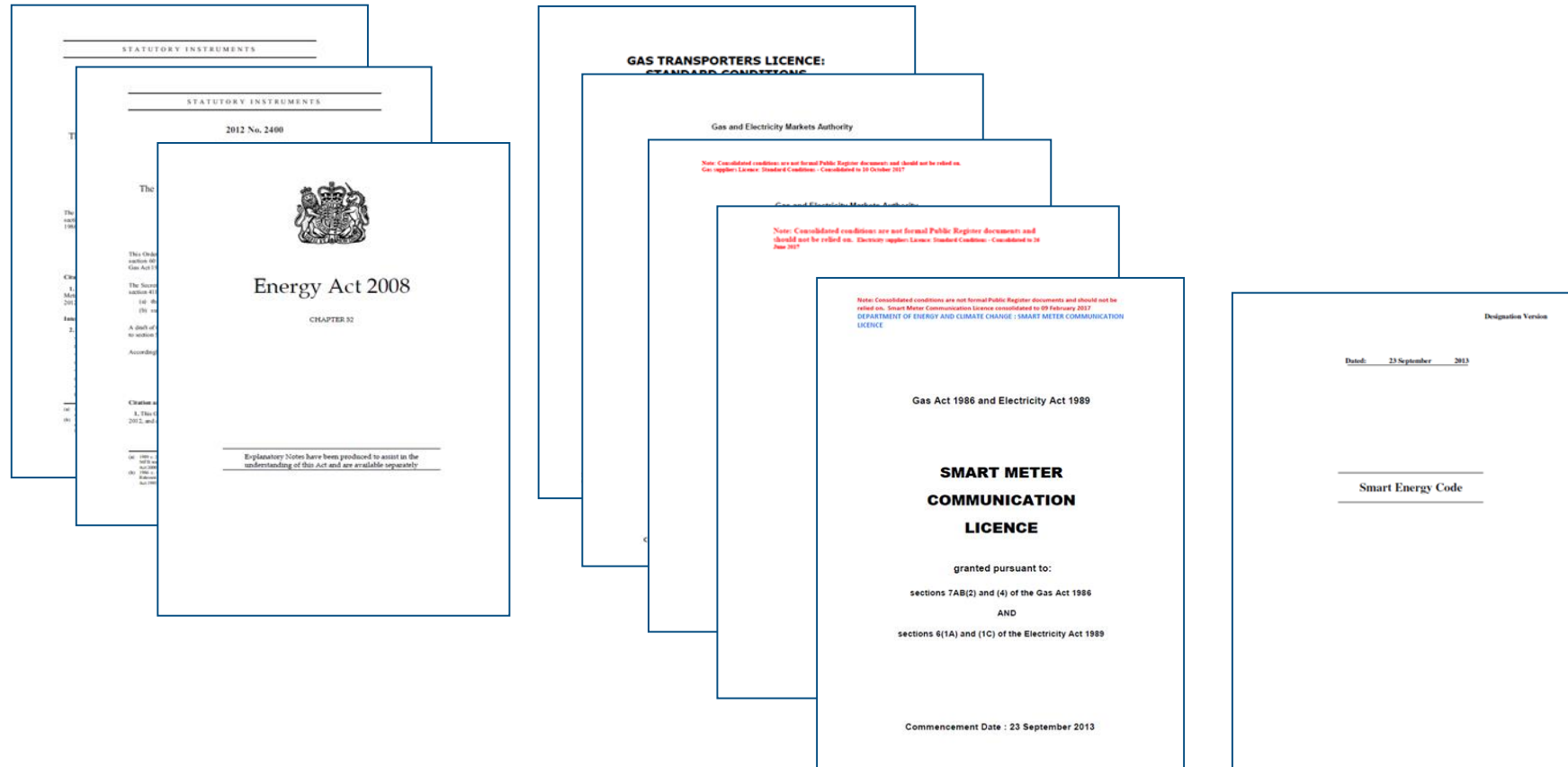
- Give consumers near real time information on energy use – expressed in pounds and pence
- Allow customer to better manage their energy use, save money and reduce emissions
- Bring an end to estimated billing – customers will only be billed for the energy they actually use, helping them budget better.
- Easier switching – smoother and faster to switch suppliers to get the best deals
- Enabling smarter energy systems



Commercial and Technical



Regulatory Framework



Conclusion

- This is a hugely ambitious programme, effecting the whole of GB, which is the catalyst for:
 - Creating an unprecedented new platform for innovation in energy data
 - Supporting the development of a wide range of new technologies
 - Empowering consumers to take energy saving measures
- Needs collaboration across a range of organisations to deliver wide range of benefits

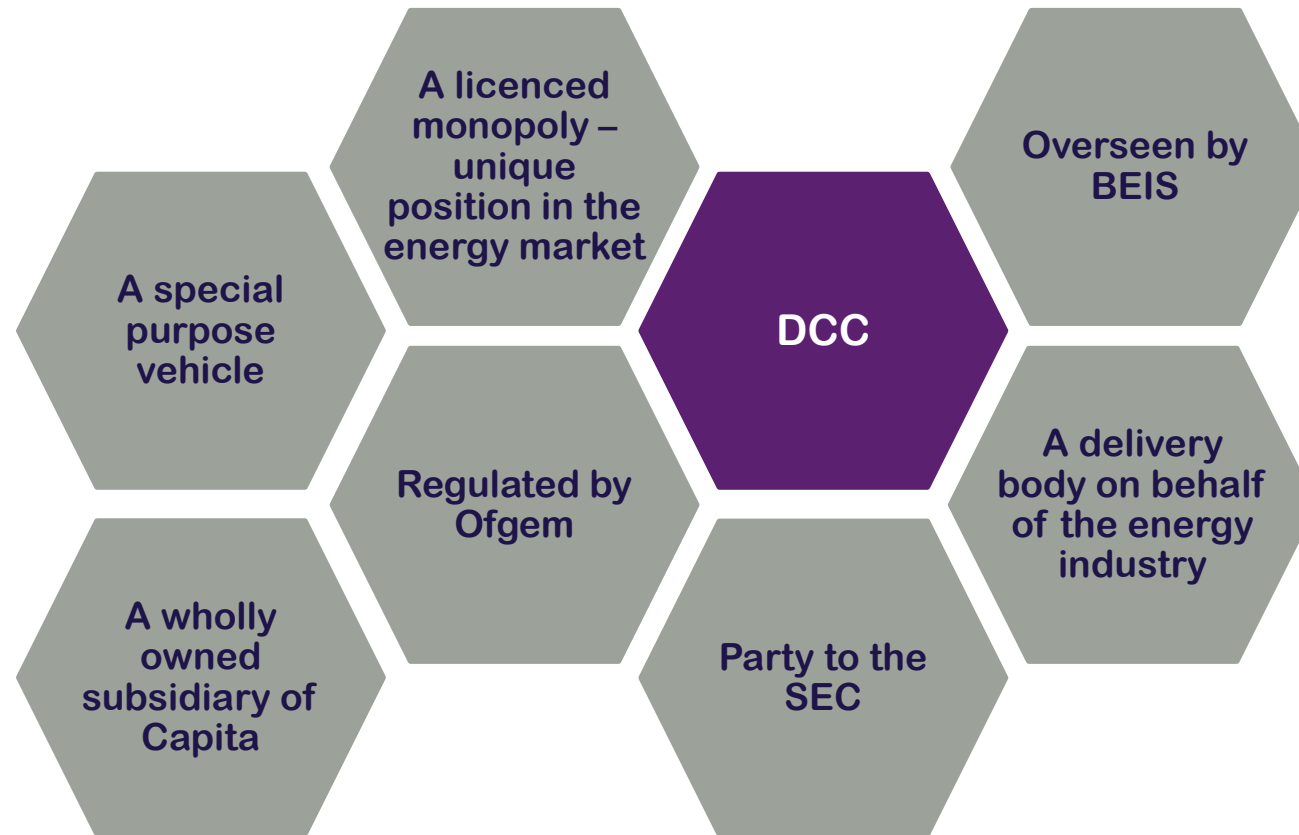


Introduction to DCC

David Nelson
Regulatory Stakeholder Management
Team



What is DCC?



The role of the Licensee (1)

- The Smart Meter Communication Licence(s) was awarded on 23 September 2013 – for current version see the Ofgem Electronic Public Register
- Smart DCC Ltd holds a licence to deliver DCC services for 12 years (with an option for Ofgem to extend for up to a further six years); then to be recompeted
- The Licence requires DCC to be a party to, and to comply with the Smart Energy Code (SEC) – it forms our contract with our customers

The primary role of the Licensee is:

- To implement and operate the smart meter communication service in line with the SEC
- To deliver this in ways that facilitate a) competition b) innovation contributing to a secure and sustainable energy supply c) reducing DCC charges (through provision of other services)

The role of the Licensee (2)

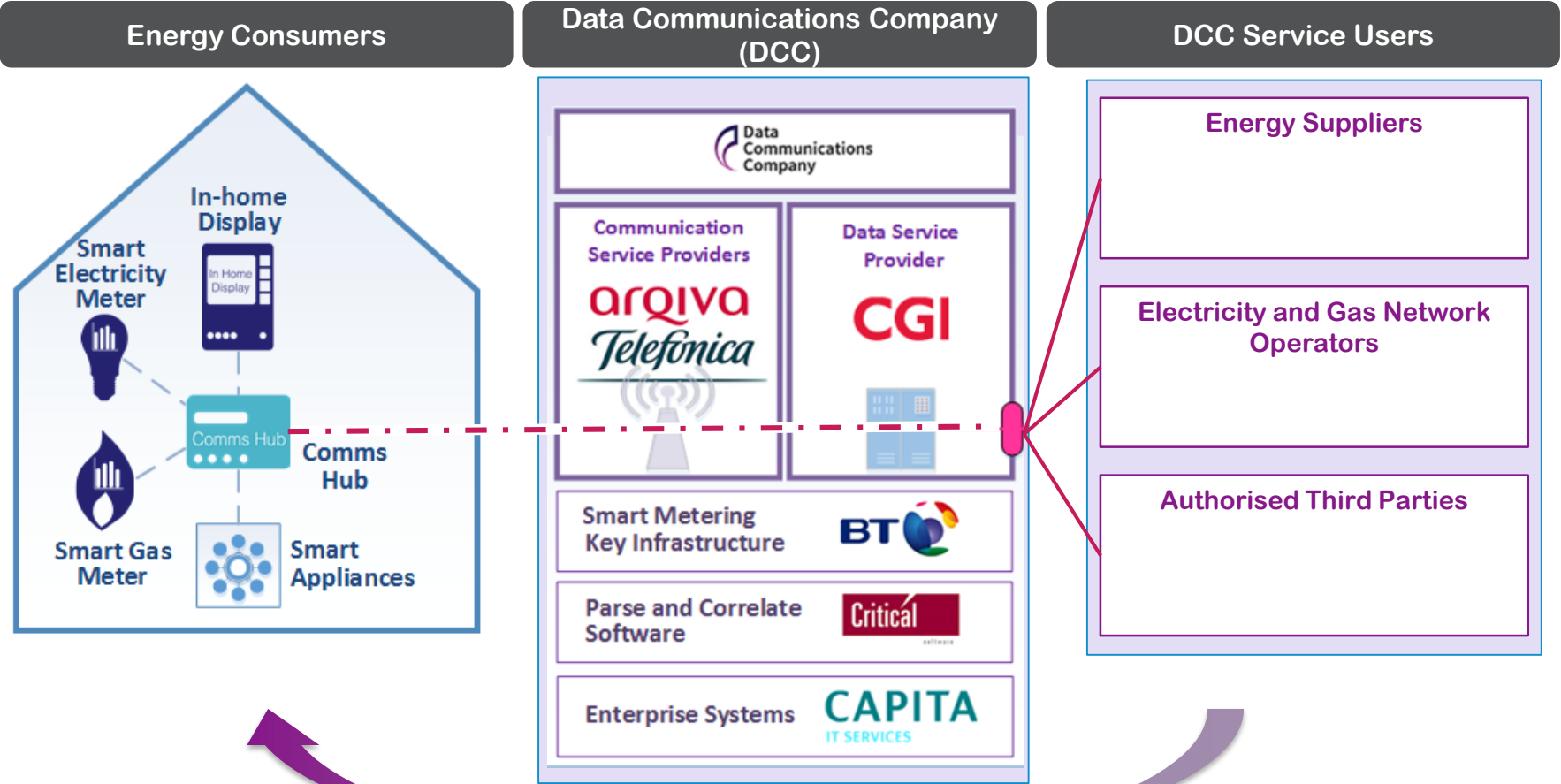
- Building new national smart metering infrastructure is not straightforward; but the system is up and running, and volumes of SMETS2 meter installations are ramping up quickly – over 30,000 installed as at end of August
- DCC has also been directed to provide the solution for bringing the first generation of smart meters – SMETS1 – into the national framework. This involves migrating millions of meters currently served by different, non-interoperable communications companies (SMSOs)
- Separately to our work under the SEC, DCC has been required by Ofgem to contribute to the design of the central switching service, and to procure the relevant service capability to deliver this.

DCC solution

- A national, centralised smart metering data and communication infrastructure
- Standard-based interoperability that allows DCC and industry to develop services against a common rulebook
- End-to-end security model to ensure that trust is maintained between consumer and interacting party
- Commercial framework that facilitates development of new services and re-use of infrastructure by other industries

DCC is an intelligent pipe – it does not see messaging between energy company and consumer / smart meter

DCC – OVERVIEW SCHEMATIC



What are the CSPs responsible for?

- Providing the Smart Metering Wide Area Network (SMWAN) to communicate between the Data Service Provider (DSP) and smart metering Communication Hubs
- Designing and procuring the Communication Hubs and supplying them to the energy suppliers for installation



For central and the south:

Telefonica

- Adapting their existing telecoms infrastructure

For the north:

arqiva

- Single long-range radio technology
- Building the network from scratch

What is the DSP responsible for?

- Developing, hosting and maintaining systems and software to support:
 - High volume, scalable service request processing
 - Handling of change of supplier and registration data updates
 - Self service portal – gives Service Users access to information and service management functions
 - An integrated service management solution across DCC, DSP and CSPs
- Underpinned by security at all times
- CGI also responsible for integration of CSP, DCC Licensee, Registration Service Providers and the business systems of DCC Service Users

The DSP is ...



Summary of Answers to Participant Questions



The DCC is preparing for enrolment of SMETS1 meters and this will be in several tranches by make and supplier, but the situation is still fluid. A particular issue is bringing dormant meters (those that lost functionality after a supplier switch) into the system. BEIS also confirmed that they will be publishing a response shortly (but no confirmed date) on whether the end date for SMETS1 will change [this is currently 5 October 2018].

The communication service used in the North Region is different from Central and South and is based on building a new radio network meaning this has been technically more challenging but now delivers good coverage. There are no plans to change the system once mobile coverage in North region improves.



An Introduction to the SEC

Marco Brunone, Party Support Senior
Analyst, SECAS

Smart Energy Code Administrator And Secretariat (SECAS)



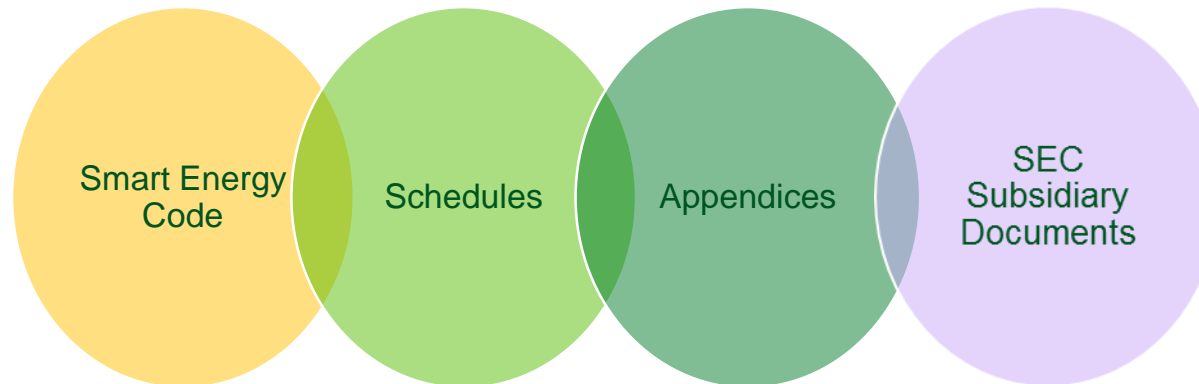
- Role defined in SEC Section C - Governance
- SECAS supports the Panel in delivering its obligations under the SEC, including:
 - Facilitating Parties to accede to the SEC
 - Become DCC Users
 - Raise modifications
 - Provide or procure information that the Panel may require
- SECAS Helpdesk is available 9am-5pm week days.
 - Email: secas@gemserv.com
 - Phone: 020 7090 7755



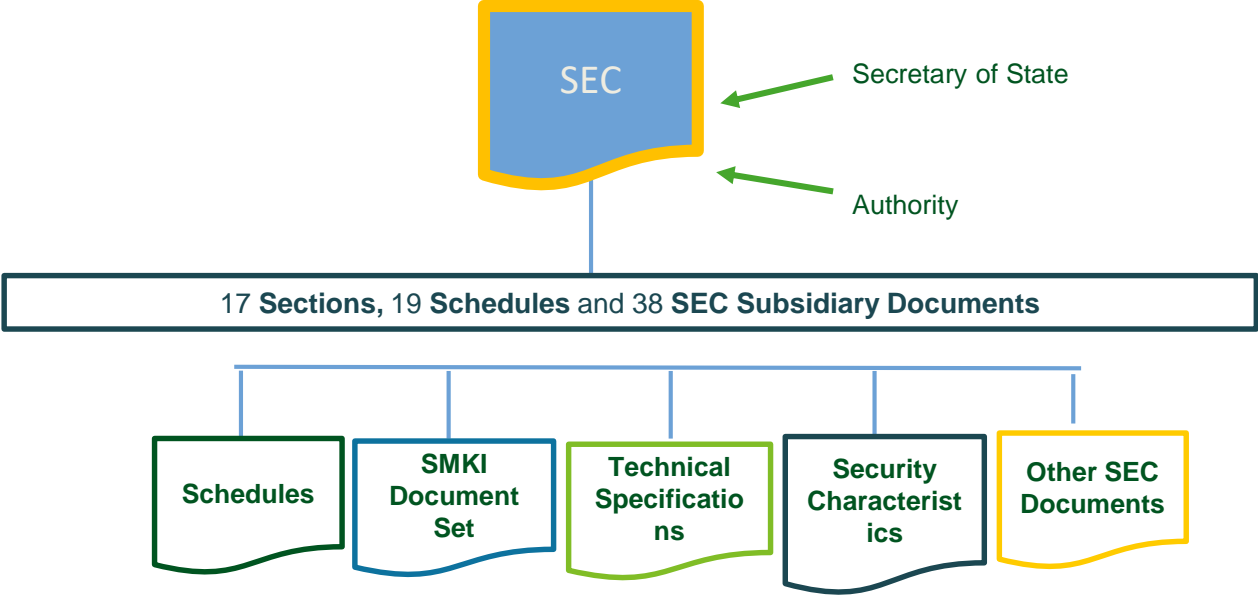
The Smart Energy Code (SEC)



- First designated 23rd September 2013, following the DCC Licence being granted. The current version is SEC 5.19.
- A multi-Party agreement:
 - DCC licence obligation for the SEC
 - Defines the rights and obligations between the DCC and the Users of the DCC Services
 - Specifies other provisions that govern the end-to-end management of Smart Metering in GB



SEC Document Architecture



What is the Make Up of the SEC?



Consolidated SEC	SEC Sections	SEC Subsidiary Document	SEC Section Guidance
Search: <input type="text"/>			
Document	Effective	Download	
SEC 5.21 - 22nd August 2018	22/08/2018	Download	
SEC 5.20 - 18th July 2018	18/07/2018	Download	
SEC 5.19 - 25th June 2018	25/06/2018	Download	
SEC 5.18 - 8th June 2018	08/06/2018	Download	
SEC 5.17 - 5th June 2018	05/06/2018	Download	
SEC 5.16 - 31st May 2018	31/05/2018	Download	
SEC 5.15 - 25th May 2018	25/05/2018	Download	
SEC 5.14 - 22nd February 2018	22/02/2018	Download	
SEC 5.13 - 1st February 2018	01/02/2018	Download	
SEC 5.12 - 22nd November 2017	22/11/2017	Download	By continuing
SEC 5.11 - 6th November 2017	06/11/2017	Download	

<https://smartenergycodecompany.co.uk/the-smart-energy-code-2/>

Using DCC Services



Section H – DCC Services

- Sets out DCC Operations
- Types of services to DCC Users
- Steps SEC Parties need to take to become DCC Users

Appendix E – DCC User Interface Services Schedule

- DCC Users send commands (Service Requests) to the DCC

Section J and K- Charges and Charging Methodology

- Determines the charges that Users have to pay to use DCC Services The actual charges are determined by the DCC and made available through the [DCC Charging Statement](#)
- Fixed Charges are based on a number of smart metering systems
- Explicit charges are determined on a user-pays basis

Smart Metering Key Infrastructure (SMKI) and DCC Key Infrastructure (DCCKI)



Section L – SMKI and DCCKI

- The SEC relies on using Public Key cryptography and Certificates to underpin cryptography related services to the GB Smart Metering.
 - Ensures secure and effective messages to and from Smart Metering Equipment.
 - Details on how to get SMKI assurance and tests you need to undertake to use SMKI
 - Three Public Key Infrastructures are used:
- Smart Metering Key Infrastructure (SMKI)
Provides certificates used for the means of establishing trust and secured communications between remote parties and smart metering devices across the DCC network.
 - Infrastructure Key Infrastructure (IKI)
Provides Users and non-DCC Users with credentials used for authentication to the SMKI service interfaces used for requesting certificates.
 - DCC Key Infrastructure (DCCKI)
Provides SEC Parties and Registration Data Providers with certificates used to authenticate and secure access to DCC interfaces such as the DCC Gateway Connection, Self Service Interface, the Registration Data Interface and the DCC User Interface.

Section E – Registration Data

SEC has three categories of security obligations on the DCC and its Users:

1) System Security

- DCC obligations - Ensures the security of the DCC Total System in accordance with CESG Good Practise and BS110008:2008
- User Obligations – System security measures DCC Users take

2) Organisational Security

- Regulates access to the SEC Parties User Systems and the DCC Total System

3) Information Security

- Requires establishing Information Security Management Systems which shall also comply with recognised International Standards

There are also obligations relating to the assurance and enforcement of these obligations. Each User has SEC responsibilities for the identification and management of the risk of Compromise, and are required to comply with ISO27005 standard or equivalent.

Registration Data



Section E – Registration Data

- The SEC requires Electricity and Gas Network Parties to provide the DCC with Registration Data in respect to each Meter Point Administration Number (MPAN) or Meter Point Reference Number (MPRN) recorded in their registration system.
- The DCC may use this for two purposes:
 - 1) Assessing a User's eligibility to receive certain Services; and
 - 2) Calculating Charges.
- The Registration Data must be digitally signed with an Organisation Certificate and is then provided via a DCC Gateway Connection

Non – Domestic Mandate



- BEIS published a consultation, Suppliers to Non-Domestic premises would be required to become DCC Users by **31st August 2018**. The full conclusion can be read [here](#).

Exemptions:

- High volume premises: If you are only intending to supply such premises through Advanced meters then the requirement to be a DCC user is less imperative.
- If supplying Small Medium Enterprises (SMEs) and microbusinesses you will need to become a DCC user and will not be allowed to leave Controlled Market Entry (CME) until you have done so.
- Those exempted energy suppliers must become DCC Users if they intend to either install a SMETS2 meter or to operate a SMETS2 meter that churns to them.


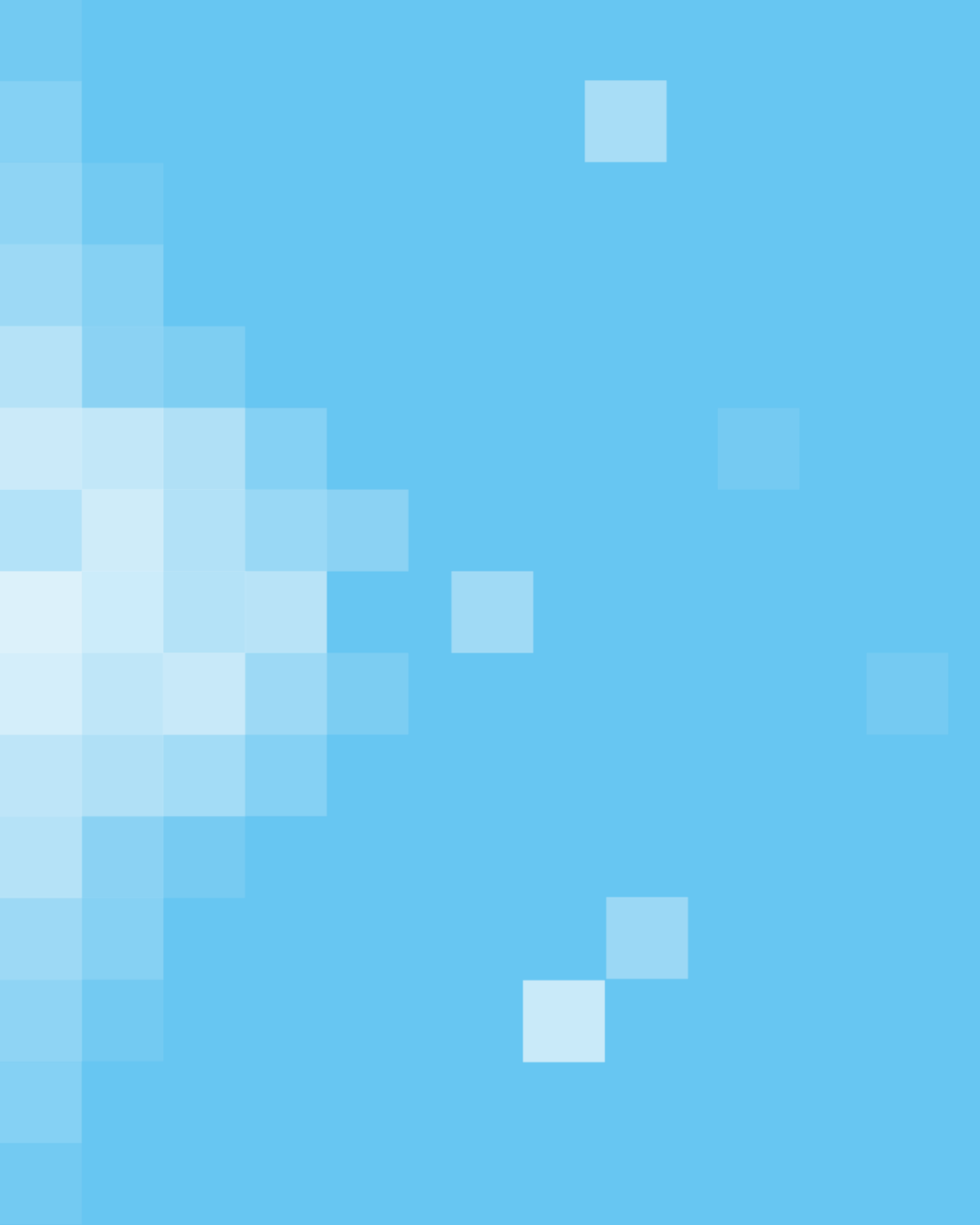
More information:

- Part B of consultation
- licensing@ofgem.gov.uk



Questions?

Marco Brunone, Party Support Senior Analyst, SECAS



SEC Governance: The SEC Panel and Sub-committees

Stephen Blann, Party Support Senior
Analyst, SECAS

Introduction



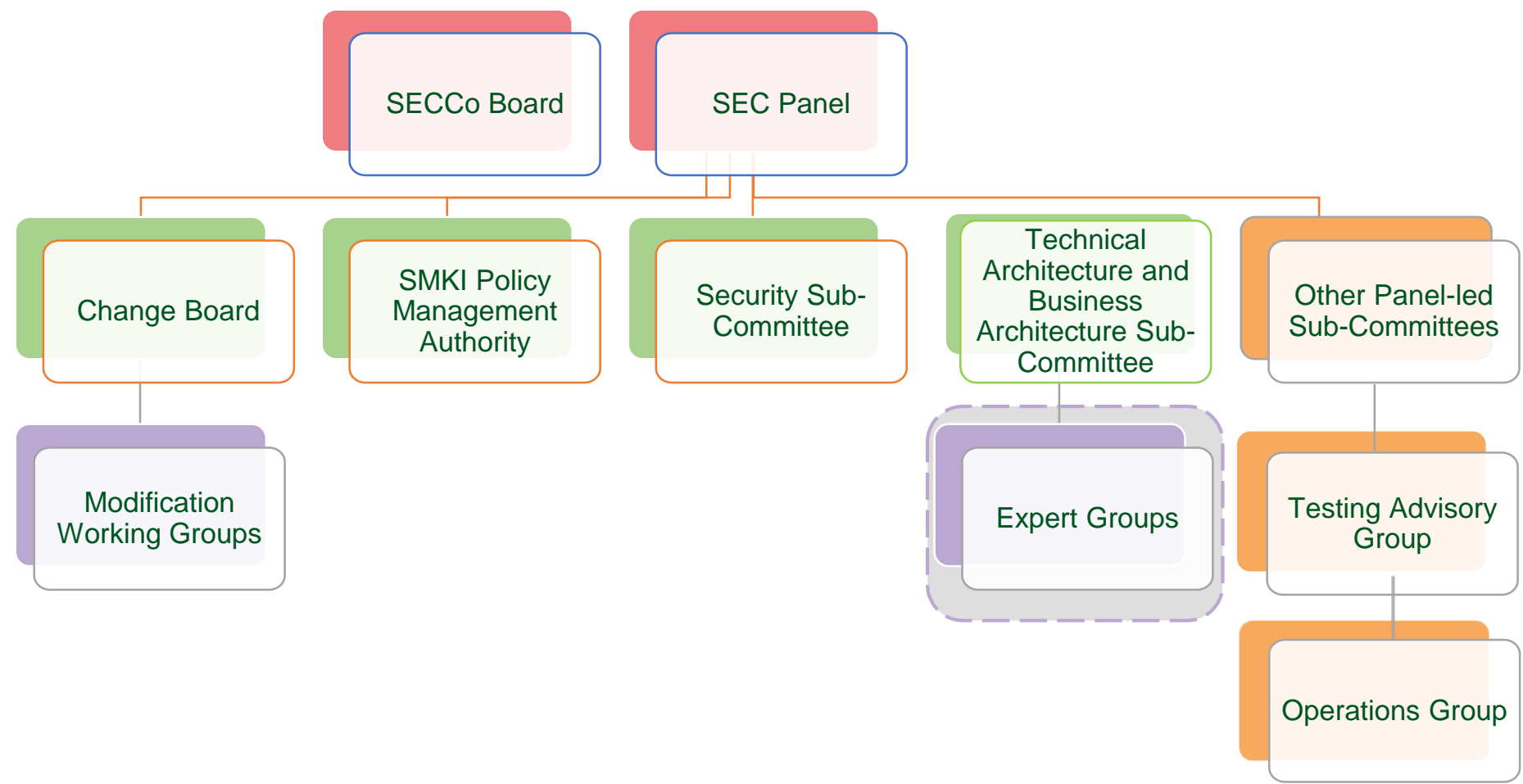
- The Smart Energy Code
- SEC Governance
- SEC Panel and SECCo Board
- Introducing the Sub Committees

SEC Objectives

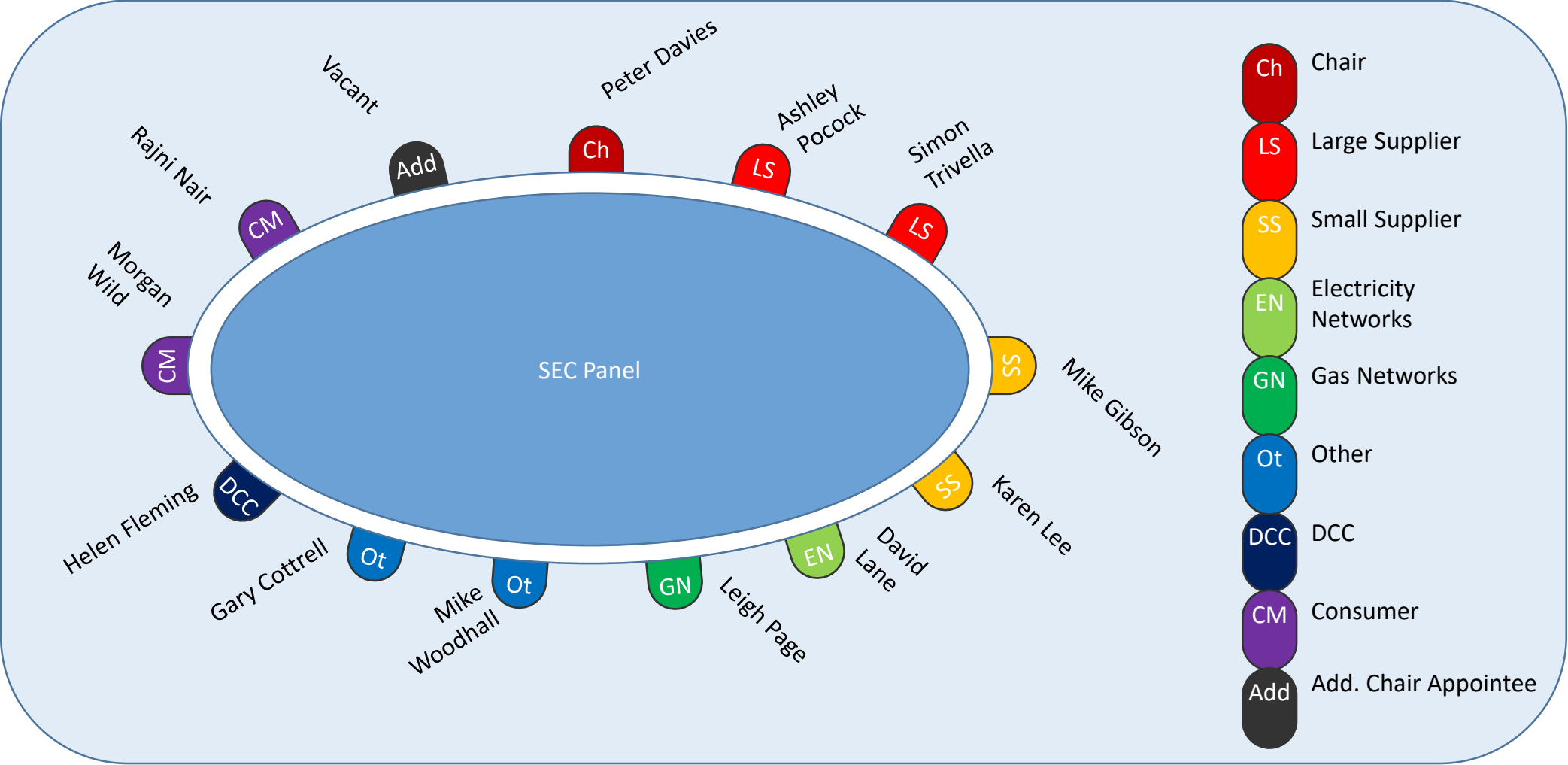


- Facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.
- Facilitate Energy Consumers' management of their use of electricity and gas by providing appropriate information through Smart Metering Systems.
- Facilitate effective competition in the Supply of Energy.
- Facilitate such innovation in the design and operation of Energy Networks as will best contribute to the delivery of a secure and sustainable Supply of Energy.
- Ensure the protection of Data and the security of Data and Systems.

SEC Governance Structure



SEC Panel



SEC Panel and SECCo Board



Panel

- Establishes budgets, Sub-Committee constitution and expert infrastructure, oversight of the Modifications Process
- Developed capability to take-on responsibilities emerging from future SEC content and handover from Transition Governance

Board

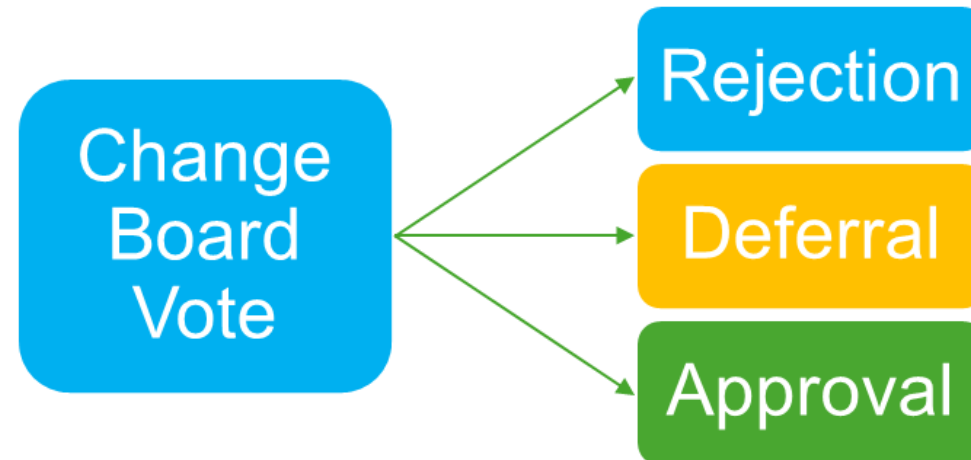
- Board of Directors of SECCo
- Looks at the corporate governance of the Code e.g. contract-holder with SECAS, Independent Chairs, PKI Expert, Lawyers, User Competent Independent Organisation and SECCo Auditor



Change Board



Sub-Committee	Function	Membership
Change Board	Reviews Modification Reports and votes on whether to approve or reject Modification Proposals	One member from each Large Supplier voting group Three members from each other category - Small Suppliers, Networks and Other SEC Parties One Consumer Representative DCC and Ofgem (not voting members) Chaired by SECAS (not a voting member)



Change Board members



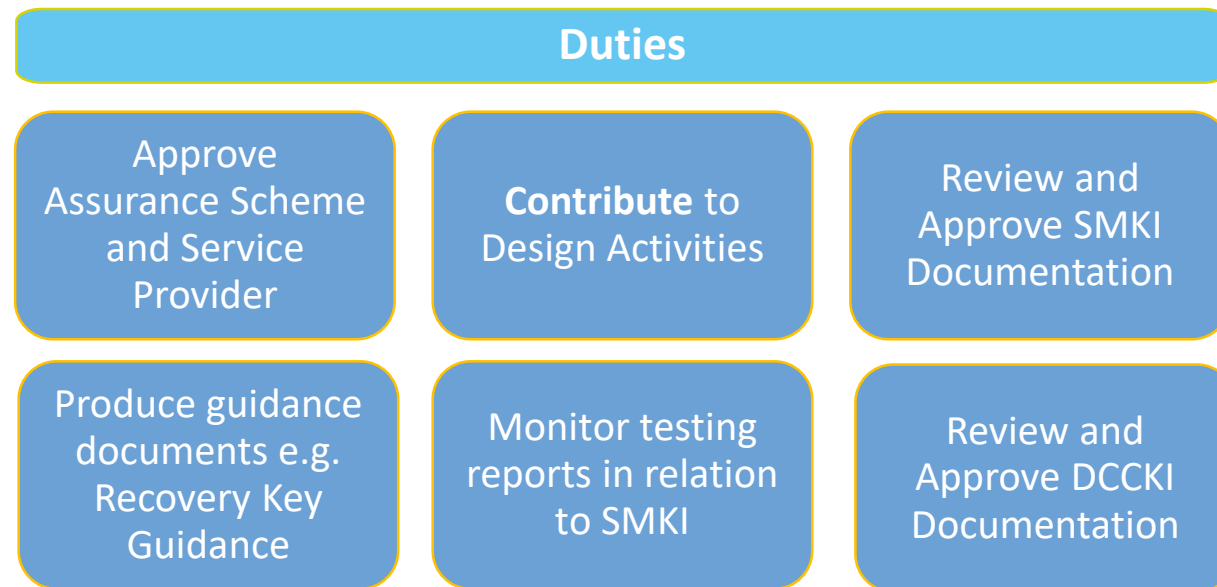
Constituency	Member
Large Suppliers	Jonathan Hawkins
	Amie Charalambous
	Stacey Brentnall
	Graham Wood
	Rachael Mottram
	Sam Cannons
	Paul Saker
	Carl Whitehouse
	David Rodger
	<i>Vacant</i>
	<i>Vacant</i>
	<i>Vacant</i>

Constituency	Member
Small Suppliers	Carolyn Burns
	<i>Vacant</i>
	<i>Vacant</i>
Networks	Jeremy Meara (electricity)
	Paul Fitzgerald (electricity)
	Shanna Key (gas)
Other SEC Parties	Mike Woodhall
	Elias Hanna
	Gerdjan Busker
Consumers	Colin Griffiths

Smart Metering Key Infrastructure Policy Management Authority



Sub-Committee	Function	Membership
SMKI Policy Management Authority (PMA)	Governs the SMKI Document Set and to monitor and gain assurance of the DCC operation of SMKI services	3 Large and 1 Small Suppliers, 2 Network, 1 SSC & 1 TABASC Representative, PKI Specialist, DCC, Ofgem, SoS and independent Chair



Security Sub-Committee



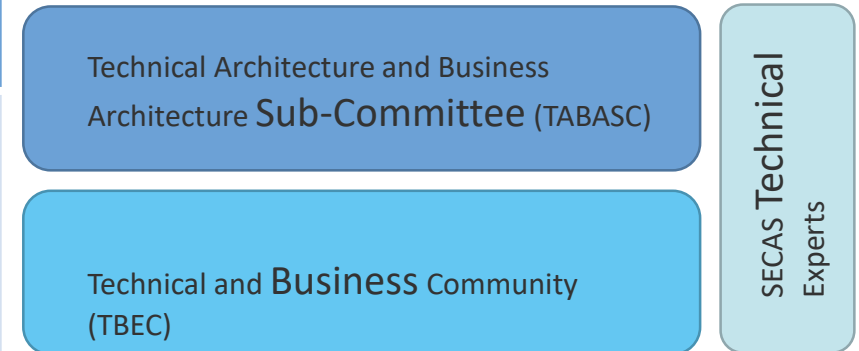
Sub-Committee	Function	Membership
Security Sub-Committee (SSC)	Develop & maintain security documents under the end-to-end security architecture	8 Suppliers (6 Large and 2 Small), 2 Networks, 1 Other User, DCC, SoS, 1 TABASC Representative and an independent Chair



Technical Architecture and Business Architecture Sub-Committee



Sub-Committee	Function	Membership
Technical Architecture and Business Architecture Sub-Committee (TABASC)	Provides support & advice on the Technical Specifications and end-to-end Technical Architecture	8 Suppliers (6 Large and 2 Small), 2 Networks (1 Gas and 1 Electricity), 2 Other Parties and an independent Chair. Also attended by the DCC, BEIS and Ofgem.



Current Priorities

- Following sufficient initial installed volumes identified, the second iteration of the Effectiveness Review Questionnaire is currently underway for SEC Parties and Users to complete. The aim is for the TABASC to obtain data and supporting information to inform its review of the Technical and Business architectures and the Home Area Network requirements.
- 6 of the TABASC Members seats are coming to the end of their 24 month term. These seats will be going up for nomination on 24th September 2018 for the new Members to take office on 30th November 2018.

TABASC Members



Category	Name
TABASC Chair	Julian Hughes
Large Supplier	Rochelle Harrison (coming to the end of 24 month term)
Large Supplier	Stacey Bentnall (coming to the end of 24 month term)
Large Supplier	Ashley Pocock (coming to the end of 24 month term)
Large Supplier	Grahame Weir
Large Supplier	Emslie Law
Large Supplier	Stephen Lovell

Category	Name
Small Supplier	Andy Knowles (coming to the end of 24 month term)
Small Supplier	James Kirk
Electricity Network	Alan Creighton
Gas Network	Leigh Page (coming to the end of 24 month term)
Other SEC Parties	Tim Boyle (coming to the end of 24 month term)
Other SEC Parties	Elias Hanna
Ofgem Representative	Michael Walls
BEIS Representative	John Eager
DCC Representative	Sylvia Ovie

Testing Advisory Group



Sub-Committee	Function	Membership
Testing Advisory Group (TAG)	Supports the Panel with their obligations throughout the testing stages. Reviews testing documentation, provides views on testing reports.	1 appointed by each Large Supplier Up to 3 each from the Small Suppliers, Electricity and Gas Networks, Other SEC Parties, 1 Consumer member and Other Interested Parties at the discretion of the Panel or Chair.

Current Priorities

- The TAG are continuing to review of the testing progress associated with Release 2.0 (R2.0), focusing on System Integration Testing (SIT) completion to inform a recommendation to the SEC Panel.
- The DCC and TAG are also discussing other aspects of R2.0 to ensure that the process leading to confirmation that Live Services Criteria will be as smooth as possible. These included an update on the use of Feature Switching, the process heading to Secretary of State approval to go live, User regression testing and how the DCC plans to address comments on the SIT Completion report.
- TAG are continuing to review of the testing progress associated with SMETS1, including device selection for SMETS1 SIT.

TAG Members



Category	Name
TAG Chair	David Barber
SECAS Representative	Phillip Twiddy
Large Supplier	Martin Bell
Large Supplier	Andrew Cameron
Large Supplier	Martin Hanley
Large Supplier	Anthony Thomas
Large Supplier	Will Leacock
Large Supplier	Adrian Wood

Category	Name
Small Supplier	Vacant
Small Supplier	Vacant
Small Supplier	Vacant
Other SEC Parties	Elias Hanna
Other SEC Parties	Lynsey Cosgrave
Other SEC Parties	Ferenc Vanhoutte
Gas Network	Tom Pollock
Electricity Network	Vacant
Gas/Electricity Network	Vacant

Operations Group



Sub-Committee	Function	Membership
Operations Group	The purpose of the Operations Group is to deal with operational matters that relate to services provided under the Smart Energy Code, including DCC Services; and, to enable close co-operation between the DCC and DCC users.	1 appointed by Large Suppliers, 3 persons from each of Small Suppliers, Electricity and Gas Networks, Other SEC Parties, 2 appointed by the DCC, TABASC representative, Ofgem and BEIS representatives

Current Priorities

- Establishing an Operational E2E view of DCC services and establishing priorities.
- Reviewing DCC reports delegated by the SEC Panel.
- Reviewing Major Incidents (not Security) understanding operational impacts, lessons learned.
- Understanding DCC plans and steps to be taken to scale up for services to support the ramp up of installation volumes.

OPSG Members



Large Suppliers

- Rochelle Harrison
- Stacey Brentnall
- David Penny
- Graham Ovenden
- Jon Hawkins
- George Macgregor
- Mark Field
- Endika Ennes

Network Operators

- Liam Cowe
- Martin White
- Tom Pollock

Small Suppliers

- Kate Barnes
- Simon Downes
- Vacancy

Other SEC Parties

- Jon Walsh
- Elias Hanna
- Geoff Huckerby

Authority / DCC / BEIS TABASC / SECAS

- Julian Hughes (TABASC)
- Ian Mckenzie (BEIS)
- Michael Walls (Ofgem)
- Gordon Riddell (DCC)
- Mo Asif (DCC)
- Dave Warner (SECAS Chair)



Questions?

Stephen Blann, Party Support Senior Analyst, SECAS

Stephen.Blann@gemserv.co.uk

020 7770 9640



Introduction to the Modification Process

Cordelia Grey, Senior Change Analyst,
SECAS

Overview



Background

Roles

Modification Process

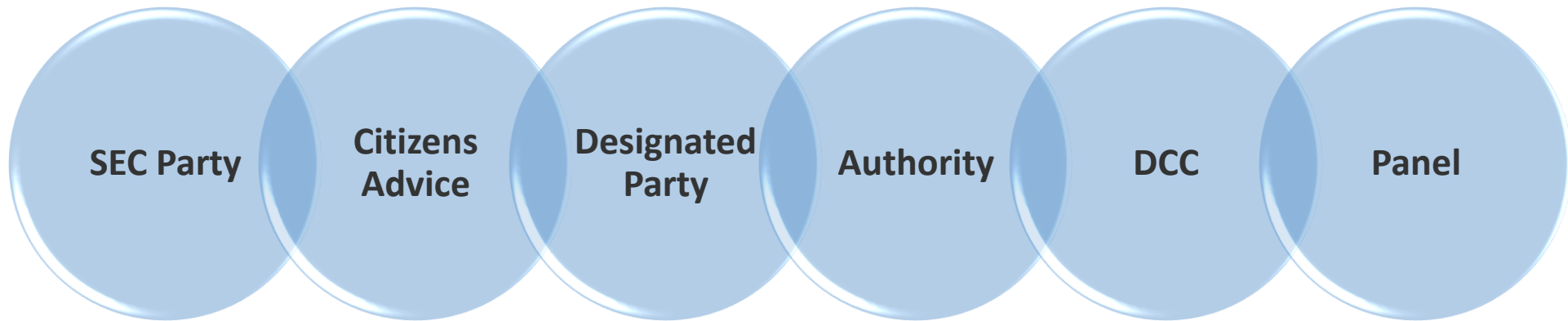
Current landscape

Contact details and further information

Smart Energy Code 'Section D'

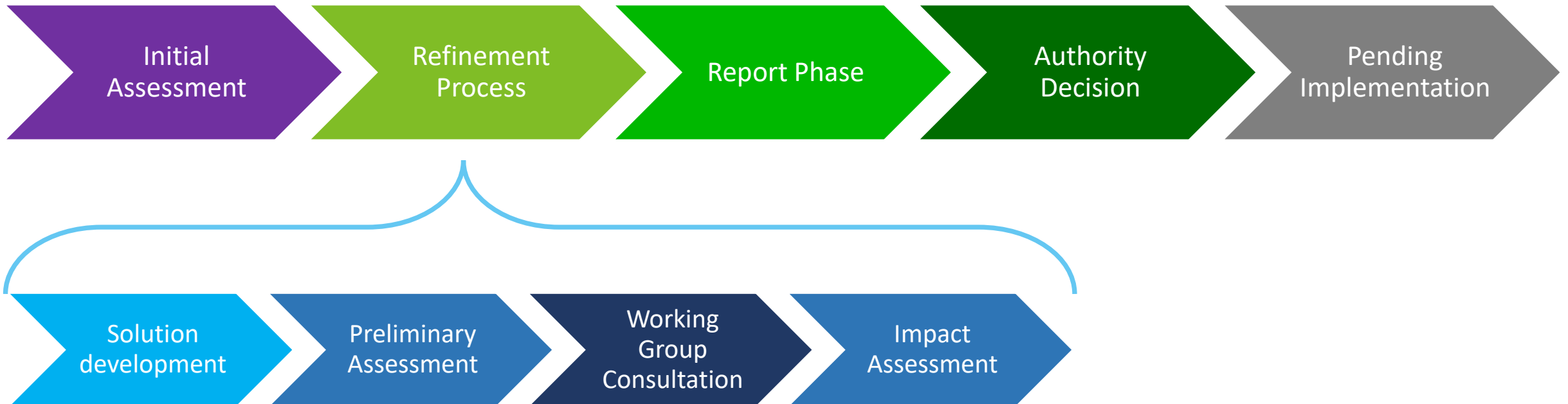


- 'Section D' outlines the Modification Process for the Smart Energy Code
- The following are eligible to propose a modification:



Modification Process

- Process to progress changes to the SEC (Section, Schedule or Appendix)



Change Team



Critical friend

Support the Proposer

Technical expertise

Lead Analyst/Chair

Draft all documents

Arrange and attend
Working Groups

End-to-End Planning

Communications

Website

Consultations and
notifications

Modifications Question
Hour

Panel

Change Board



Progression

Modification Path
Type

Timetable

Refinement/
Report

Advisory

Group Mods
together

Working Group
Terms of
Reference

Technical
Expertise

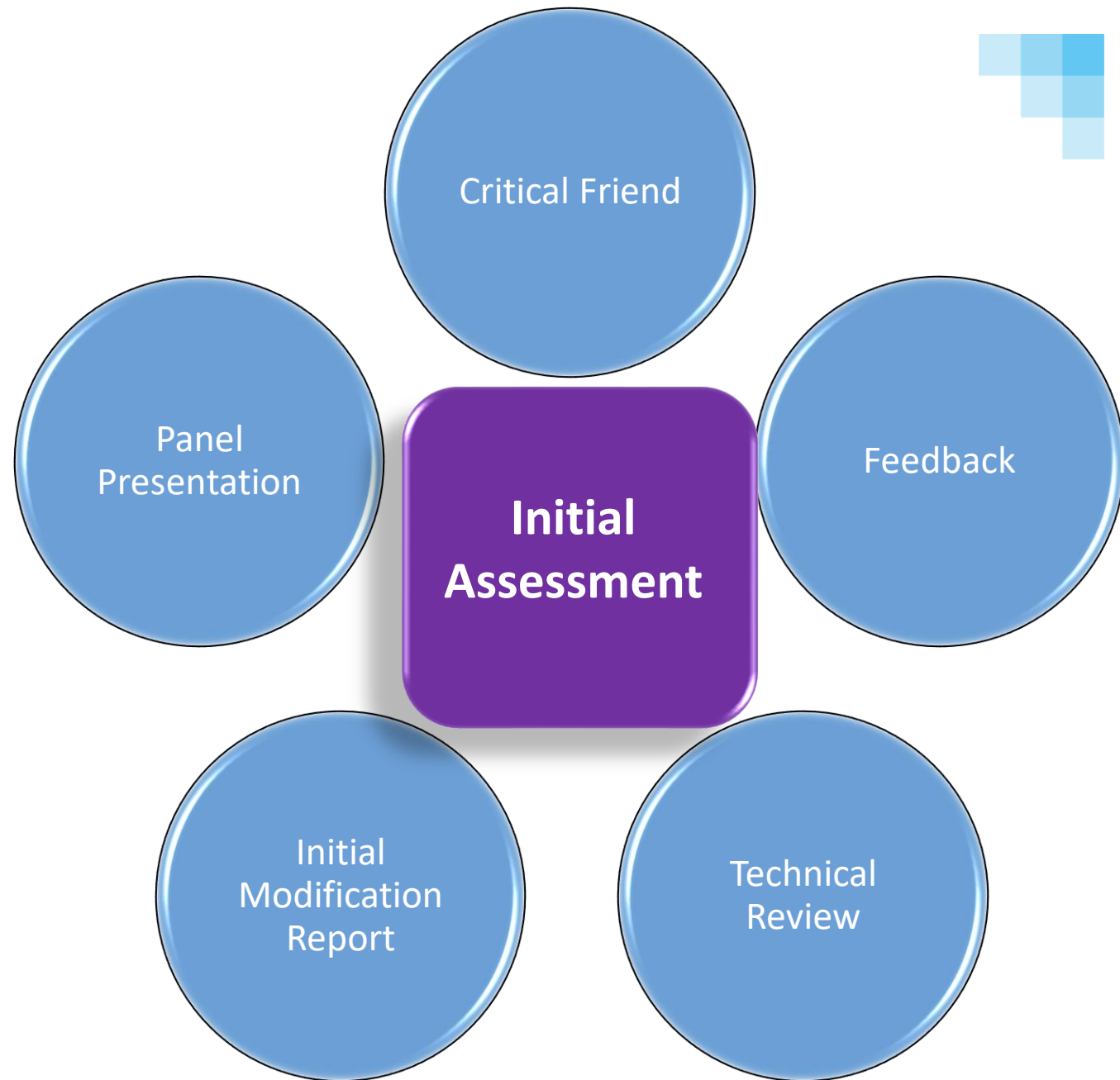
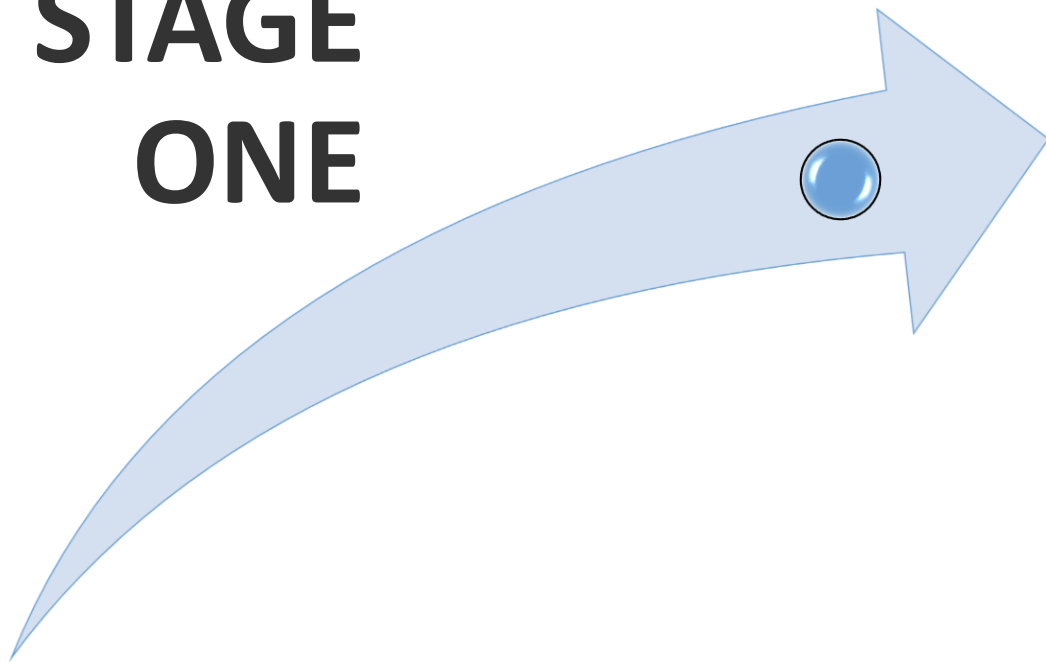
Final Decision-Makers

Benefits Case

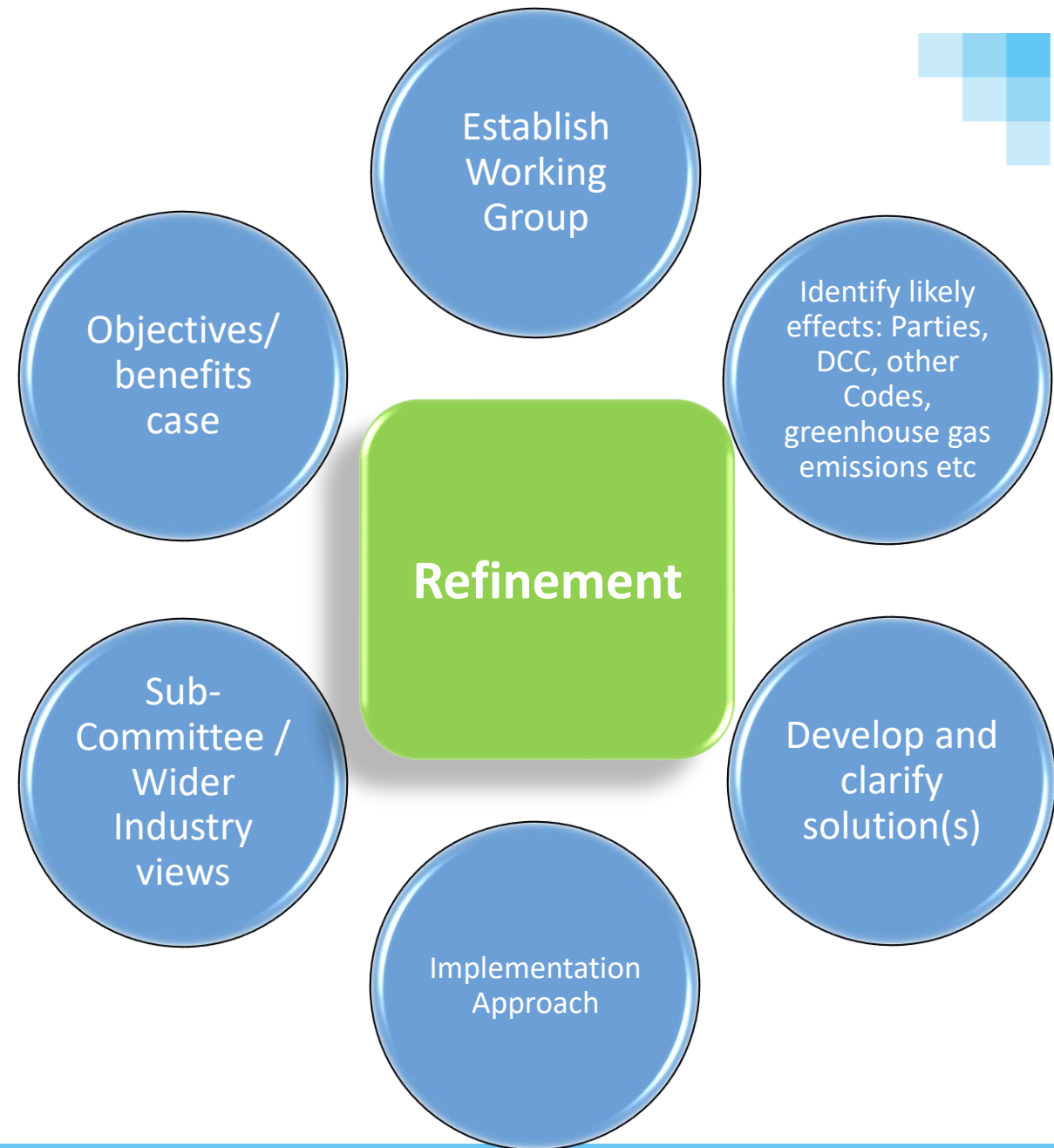
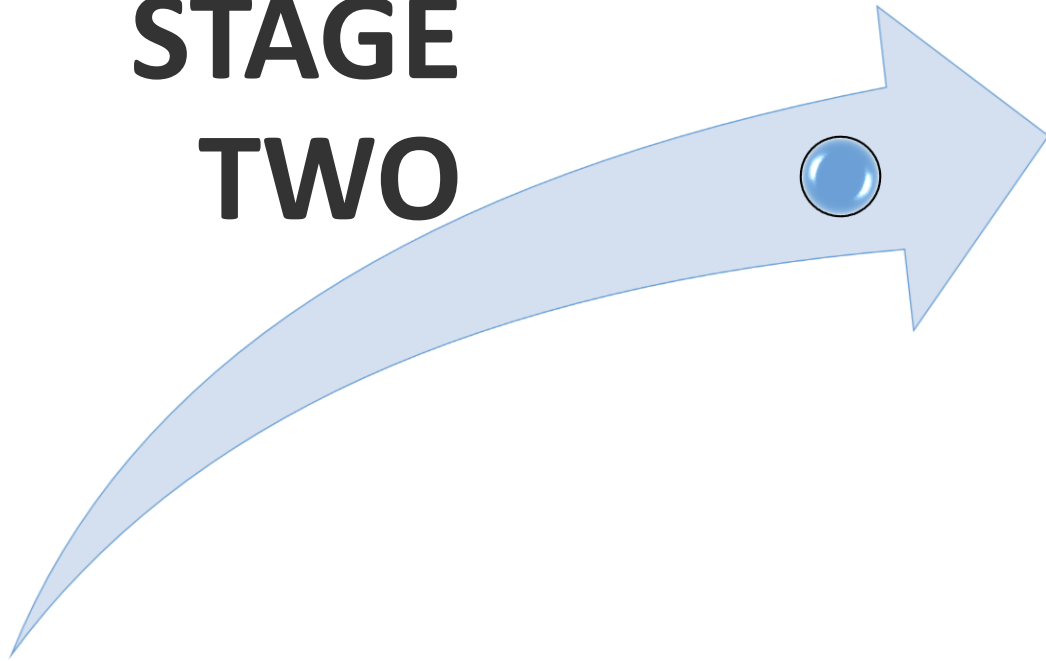
Objectives

Solution/ Alternative Solution

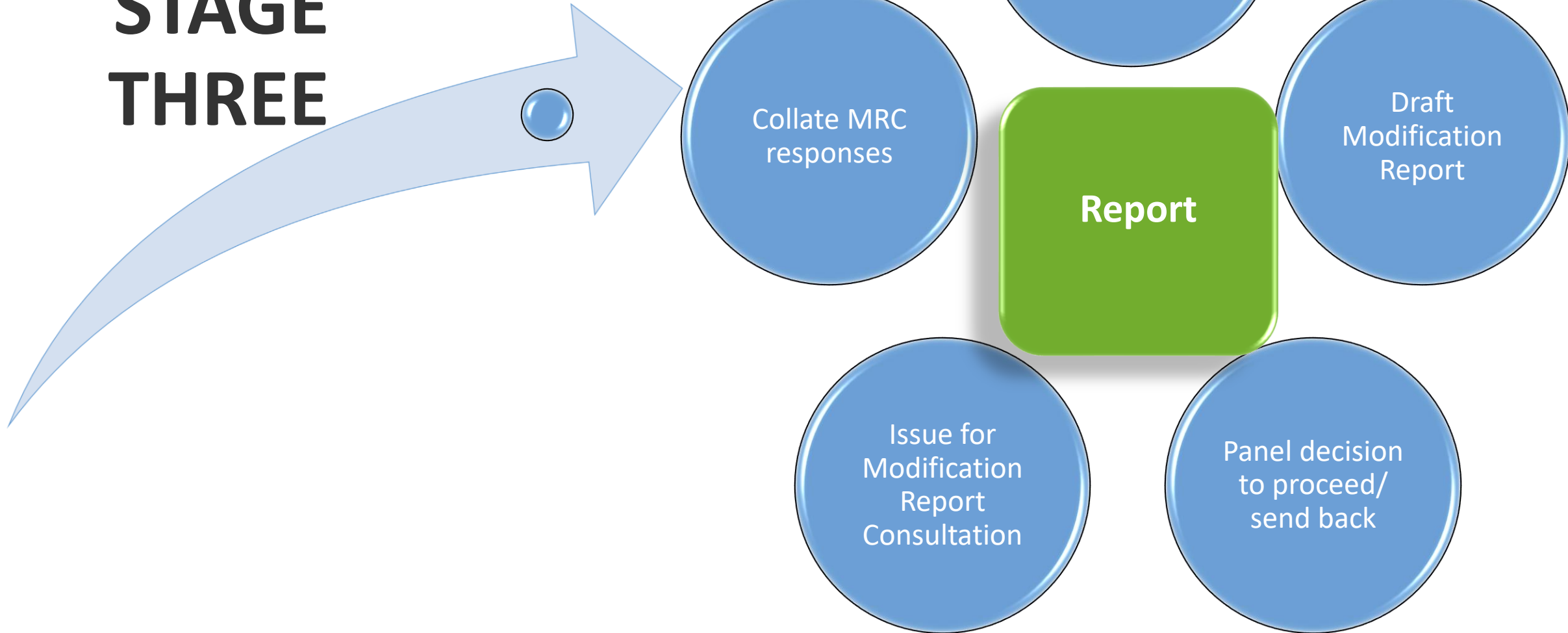
STAGE ONE



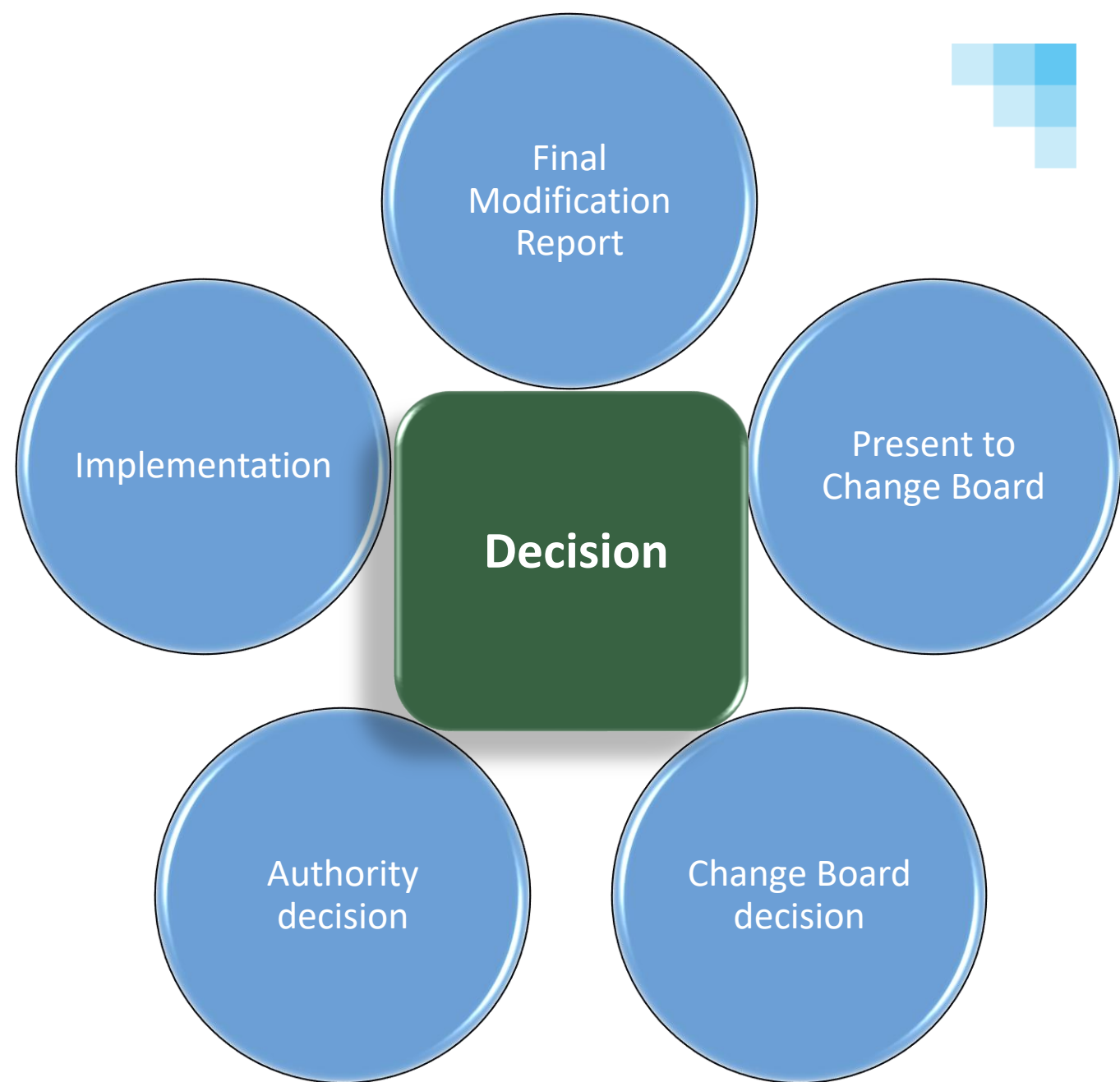
STAGE TWO



STAGE THREE



STAGE FOUR

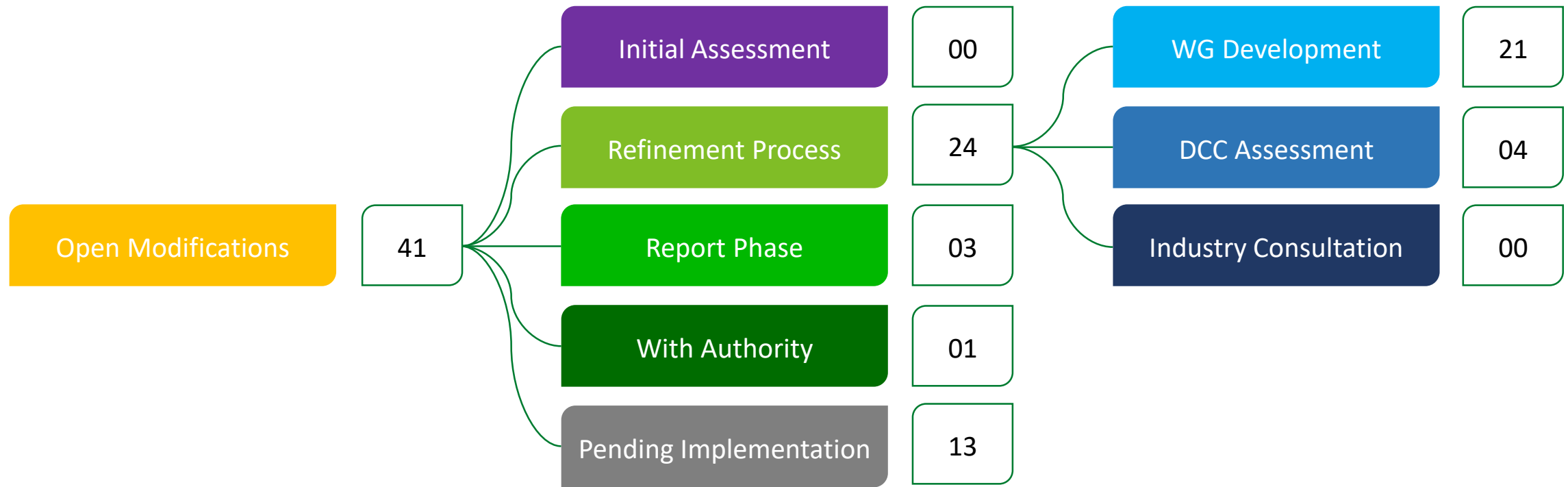


Open and New Modifications

- A list of all open modifications can be found on the SEC Modifications Register [here](#).

Modification Register																				
Modification					Overview										Decision					
Modification	Title	Proposer	Date raised	Path	Summary	Latest progress	Change Board determination	Date of review	Authority determination	Date of determination	Implementation date	Sep 18	Oct 18	Nov 18	Dec 18					
Open Modifications																				
SECMP0006	Specifying the number of digits for device display	SSE	01 Mar 16	Path 2	Include a specification for the number of digits for devices' display of meter registers in SMETS2 in relation to the provision of energy measurement information.	On 29th September 2017, the Authority (BERR) approved this modification subject to European Commission (EC) Notification. The modification will be notified in draft to the EC. The decision to approve will come in to effect once the standstill period has ended (30 days), provided that no comments have been received and/or there are no issues outstanding. On 9th March 2018, the SEC Panel recommended the implementation date be changed to 30th September 2018, to align with Release 2.0. The Authority approved this change of date on 29th September 2018.	Approve	23 Aug 17	Approve	23 Sep 17	30 Sep 18	Impl. Date								
SECMP0007	Firmware updates to mandated HAN devices	Npower	01 Mar 16	Path 2	This modification proposes including the capability to update firmware Over-The-Air (OTA) for mandated HAN devices (BD / PPMID) via the DCC's infrastructure.	A DCC PA has been requested. There was a Working Group meeting on Tuesday 24th July 2018. Requirements will be added for the DCC to assess against. There was a meeting between SECAS and DCC to discuss the PA technicalities on 7th September 2018. SECAS will confer with the Working Group to determine the next steps.														
SECMP0008	Provision of a DCC Alert (formerly Service Request Error Response) for Quarantined Service Requests	Scottish Power	01 Mar 16	Path 2	Provide a new DUIS Service Request error response to give DCC Service Users visibility of quarantined Service Requests following a breach of the DCC's Anomaly Detection Threshold and / or the individual DCC Service User's Anomaly Detection Threshold.	On 29th September 2017, the Authority approved SECMP0008. On 9th March 2018, the SEC Panel recommended the implementation date be changed to 30th September 2018, to align with Release 2.0. The Authority approved this change of date on 29th September 2018.	Approve	23 Aug 17	Approve	23 Sep 17	30 Sep 18	Impl. Date								
SECMP0009	Centralised Firmware Library	Npower	01 Mar 16	Path 2	Establishment of a repository of firmware images, with access provided to all Parties responsible for the management of SMETS1 and/or SMETS2 meters.	The Modification Report closed on 5th September 2018. The Change Board vote will take place on 19th September 2018.					Targeted for 01 Nov 18	FMR presented to Change Board	Authority decision							
SECMP0010	Introduction of triage arrangements for Communication Hubs	British Gas	02 Mar 16	Path 2	SEC Supplier parties should be permitted to carry out basic 'triage' checks on Communications Hubs following their removal from a consumer's property.	This Modification is progressing in tandem with SECMP0013, for which a Preliminary Assessment from the DCC was received on 10 July 18. Working Group meetings for SECMP0010 and SECMP0013 arranged for the 24th September. DMR due to be presented to the Panel in February 2019.														
SECMP0012	Channel selection to support Shared HAN solutions	Siemens Plc	05 May 16	Path 2	Seeks to enable channel selection at the mandated 2.4GHz frequency to facilitate the efficient provision, installation, operations and interoperability of Smart Metering Systems in premises where standard HAN solutions are unsuitable and Shared HAN solutions necessary.	The DCC has provided the Preliminary Impact Assessment for SECMP0012. A Working Group was scheduled for 16 July 2018, but will now be rescheduled when the Air HAN project reaches a position that can inform the Working Group of the value of progressing the Modification. DMR to be presented to the Panel in January 2019.														
SECMP0013	Smart meter device diagnostics and triage	E.ON	04 May 16	Path 2	The proposal seeks to amend the SEC and DCC's systems to provide Suppliers with a means of performing quality assurance and fault diagnostics on SMETS2 devices returned by meter operatives.	This Modification is progressing in tandem with SECMP0010. The Preliminary Assessment from the DCC was received on 10 July 18. Working Group meeting for SECMP0010 and SECMP0013 arranged for 24th September. DMR due to be presented to the Panel in February 2019.														
SECMP0015	Add Timestamp to Read Instantaneous Prepay Values response message	E.ON	31 May 16	Path 2	The Gas Instantaneous Prepay Values are retrieved from the Gas Proxy Function and as such, these may not be in-line with the Gas Meter. Without a timestamp to indicate the timeliness of these values, it prevents the supplier from knowing how up to date the information is.	The DMR presentation date is currently being sought to be extended to December 2018. This is due to the Panel's request to acquire the full Impact Assessment costs and have the Working Group give their opinion on these full costings before presenting the report to Panel.					Targeted for 07 Nov 18	DMR presented to Panel	FMR presented to Change Board	Authority decision						
SECMP0018	Standard Electricity Distributor Configuration Settings	Northern Powergrid	23 Jun 16	Path 2	Amendments to the Great Britain Companion Specification (GBCS) to specify the standard Electricity Distributor configuration settings to be applied to an electricity smart meter by the Manufacturer. Application of default configuration settings will reduce the need for Electricity Distributor to apply settings immediately after commissioning.	At August's Change Board meeting on 22nd August 2018, this modification was requested to be sent back to the SEC Panel for further refinement with the rationale being that the full costings are required to make an informed decision on whether or not it should be approved.					Targeted for 27 Jun 19	Sent Back presented to Panel								
SECMP0019	ALCS Description Labels	SSE	14 Jul 16	Path 3	This Proposal recommends that there should be some form of guidance / rules (Naming Conventions) / standardisation when defining any of the 5 Auxiliary Load Control Switches (ALCS) or HAN Connected Auxiliary Load Control Switch (HCALCS).	The modification was presented to the Change Board where they decided to approve it, the referral window closed on 8th August 2018 and the modification is now awaiting implementation on the 1st November 2018.	Approve	25 Jul 18	N/A	N/A	01 Nov 18		Impl. Date							
SECMP0020	Correct Units of Measure for Uncontrolled Gas Flow Rate	Npower	26 Oct 16	Path 3	Currently GBGS limits the values of the Uncontrolled Gas Flow rate to be in whole numbers of m3. This modification proposes to change that to allow m3 with accuracy to 3 decimal places to be specified.	The FMR has been approved by the Change Board with a 10 WD referral period due to close on 8th June 2018. No responses were received in this window so the modification is now due to be implemented on 27th June 2018.	Approve	23 May 18	N/A	N/A	27 Jun 19									
					The Proposer seeks to develop requirements for an enduring solution for a Supplier-	A DCC PA has been requested. There was a Working Group meeting on Tuesday 24th July 2018.										Interim DMR				
<div><div>« »</div><div>IntroductionModification RegisterRelease ScopeImpacts Matrix</div><div><div>+</div><div>« »</div></div></div>																				

Current status of open modifications



Contact us and further information



- **Email:**

- SEC.Change@Gemserv.com

- **Helpdesk:**

- 0207 090 7755

- **Website:**

- <https://smartenergycodecompany.co.uk/about-modifications/>

- <https://smartenergycodecompany.co.uk/modifications/>

- **Change Delivery Manger:**

- David Kemp

- **Change Consultant:**

- Alison Beard

- **Change Lead Analysts:**

- Cordelia Grey

- Harry Jones

- Joe Hehir

- Nikki Olomo



Questions?

Cordelia Grey, Senior Change Analyst,
SECAS

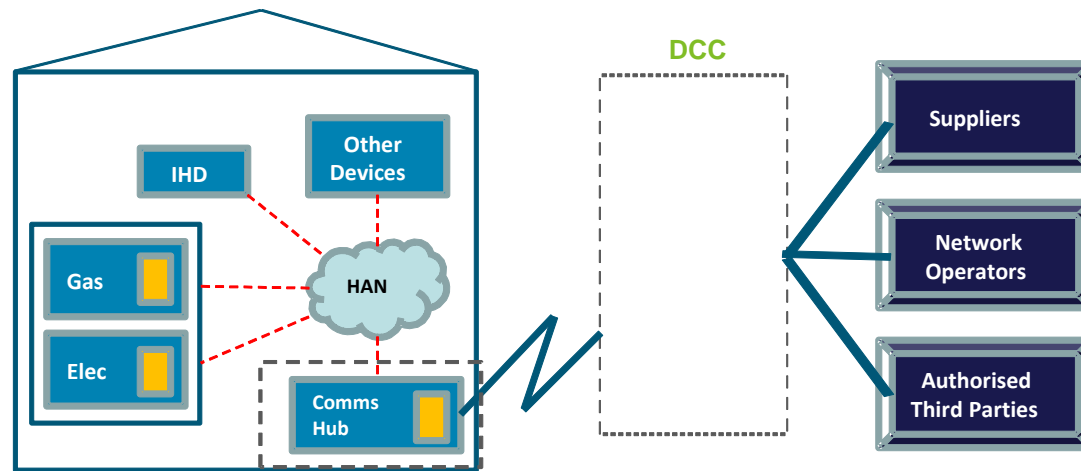


Introduction to Technical Specifications

Phillip Twiddy, Principal Consultant,
Gemserv

What makes a Smart Meter smart?

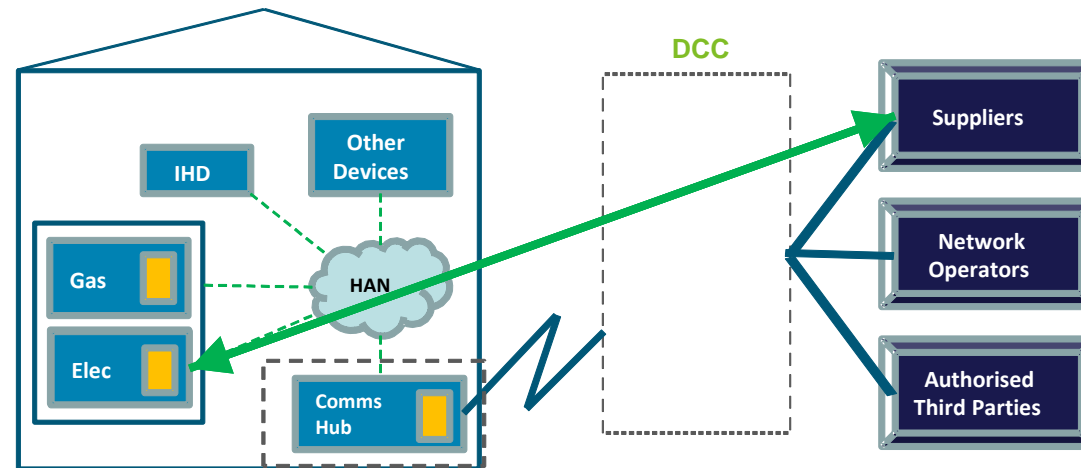
- Two way communications:
 - With other devices in the premises
 - With organisations outside the premises



- To control or use functions on the device:
 - What the meter measures
 - How much is consumption costing
 - How much credit the consumer has
 - How much debt the consumer owes and payments against that
 - Whether the supply is enabled or not

(Some) Objectives of Smart Metering

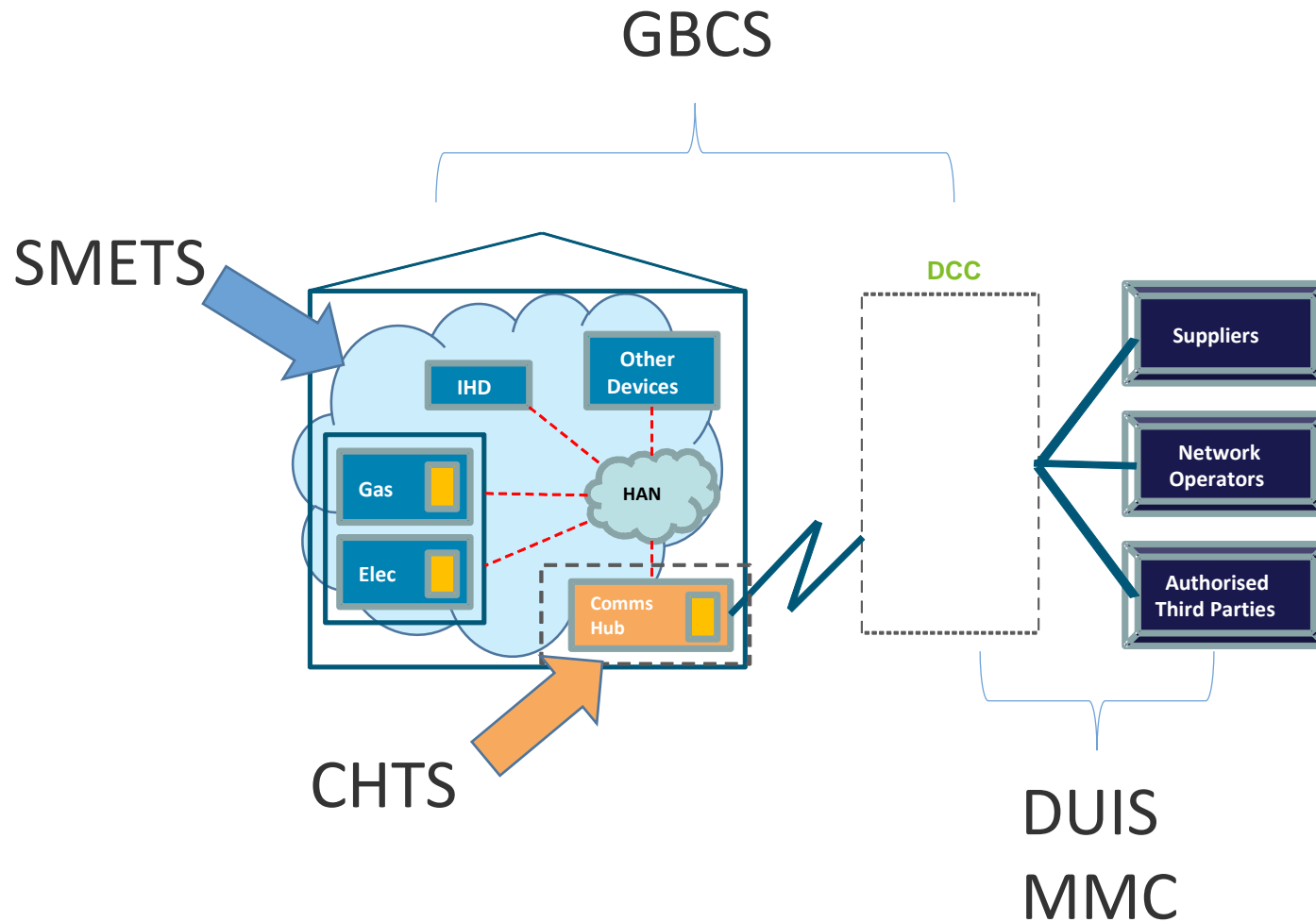
- Any 'compliant' device will:
 - Work with the DCC...
 - ... just like any other 'compliant' device



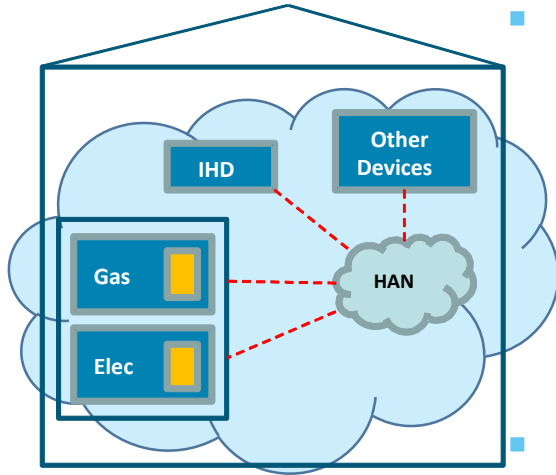
- And with all the other 'compliant' devices.

Achieving Uniformity

- Technical Specifications!

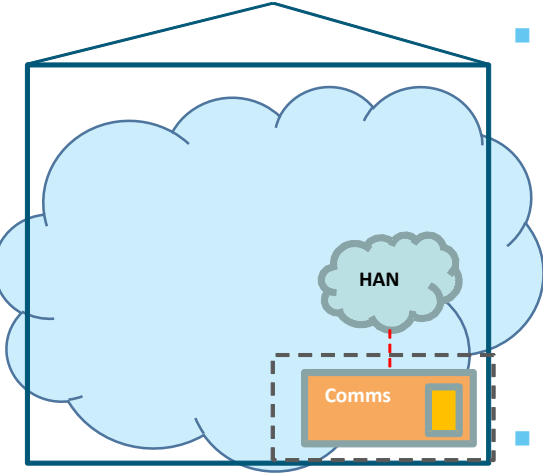


Smart Metering Equipment Technical Specification (SMETS)



- Suppliers' licences require them to roll out Smart Meters:
 - Devices must meet the requirements in SMETS
 - Most of the requirements in SMETS are about
 - the functions the device has to be capable of doing,
 - and so the data it is capable of storing
- SMETS covers:
 - Gas Smart Metering Equipment (GSME)
 - Electricity Smart Metering Equipment (ESME)
 - In-Home Display (IHD)
 - Prepayment Interface Device (PPMID)
 - Home Area Network Connected Auxiliary Load Control Switch (HCALCS)
- SMETS defines the 'WHAT' for Supplier-procured Devices

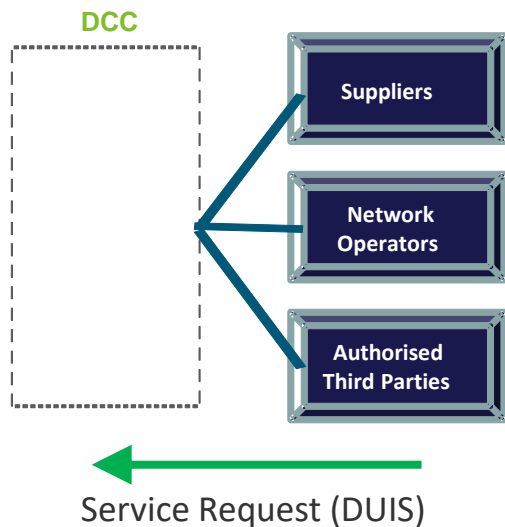
Communications Hubs Technical Specifications (CHTS)



- DCC Licence requires it to make Communications Hubs available:
 - Communications Hubs must meet the requirements in CHTS
 - Similar to SMETS, but for Communications Hubs
- CHTS has two groups of requirements for functions it has to be able to do:
 - Gas Proxy Function (GPF)
 - A view of GSME data to allow the GSME to go to sleep
 - Communications Hub Function (CHF)
 - To manage communications to, and between, Devices
- CHTS defines the 'WHAT' for DCC-supplied Communications Hubs

DCC User Interface Specification (DUIS)

- (DCC) Users communicate with Devices via the DCC by sending Service Requests.
- These are (reasonably) human-readable, using Extensible Markup Language (XML) 1.0.

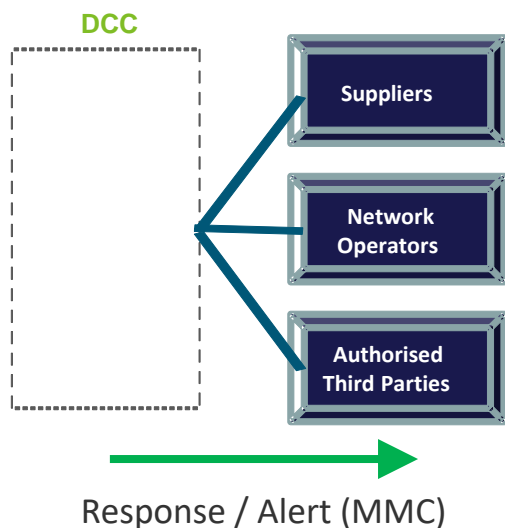


```
<?xml version="1.0" encoding="UTF-8"?>
<sr:Request schemaVersion="1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:sr="http://www.dccinterface.co.uk/ServiceUserGateway" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  - <sr:Header>
    <sr:RequestID>90-B3-D5-1F-30-01-00-00:00-DB-12-34-56-78-90-A0:1006</sr:RequestID>
    <sr:CommandVariant>4</sr:CommandVariant>
    <sr:ServiceReference>1.1</sr:ServiceReference>
    <sr:ServiceReferenceVariant>1.1.1</sr:ServiceReferenceVariant>
  </sr:Header>
  - <sr:Body>
    - <sr:UpdateImportTariffPrimaryElement>
      - <sr:ElecTariffElements>
        <sr:CurrencyUnits>GBP</sr:CurrencyUnits>
      - <sr:SwitchingTable>
        - <sr:DayProfiles>
          - <sr:DayProfile>
            <sr:DayName>1</sr:DayName>
          - <sr:ProfileSchedule>
            <sr:StartTime>00:00:00.00Z</sr:StartTime>
            <sr:TOUTariffAction>2</sr:TOUTariffAction>
          </sr:ProfileSchedule>
        </sr:DayProfile>
      </sr:DayProfiles>
    </sr:SwitchingTable>
  </sr:UpdateImportTariffPrimaryElement>
  </sr:Body>
</sr:Request>
```

- DUIS sets out the definition for all Service Requests.

Message Mapping Catalogue (MMC)

- (DCC) Users receive Responses & Alerts Devices via the DCC.
- They are received in machine-readable format and converted to human-readable (XML) format usually using Parse & Correlate, which implements MMC.



```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <ra:GBCSResponse schemaVersion="1.0" xmlns:sr="http://www.dccinterface.co.uk/ServiceUserGateway"
  xmlns:ra="http://www.dccinterface.co.uk/ResponseAndAlert">
  - <ra:Header>
    <ra:BusinessOriginatorID>00-DB-12-34-56-78-90-A0</ra:BusinessOriginatorID>
    <ra:BusinessTargetID>90-B3-D5-1F-30-01-00-00</ra:BusinessTargetID>
    <ra:OriginatorCounter>1002</ra:OriginatorCounter>
    <ra:GBCSHexadecimalMessageCode>0037</ra:GBCSHexadecimalMessageCode>
    <ra:ServiceReference>4.8</ra:ServiceReference>
    <ra:ServiceReferenceVariant>4.8.1</ra:ServiceReferenceVariant>
  </ra:Header>
  - <ra:Body>
    - <ra:ResponseMessage>
      - <ra:SMETSData>
        - <ra:ReadActiveImportProfileDataRsp MessageSuccess="true">
          - <ra:LogEntry>
            <ra:Timestamp>2014-12-31T00:00:00.00Z</ra:Timestamp>
            - <ra:Electricity>
              <ra:PrimaryValue>95</ra:PrimaryValue>
            </ra:Electricity>
          </ra:LogEntry>
          - <ra:LogEntry>
            <ra:Timestamp>2014-12-31T00:30:00.00Z</ra:Timestamp>
            - <ra:Electricity>
              <ra:PrimaryValue>243</ra:PrimaryValue>
            </ra:Electricity>
          </ra:LogEntry>
        </ra:ReadActiveImportProfileDataRsp>
      </ra:SMETSData>
    </ra:ResponseMessage>
  </ra:Body>
</ra:GBCSResponse>
```

- MMC sets out the definition for Service Responses & Alerts.

Great Britain Companion Specification (GBCS)



- When a User sends a Service Request to communicate with a Device, DCC translates it into a machine-readable format.

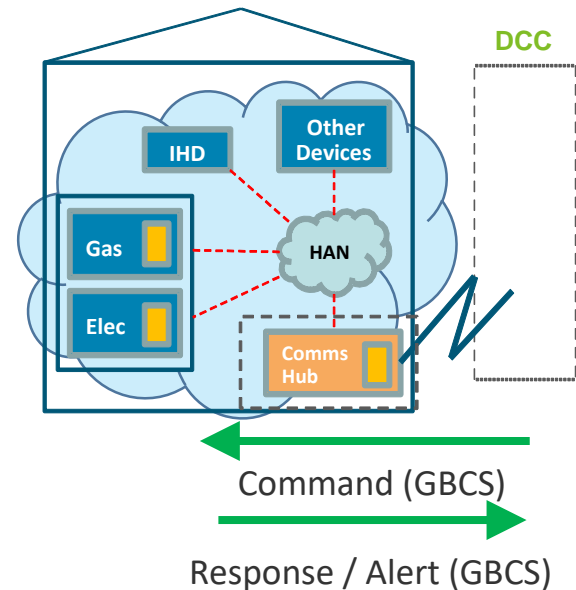
- Messages to Devices are GBCS Commands.

```
DD00000000000008205881100000000DF090100000000000003EE0890B3D51F30
0100000800DB1234567890A000020019820512D9200003EE001502001400000D
0000FF0702001400000D0000FF0802001400000D0000FF0902000B00010B0000
FF02020015000010010BFF02020015000010010CFF02020015000010010DFF02
020015000010010EFF02020015000010010FFF020200150000100110FF020200
150000100111FF020200150000100112FF0202232800005E2C02000402007100
00131404FF060200710000131400FF0602001400000D0000FF0A02232800005E
2C801D0602232800005F2C0200060200710000131404FF070200710000131400
```

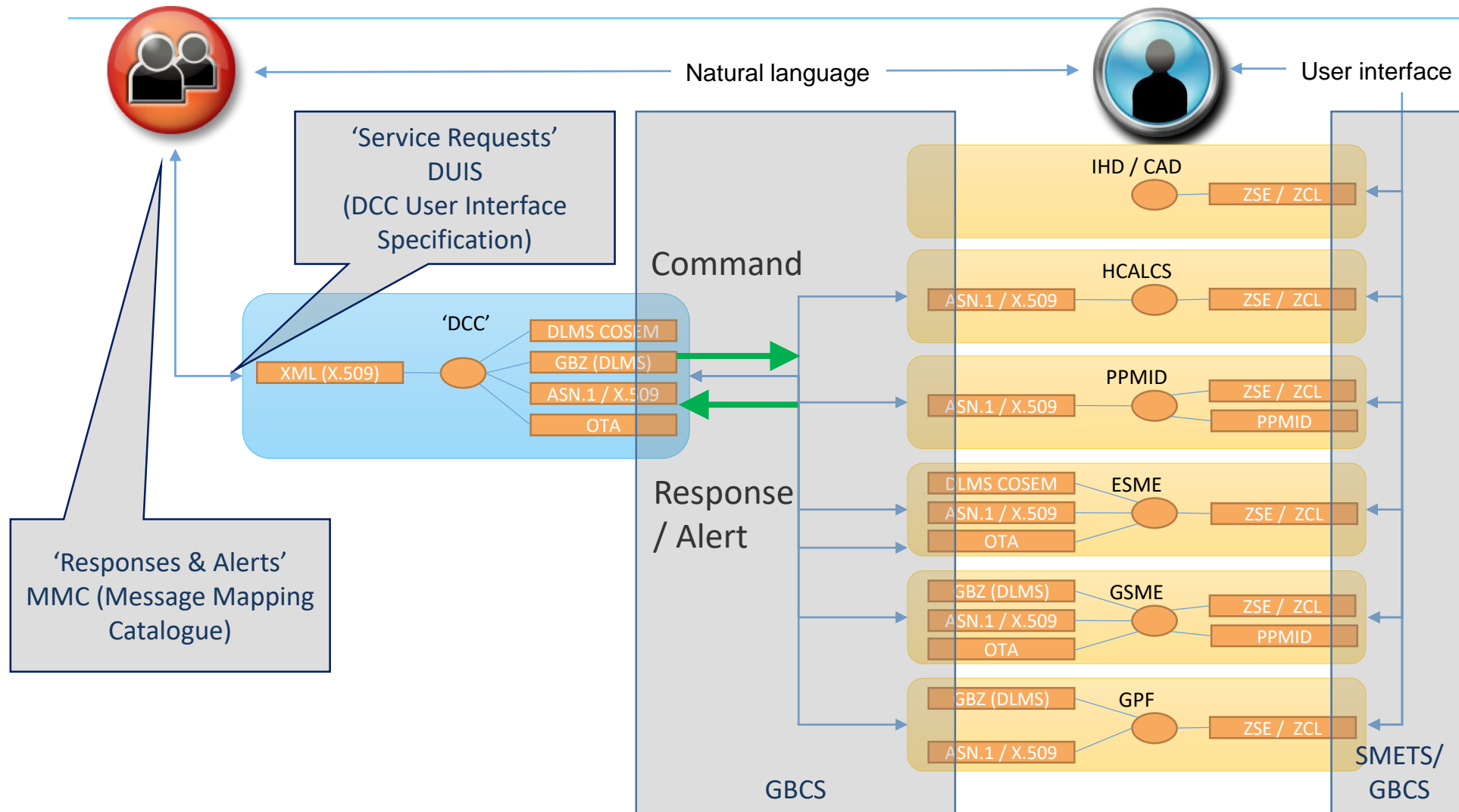
- Messages from Devices are GBCS Responses or Alerts.

```
pF09020000000000000003EE0800DB1234567890A00890B3D51F300100000C0
7DF0101FF000000008000FF02001948DA200003EE00001500000000000000
00000000000000000000000000000000000000000000000000000000000000
0020002000200020002000200020002000200020002000200020002000200020
358AB3AA0FC5D00F9F200F41141747AF694R2379ACFA0A3FRF5F9R1D47RD2
```

- GBCS sets out the definition for Responses & Alerts.



Which documents lay out how to use which protocols? (... and finally, a customer)

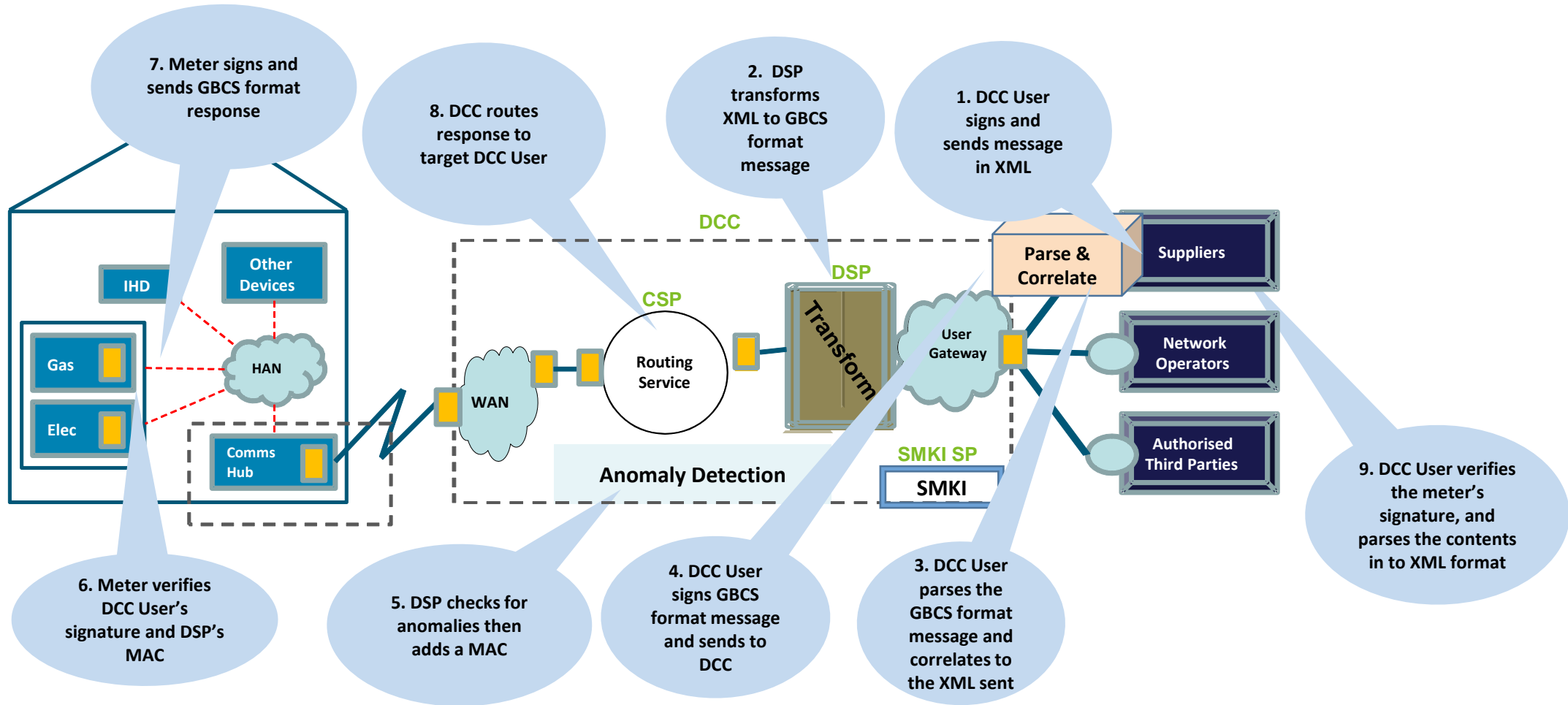


Some specific big numbers in messages



- (Digital) Signature:
 - tells anyone reading it that:
 - that the rest of the message is as it was sent, and
 - the sender definitely sent it (and can't deny sending it)
- Message Authentication Code (MAC):
 - tells the intended receiver:
 - that the rest of the message is as it was sent, and
 - the sender (or the receiver) sent it

An example that enables supply



Thank you



- References:
 - Smart Metering Equipment Technical Specification ([SMETS2v2](#)) – SEC Schedule 9
 - Communications Hubs Technical Specification ([CHTSv1.2](#)) – SEC Schedule 10
 - DCC User Interface Specification ([DUISv2.0](#)) – SEC Appendix AD
 - Message Mapping Catalogue ([MMCV2.0](#)) – SEC Appendix AF
 - Great Britain Companion Specification ([GBCSv3.1](#)) – SEC Schedule 8



Questions?

Phillip Twiddy, SMDA Scheme

Introduction to Alternative Home Area Network

Introduction to the SEC
19th September 2018

Caroline Milner
Alt HAN Business Support



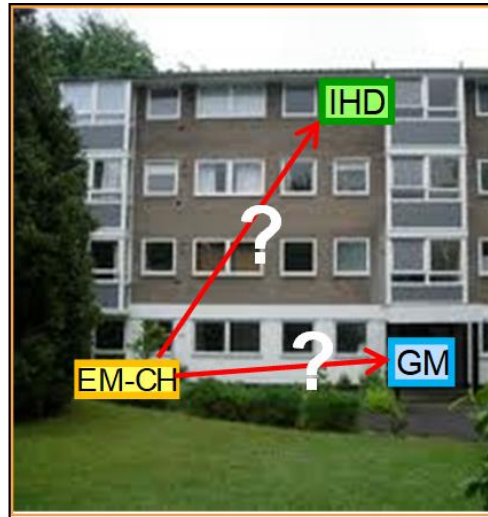
Agenda

1. What is Alternative HAN?
2. Why is Alternative HAN significant?
3. Key developments in preparing for delivery

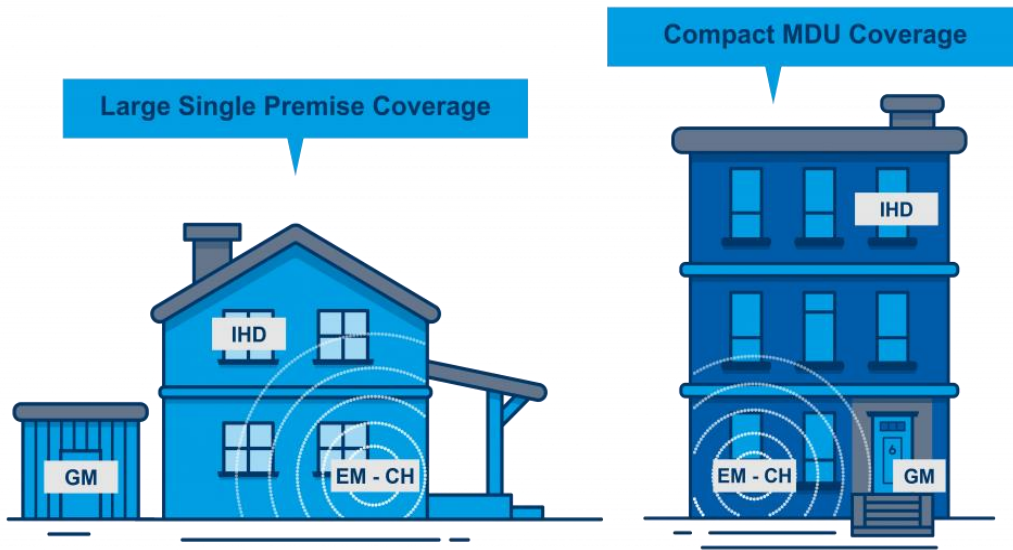
What is Alternative HAN?

A service to Suppliers that solves a problem:

- “Missing piece of the jig-saw”, where:
- Meter + DCC services \neq full smart customer experience
- Because 2.4 GHz or 868 MHz cannot propagate far enough, given distance in some premises from Comms Hub (CH) to IHD and/or Gas Meter



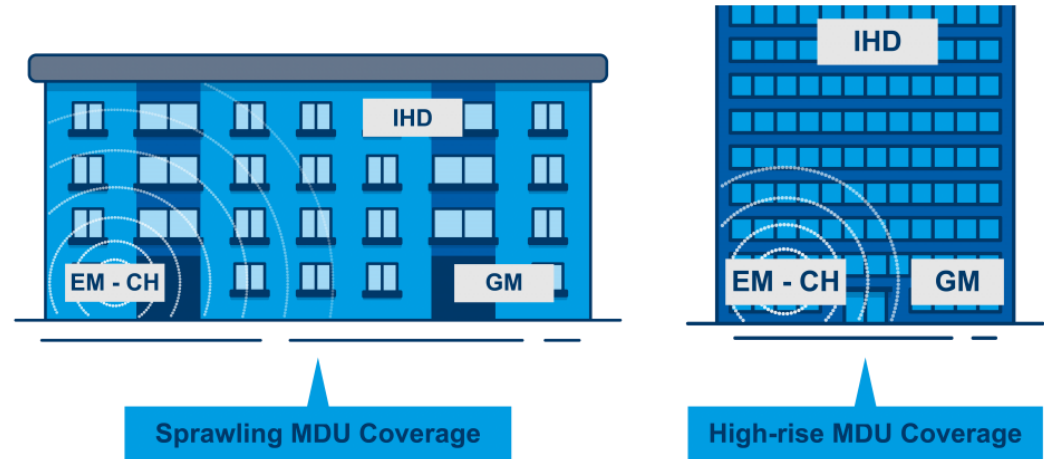
Alternative HAN – routes to solution



KEY

- CH – Communications Hub. The Communications Hub is the device that enables the Smart meter to communicate to the devices in the home.
- IHD – In home Display. All energy suppliers provide an IHD to all their customers when a Smart meter has been installed. This provides the customer with information regarding their energy usage.
- EM – Electricity Meter
- GM – Gas Meter

- **Simple Solution** – point-to-point repeater-like device to extend the range. Likely to be installed by the supplier at the time of smart meter installation
- **Complex Solution** – managed end-to-end service to include building assessment, building sponsor engagement, separate installation visit, maintenance and logistics Shared between multiple suppliers



What is Alternative HAN?

A “regulated co-operative” of Suppliers

- Empowered by the Smart Energy Code to make commercial decisions with the eighth general SEC objective being to facilitate the establishment and operation of the Alt HAN Arrangements
- Underpinned by Energy Supply Licence obligations on Suppliers to ensure the availability of services to facilitate the installation and operation of equipment that will enable the extension of the HAN
- Costs recovered via DCC charges
- Alt HAN Forum as decision-making body
- Alt HAN Company as contracting vehicle with a single purpose to serve the Alt HAN arrangements

Why is Alternative HAN significant?

1. Opportunity

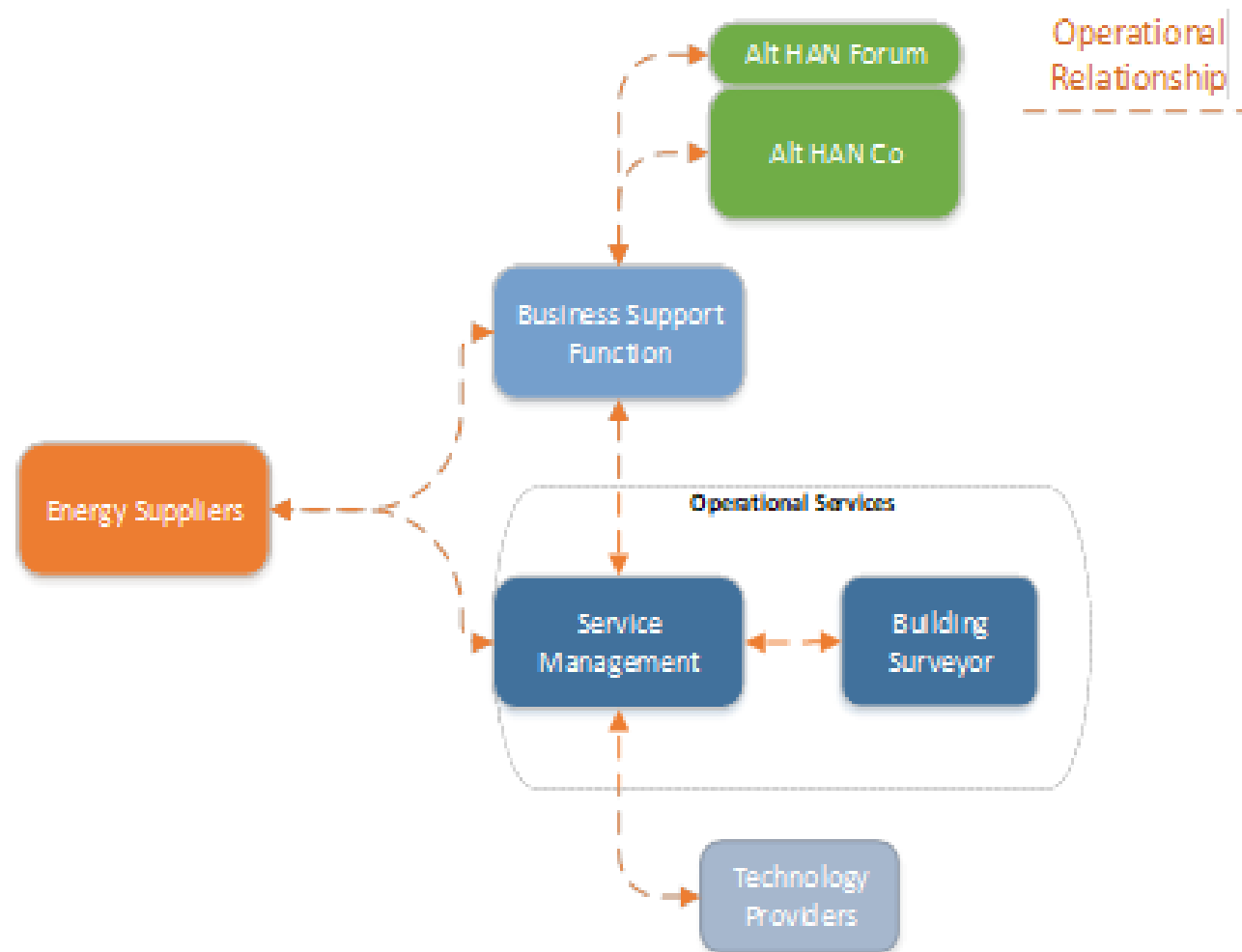
- To extend the full smart customer experience, and benefits
- To an estimated extra 5% (or ~1.5 million) premises in GB
- Including many disadvantaged areas

2. Risk

- Contribution to potential shortfall against 2020
- More distance to travel, less time available
- Scenario of Alt HAN being large % of overall under-delivery

Target Operating Model (TOM)

- The TOM describes how Alt HAN will organise itself to deliver Alt HAN services to energy suppliers.
- This slide shows the view from the perspective of operational relationships.
- A key point to note is that energy suppliers will engage through a service management layer – and not directly with technology providers.



Key Developments

Technology Procurement

1. Revised commercial strategy – “technology partnership” model
2. Stage gates process:
 - Gate 1 = Selection and Initial Design
 - Gate 2A = Detailed Design
 - Gate 2B = Design Assurance & Prototyping
3. Issued ITT – requested coverage of all use cases - a number of tenders received
4. Forum decision made in August 2018 to move to Phase 2

Operational Services Procurement

1. Operational Services Commercial Strategy developed
2. Requirements Set
3. Vendor engagement – positive
4. Issued ITT to the market
5. Now closed – a number of tenders received
6. Undergoing evaluation

Key Developments

Alt HAN Co/Supplier Contract

1. Standardised agreement and a number of schedules to cover the relationship between Alt HAN Co and Energy Suppliers
2. Suppliers will be required to accede to the contract in order to use Alt HAN Services
3. Framework being created with the support of the Supplier Contract and Governance Sub-Group
4. Consultation planned for Q1 2019
5. Accession Q3 2019

Key Developments

Exempt Premises List

1. EPL will identify premises where an Alt HAN solution is either 'technically impossible' or 'economically impractical'
2. Underpinned by Licencing obligations for Suppliers to work together to create the list;
 - 55.11 Where the licensee is a Relevant Supplier, it must, in conjunction and co-operation with all other Relevant Suppliers, establish and maintain the Exempt Premises List in accordance with this condition
3. Required to be approved by BEIS before Technology Manufacture begins
4. All Relevant Suppliers workshop held on 2nd August to agree the key concepts underpinning the development of the EPL
5. Further workshops to be held as the EPL develops

Key Planning Milestones

From Alt HAN Forum High-Level Programme Plan

1. Technology Services Contract Signature: Sep 2018
2. Operational Services Contract Signature: Nov 2018
3. Supplier Forecasting capability mobilises: Q2 2019
4. Alt HAN Co/Supplier Contract Accession: Q3 2019
5. Exempt Premises List Approval: Q3 2019
6. Alt HAN services P2P “safe launch”: Q4 2019
7. Alt HAN services Shared Solution “safe launch” Q2 2020

Contact the Alt HAN Secretariat to join the Forum and/or become further involved in Alt HAN

althan@gemserv.com or 0207 090 7766.

Summary of Answers to Participant Questions



There is a supplier obligation to accede to Alt Han CO Forum and to pay Alt HAN charges but there is no obligation to actually use the Alt HAN solution once developed if Suppliers have their own functioning solution. It is recognised that this creates a risk that solutions may not be interoperable, but this estimated not to be very large.

A property survey will be conducted in 2019 to identify where Alt HAN solutions are needed prior to the solution being available to install in late 2019. In the meantime Suppliers have a knowledge of the type of customers and properties they serve and estimate their need, but need not conduct their own surveys.



Smart Meter Device Assurance Scheme (SMDA)

Intro to the SEC
19 September 2018

Presenter: Louise Singleton



Agenda

- What is SMDA?
- What and how we test
- Current status
- Priorities and future plans
- Membership

What is SMDA?

A voluntary Scheme set up by members to provide assurance that smart meters will work effectively in a smart environment

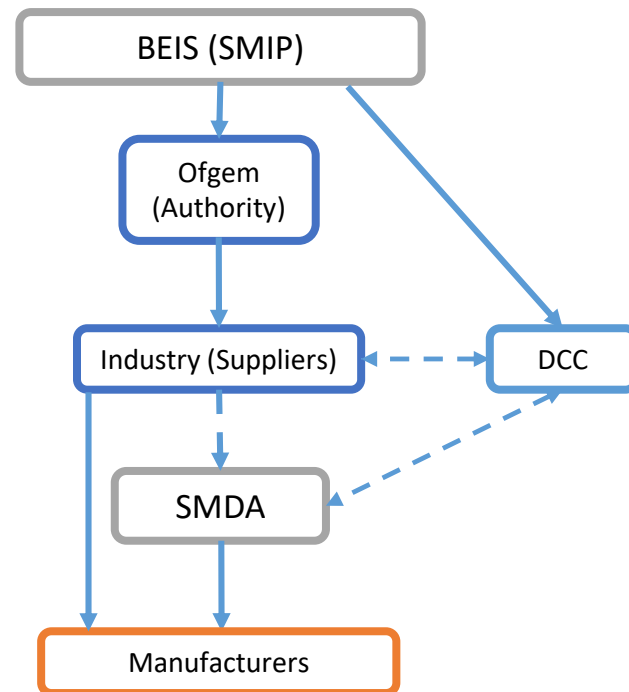
Interoperability

- Evidence for Suppliers that devices and firmware are interoperable with the DCC and its systems
- Assurance for Suppliers that any SMDA assured Device can be operated in the same manner and produce the same results whether installed or inherited

Interchangeability

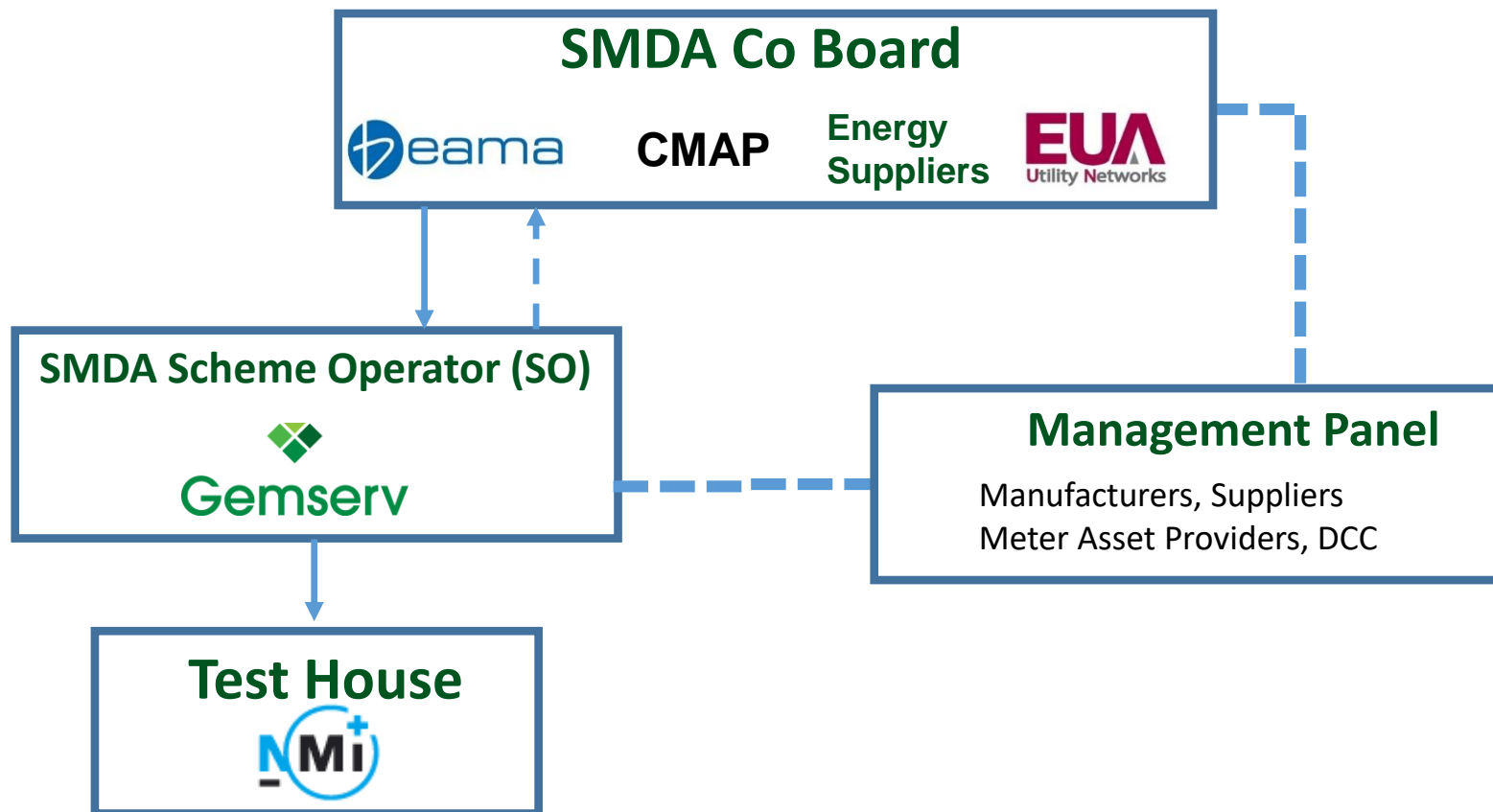
- A level of assurance that different combinations of device hardware models/versions, manufacturers and firmware versions are compatible with each other

SMDA relationship with SMIP



- SMDA is not formally part of BEIS SMIP, and does not currently appear on the JIP. However, regular updates on progress are provided, given its importance to overall rollout plans

The scheme is lead by industry for industry



SMETS compliance

- Suppliers' obligation to ensure devices are SMETS compliant (referenced in Ofgem Open Letter May 2018)

"Suppliers are responsible for ensuring that all smart meters in their portfolio are SMETS compliant, and should make sure they have processes in place to satisfy themselves before including meters in their reporting. Suppliers might find it useful to be aware of the Smart Meter Device Assurance (SMDA) Scheme. This scheme is not mandatory, but it aims to provide assurance that any approved smart metering equipment can effectively interface with other equipment on the Home Area Network (HAN) and receive and interpret messages from the DCC."

- SMDA testing covers c67% of SMETS2 requirements

In scope	67%
Not planned	24%
Not testable	9%
Total	100%

Requirements don't relate to interchangeability or interoperability

e.g. Security issues tested by CPA

- A device must pass ALL tests in order to receive SMDA Assurance - a fail would indicate device is not SMETS compliant



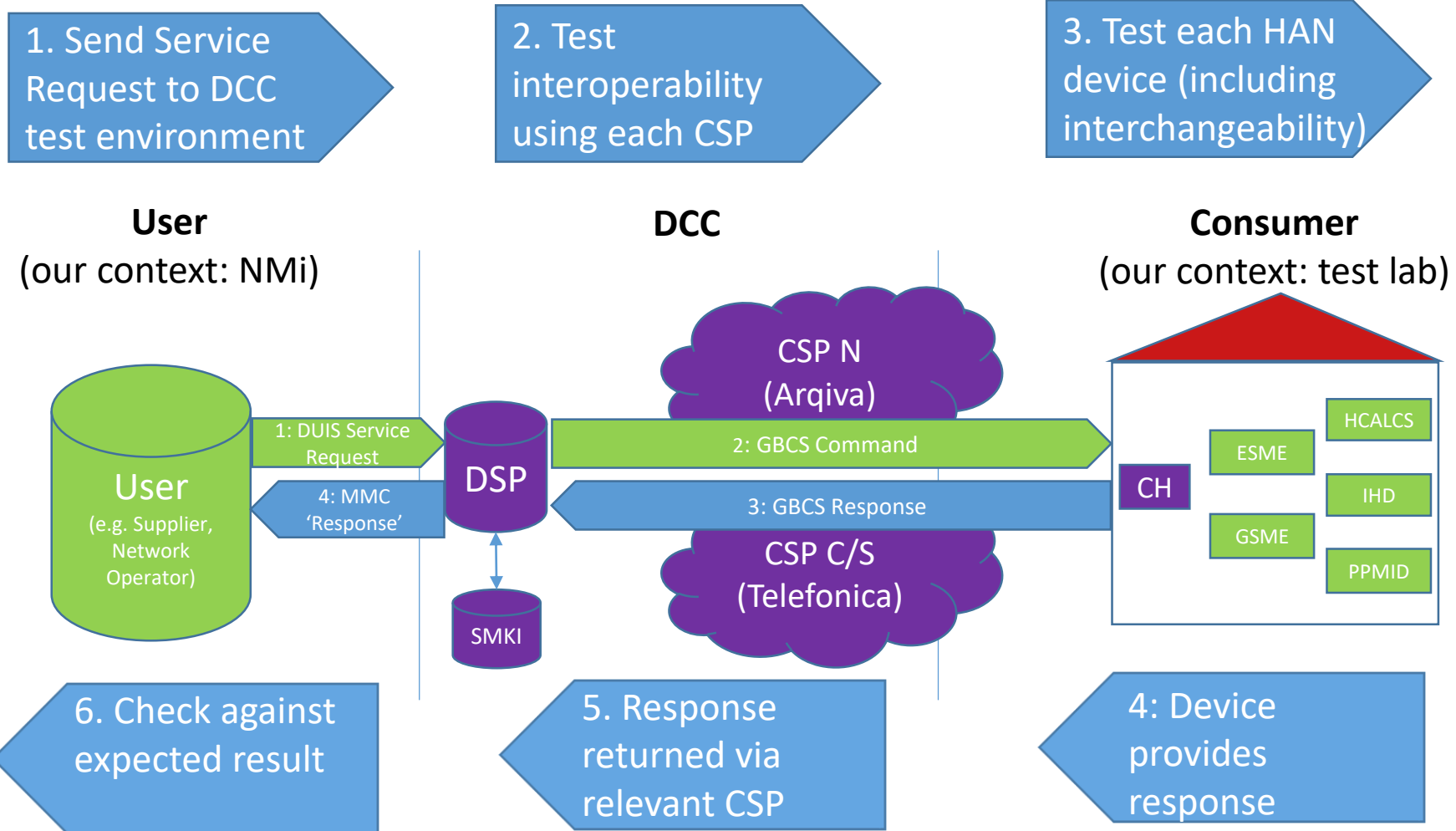
Agenda

- What is SMDA?
- What and how we test
- Current status
- Priorities and future plans
- Membership

What we test

- Over 300 test scripts designed to test:
 - Interoperability: Correct processing and Response to valid Commands
 - Interchangeability: Correct operation between Devices on the HAN
 - Correct generation of Alerts and event logging
 - Support for SMKI Recovery
 - Additional SMETS requirement, including recording consumptions against tariffs correctly
- Devices will be tested against different combinations of IC units
 - 3 of each device type (ESME, GSME, Combined PPMID) currently being tested will become the initial set of IC units
 - These will be published on our website and will be refreshed over time

How we test



Issue triage & learnings share

- We operate a comprehensive issue triage process using a variety of means
 - Emulators
 - Sniffers
 - DCC Test Lab
 - Manufacturer debugging
- We identify root cause of test failures
 - Test House failure
 - Device failure
 - Comms Hub, CSP, DCC failure
- We resolve and communicate with relevant parties

How SMDA differs to other testing

- CPA
 - A security assurance regime which sets out specific security-related requirements for design and assurance
 - CPA does not check for interoperability with the DCC systems, whereas SMDA does
 - Device doesn't need to be CPA approved to START SMDA testing, but must be in place before SMDA Assurance can be awarded
- Manufacturer testing
 - Unable to test interoperability with the DCC systems as don't have access to DCC systems
- Supplier testing
 - If using Friends & Family devices in a live environment, will get visibility of how business processes work but won't know '*why*' something has gone wrong – diagnostics lost in live
- SMDA Testing is unique
 - Test one device against multiple devices
 - Connection to DCC test systems



Agenda

- What is SMDA?
- What and how we test
- Current status
- Priorities and future plans
- Membership

Current status

- Early Mover Devices being tested
 - 8 devices which will become the 'Interchangeability Units' against which other devices will be tested
 - 3 ESMEs
 - 2 GSMEs
 - 3 Combined PPMIDs
- 90% of test scripts have been 'proven' – working through remaining issues which are a combination of device, testing infrastructure and DCC



Agenda

- What is SMDA?
- What and how we test
- Current status
- **Priorities and future plans**
- Membership

Priorities & future plans

Short term

- Completion of Early Mover testing
- Device bookings post 'Early Mover' testing
- Increased membership from small suppliers
- Release 2 preparation

Medium term

- We are actively pursuing ways to leverage the testing infrastructure we have built
 - DCC Communications Hub Testing
 - Additional Device Types



Agenda

- What is SMDA?
- What and how we test
- Current status
- Priorities and future plans
- Membership

Membership benefits for suppliers

Benefit	Benefit Details
Access to SMDA Documentation	<ul style="list-style-type: none">✓ Access to Test Specifications✓ Full access to all scheme documents and procedures, including traceability matrix
Access to the Device Assurance Register (DAR)	<ul style="list-style-type: none">✓ Only accessible by members✓ Assured devices listed with key features, such as make, model, SMDA baseline version, SMETS version, device history✓ Ability to check assurance status whether installed or inherited
Access to Test Reports	<ul style="list-style-type: none">✓ Manufacturers provided with a Test Report upon completion of testing✓ Supplier members (only) provided with SMDA Test Reports where evidence of testing required by Ofgem, through a governed process
Scheme Governance	<ul style="list-style-type: none">✓ Input into scheme governance, including testing requirements and future scope✓ Communication on testing progress✓ Representation on Management Panel & Board

Membership details & contacts

- One-off Membership Fee £2,500
- Annual Subscription Fee £250
- For details of how to apply, please find the application form and joining pack on SMDA website

www.smdascheme.co.uk

Tab: ABOUT/HOW TO BECOME A MEMBER

- Contact Us for more information

smdaso@gemserv.com

020 7090 1089

Testing Fees

- Supplier members funded set up of the scheme
- Manufacturers pay device testing fees, with SMDA members benefitting from reduced rates

Device	Member	Non-Member
ESME	£90,000	£99,000
GSME	£95,000	£104,500
PPMID/IHD Combined	£49,500	£55,935
IHD	£40,000	£45,250



Summary of Answers to Participant Questions



Membership will be Suppliers, meter manufacturers and Meter Asset Managers and it is planned that by the end of 2018 a set of “Golden Units” – Meters and other Devices will have been tested and provide a benchmark. The current SMETS2 meters in place have been subject to self-assurance by manufacturers but as roll out increases and thresholds are reached external testing will be needed. Whilst SMDA can only offer testing for two thirds of characteristics no other testing service can provide 100% testing – and 9% of testing (in addition to SMDA) will be covered as part of security assessment in any event.



User Entry Process - Becoming a DCC User

Mertcan Agir, Senior Security Analyst,
SECAS

Introduction



- User Entry Process Overview
- User ID
- Credit Cover
- SMKI & Repository Entry Process Tests
- User Entry Process Tests (UEPT)
- Security and Privacy Assessments

UEP Overview



User ID

Obtained from Panel via
SECAS
EUI-64 Compliant
Notified to the DCC

Credit Cover

Lodged with DCC (if
applicable)

SMKI and Repository Entry Process Tests (SREPT)

In accordance with
SMKI RAPP and

User Entry Process Tests (UEPT)

In accordance with
Common Test Scenarios

User Security Assessment

Undertaken by Competent
Independent Organisation
procured by SEC Panel
SEC Section G3-G6

User Privacy Assessment

Undertaken by Independent
Privacy Auditor procured by
SEC Panel
SEC Section I2 requirements

Section B2 – obtain an EUI-64 Compliant identifier used to identify a User acting in a particular User Role.

- SECAS advises Parties of their allocated EUI-64 Compliant identifiers for User IDs upon completion of the SEC Accession process.
- Parties are required to propose to the DCC the User IDs that the Party would like to use for each User Role.

User ID Checklist

- ✓ Can provide confirmation to SECAS that your User ID has been accepted by the DCC

Credit Cover



SEC Section J3 – Put in place a form of Credit Support if Credit Cover Requirement is over the Credit Cover Threshold

- The value of Credit Cover is determined by the DCC and will be notified to the Party upon acceding to the SEC.
- **Credit Cover Requirement = Value at Risk – Unsecured Credit Limit**
- No credit cover is required until the monthly DCC invoice surpasses £2000.

Credit Support Checklist

- ✓ Can confirm that Credit Cover arrangements have been agreed with the DCC

SMKI & Repository Entry Process Tests



SEC Sections H14 and L7 – become an Authorised Subscriber and interoperate with the SMKI Repository.

- In accordance with the SMKI & Repository Test Scenarios Document
- Is an Authorised Subscriber and a Subscriber under the Organisation and/or Device Certificate Policies
- Is eligible to access the Repository as set out in the SMKI RAPP
- Completed when DCC considers the Party has met the requirements of its SREPT

SREPT Checklist

- ✓ Can fulfil the requirements to be an Authorised Subscriber
- ✓ Can access the SMKI Repository

User Entry Process Tests (UEPT)



SEC Section H14 – UEPT tests the capability of a User to interoperate with the DCC.

- For each User Role and in accordance with the Common Test Scenarios Document
- Using Devices selected by the DCC
- Communications to and from the User and the DCC
- Test scripts and sequences developed by Party, and approved by the DCC
- Completed when DCC considers the Party has met the requirements of its UEPT

UEPT Checklist

- ✓ Can establish a DCC Gateway Connection
- ✓ Can use the DCC User Interface
- ✓ Can use the Self-Service Interface

Security and Privacy Assessments



Security obligations: SEC Sections G3 – G6

Privacy obligations: SEC Sections I2 – I5

Security Assessment

- All Parties require an initial Full User Security Assessment conducted by the User CIO
- Privacy Assessment
- ‘Other Users’ are required to undergo a Privacy Assessment to assess their compliance against the obligations set out in SEC Sections I1.2 to I1.5

Checklist

- ✓ Can complete the Initial Full User Security Assessment with an Assurance Status of ‘Approved’
- ✓ Can complete the Full Privacy Assessment with an Assurance Status of ‘Approved’

Who does what?



Requirement	By	From?
User ID RDP ID	User Role eligibility through Users notifying DCC of their EUI-64 identifier, and DCC accepts	Panel – (Section B2) SECAS issue these following accession
User Entry Process Test (UEPT)	User successfully completing UEPT for each User Role you will operate in line with the Common Test Scenarios Document (CTSD) <i>Note: RDPs are not a DCC User Role</i>	DCC – (Section H14) Party demonstrates to DCC's satisfaction that they meet the criteria to enter and exit
SMKI & Repository Entry Process Test (SREPT)	Users successfully completing SREPT in order to be an Authorised Subscriber for Organisation and/or Device Certificates	DCC – (Section L7) sets out that DCC confirms completion
Security Assurance	All Users complete their CIO Assessment under Security Controls Framework	Panel – (Section G8) via SSC consideration of CIO report
Other User* Privacy Audit	Other Users complete their CIO Assessment under Privacy Controls Framework	Panel - (Section I2)
Credit Cover	Provide credit support to DCC for User Role	DCC – (Section J3)

UEP Evidence Form



Smart Energy Code (SEC) User Entry Process (UEP) Evidence Form

SEC Section H1.11 states that a Party will have successfully completed the User Entry Process for a particular User Role once the Code Administrator has received confirmation from the body responsible for each of the requirements set out in SEC Section H1.10 that the Party has met all such requirements.

The SEC Party is required to tick the User Role(s) that they have undertaken as part of their User Entry Process:

User Role	
Import Supplier	<input type="checkbox"/>
Export Supplier	<input type="checkbox"/>
Gas Supplier	<input type="checkbox"/>
Electricity Distributor	<input type="checkbox"/>
Gas Transporter	<input type="checkbox"/>
Registered Supplier Agent	<input type="checkbox"/>
Other User	<input type="checkbox"/>

The responsible bodies are as follows:

- DCC – SEC Section H1.10 (a) – we would expect the Party to forward to SECAS the DCC's confirmation that a User ID for the Party for a particular User Role has been accepted. This will likely be a copy of an email from the DCC confirming the above (unless there is a formal document issued by the DCC).
- DCC – SEC Section H1.10 (b) – we would expect the Test Completion Reports to be submitted by a Party to SECAS as evidence to show they have completed Testing.
 - Although not explicitly set out in the SEC, Parties will need to have successfully completed SMKI and Repository Entry Process Testing (SREPT) before they can commence User Entry Process Testing (UEPT).
- SEC Panel – SEC Section H1.10 (c) – we would expect an email / report from the SEC Panel to notify that a Party has had an assurance status set to 'Approved'.
- SEC Panel – SEC Section H1.10 (d) (if applicable) – we would expect an email / report from the SEC Panel to notify that a Party has had an assurance status set to 'Approved'.
- DCC – SEC Section H1.10 (e) – we would expect the DCC to confirm to SECAS that Credit Support (or additional Credit Support) has been lodged for a SEC Party. This will likely be a copy of an email from the DCC confirming the above (unless there is a formal document issued by the DCC).

We expect the SEC Party to provide the above. However, if this has been misplaced or lost, SECAS can and may contact the responsible bodies who oversee the above requirements.



This UEP Evidence Form has been produced in order to confirm the same to the Party, capturing evidence as Appendices and time-stamping when each step has been completed.

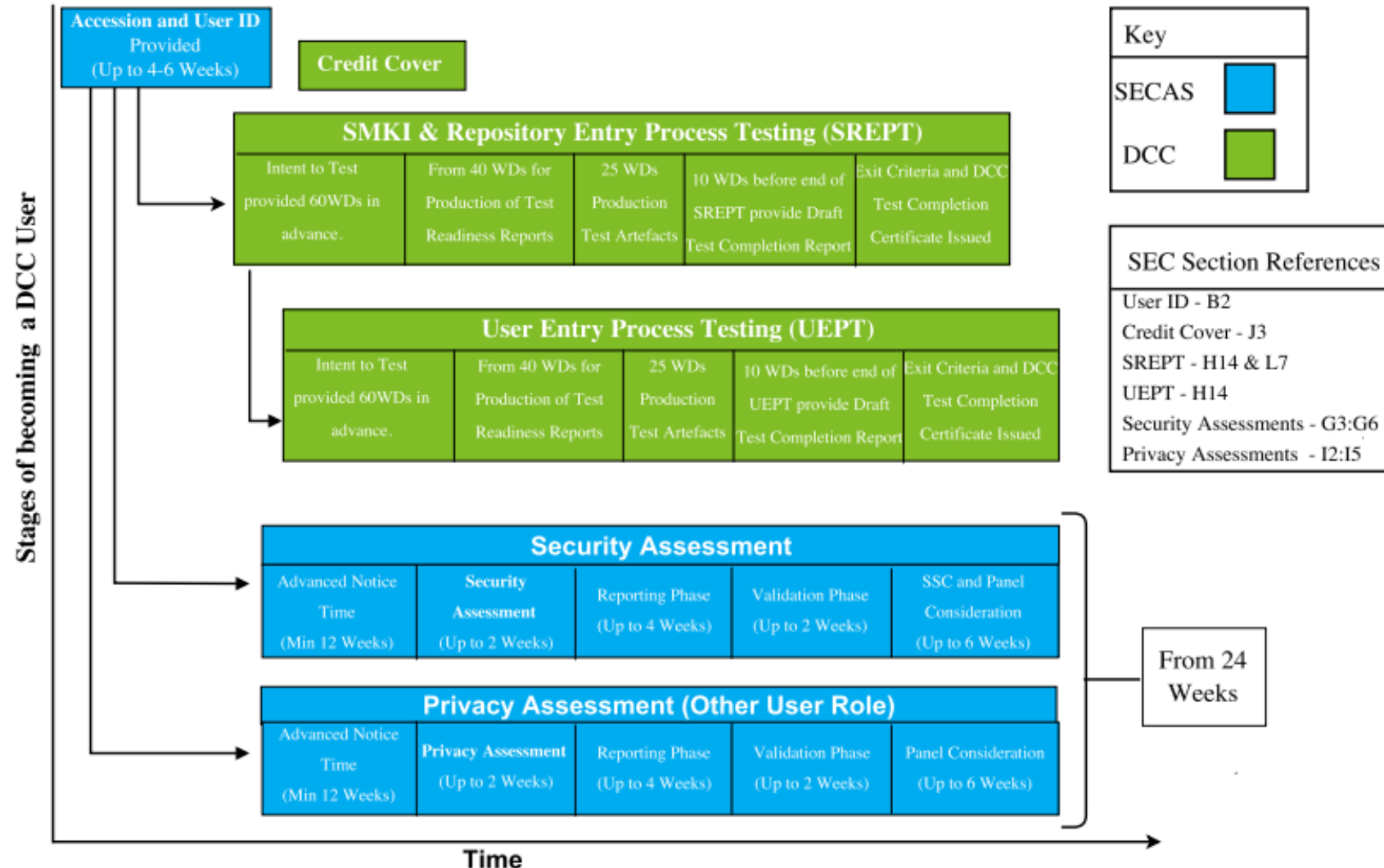
SEC Section H1.10 Clauses	Date Received	Evidence
SEC Section H1.10 (a) <i>Receive confirmation from the DCC that a User ID for the User Role has been accepted</i>		
SEC Section H1.10 (b) <i>Complete the required User Entry Process Tests for the User Role</i>		
SEC Section H1.10 (c) <i>Demonstrate the applicable security requirements were met, via a Security Assessment</i>		
SEC Section H1.10 (d) <i>If undertaking the process to act as an Other User, demonstrate that the applicable privacy requirements were met, via a Privacy Assessment</i>		
SEC Section H1.10 (e) <i>Provide Credit Support or additional Credit Support as required by the DCC</i>		

Table 1: UEP Evidence Form

If the above UEP Evidence Form has been completed incorrectly, or does not align to your own records, please contact the SECAS Helpdesk (secas@gemserv.com).

Please note: as required by the SEC, SECAS shall notify both the Party, as well as the SEC Panel and the DCC that a Party has completed UEP for a particular User Role.

Estimated Timeline for Becoming a DCC User





Questions?

Mertcan Agir, Senior Security Analyst,
SECAS



Security and Privacy Overview

Nick Blake, Senior Security Analyst,
SECAS

Introduction



1. Types of Assessment
2. Overview of the Controls Frameworks
3. Summary

Types of security assessment



Full User Security Assessment

Carried out by the User CIO to checks compliance with System, Organisational and Information Security obligations.

Verification User Security Assessment

Carried out by the User CIO to checks for any material increase in security risk since the last Full User Security Assessment

User Security Self-Assessment

Carried out by a User and reviewed by the User CIO.

Follow-Up Security Assessment

Carried out by the User CIO following an assessment to verify implementation of actions detailed within the User Security Assessment Response

Security assessment frequency

Supplier Parties			
Smart Metering Systems	Entry/Year One	Year Two	Year Three
More than 250,000	Full Assessment	Full Assessment	Full Assessment
Less than 250,000	Full Assessment	Verification Assessment	Self-Assessment
Network Parties			
Smart Metering Systems	Entry/Year One	Year Two	Year Three
More than 250,000	Full Assessment	Verification Assessment	Verification Assessment
Less than 250,000	Full Assessment	Verification Assessment	Self-Assessment
Other Users			
	Entry/Year One	Year Two	Year Three
	Full Assessment	Self-Assessment	Self-Assessment

Types of Privacy Assessment

Full User Privacy Assessment

User CIO checks compliance with I1.2 to I1.5 and review the systems / processes in place for ensuring compliance.

User Privacy Self-Assessment

Carried out by a User and reviewed by the CIO to identify material change in the systems in place to comply and the quantity of data being obtained

Random Sample Privacy Assessment

User CIO checks compliance in relation to a limited (sample) number of Energy Consumers (I1.2 – I1.5).

	Other Users		
	Entry/Year One	Year Two	Year Three
Three Year Privacy Assessment Cycle	Full User Privacy Assessment	User Privacy Self-Assessment	User Privacy Self-Assessment
On instruction from the Panel	Random Sample Privacy Assessment		

Prior to an assessment



Engaging with the User CIO

- Engagement with the User CIO shall be managed via SECAS;
- Users should seek to engage with the User CIO at least 12 weeks prior to their desired review date. Early engagement to schedule an assessment is strongly recommended;
- It is the responsibility of the User to engage the User CIO in accordance with the review cycle;
- Users should seek to engage with the User CIO when they have system stability and are confident that significant change will not occur;
- Users wishing to change the dates of an assessment must inform the User CIO at least 4 weeks prior to the original assessment start date. Failure to comply with this period may see the User incur a cancellation charge;
- Cancellation charges will be applicable if the User fails to comply with the appropriate cancellation period.

Prior to an assessment



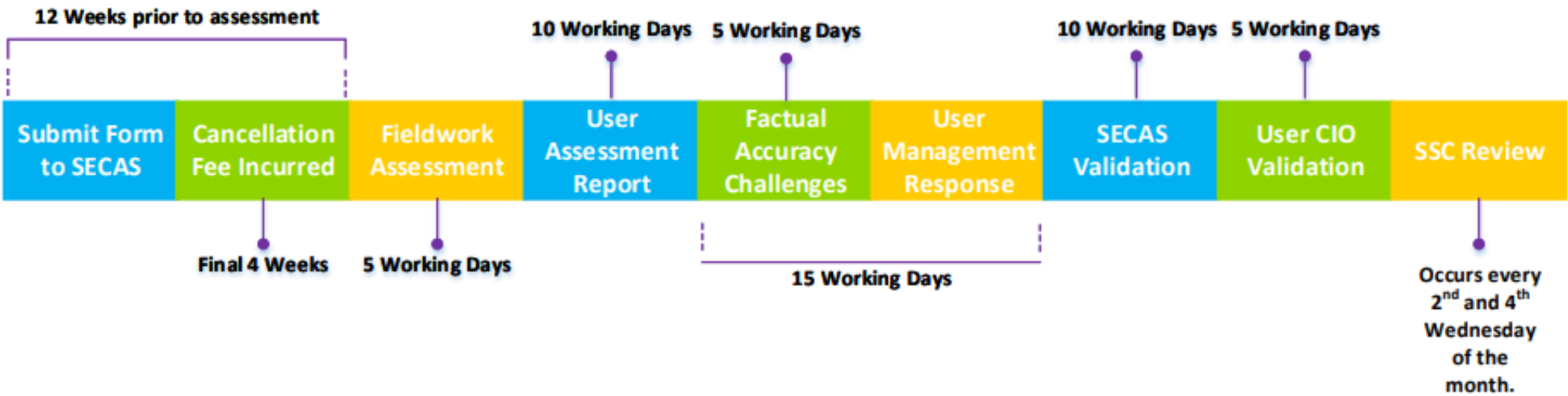
Information required by the User CIO

- The User CIO will engage with the User to determine the scope of the assessment as well as determine the scale, length, and involvement of User Personnel;
- User System scope document including key definitions;
- Locations within the scope of the User Systems and therefore the assessment;
- A nominated point of contact for the administration and planning of the assessment.

Information to be provided by the User CIO

- The User CIO will engage with the User to determine the scope of the assessment as well as determine the scale, length, and involvement of User Personnel.
- Where applicable, a preliminary schedule and assessment timetable;
- A list of key User Personnel, by role, who the User CIO may need to meet with during the assessment. This may include third party suppliers;
- A document request list;
- A proposed assessment team with a User CIO key point of contact.

Security and Privacy Assessment Timeline



During a Full User Security Assessment



A “Full User Security Assessment” is an assessment carried out by the User CIO to assess compliance against the obligations specified in SEC Sections G3 to G6 in each of its User Roles.



It is performed onsite and should take between 3 and 10 days on site primarily dependent on whether the User is engaged with an established Shared Resource or is seeking to create a bespoke User System.



The level of preparatory work completed by the User in advance of the User CIO assessment is another key factor determining how long the assessment will last.

Verification assessments



- Required for:
 - **Small Suppliers (Year 2)** – noting that those Users operating with Shared Resources will be treated as Large Suppliers for the purposes of assigning the assessment type
 - **Large Network Operators** (Years 2 & 3)
 - **Small Network Operators** (Year 2)
- ‘A "**Verification User Security Assessment**" shall...identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User’.

All Verification Assessments will use the previous FUSA as a starting point, with Users questioned on any changes made since that FUSA to maximise efficiency.

Verification assessment approach



- A Verification Assessment will address three key areas to determine the extent of any changes since the previous FUSA in:
 1. **Scope of the User System:** Users shall be questioned on the 'User System' and 'Separation' Als to understand whether any changes have been made.
 2. **Risk levels:** Re-assessment against G5.14 and G5.15 to understand whether the User has maintained an up-to-date risk assessment and assess whether the User has detected a change in its level of risk exposure.
 3. **Changes in approach to risk mitigation:** Re-assessment of the risk appetite to understand whether any changes have been made there, and of the high-level alignment with ISO 27001, to include the 'proportionality' obligation.

Verification assessment scope



All Users

- User System: Agreed Interpretation
- Separation: Agreed Interpretation & G3.14
- Risk Management: G5.14 – G5.16
- Overall alignment with ISO 27001: G5.17 – G5.18 (part (b) (iv) only)
- Setting Anomaly Detection Thresholds: G6.3 – G6.4
- Vulnerability Assessment review: G3.8
- Vulnerability Management & Reporting: G3.9

Supplier Parties only

- Supply Sensitive Check: G3.23 – G3.25
- Detection of Anomalous Events: G3.15 – G3.16
- Penetration testing review: G3.7

During a User Security Self-assessment



A “User Security Self-Assessment” is an assessment carried out by the User to identify any material increase in the security risk since the last occasion on which either a Full User Security Assessment or Verification User Security Assessment was carried out.



The scope of this assessment focuses on those areas exposed to any material increase in security risks as indicated by a User’s obligation to identify and manage risk (in accordance with G5.14).



The User is required to produce a report for review and corroboration by the User CIO prior to presentation to the SEC Panel.



The template containing the questions posed to the User is currently under review by the SSC, and will be included within the next draft of the SCF.

Self-assessment questionnaire



To support the User Security Self-Assessment the User CIO has developed a Self-Assessment template consisting of 4 sections:

1. Introductory Information

- i. How has your customer base changed with regards to number of smart metering systems (SMETS2)?
- ii. Have there been any changes to arrangements with Shared Resource?

2. How has the scope or method of operation of your User System changed, if at all, since your last Full Assessment?

- i. Have there been any changes to the functionality that you offer to customers with regards to Smart Metering solution?
- ii. How has the configuration of your User System changed?

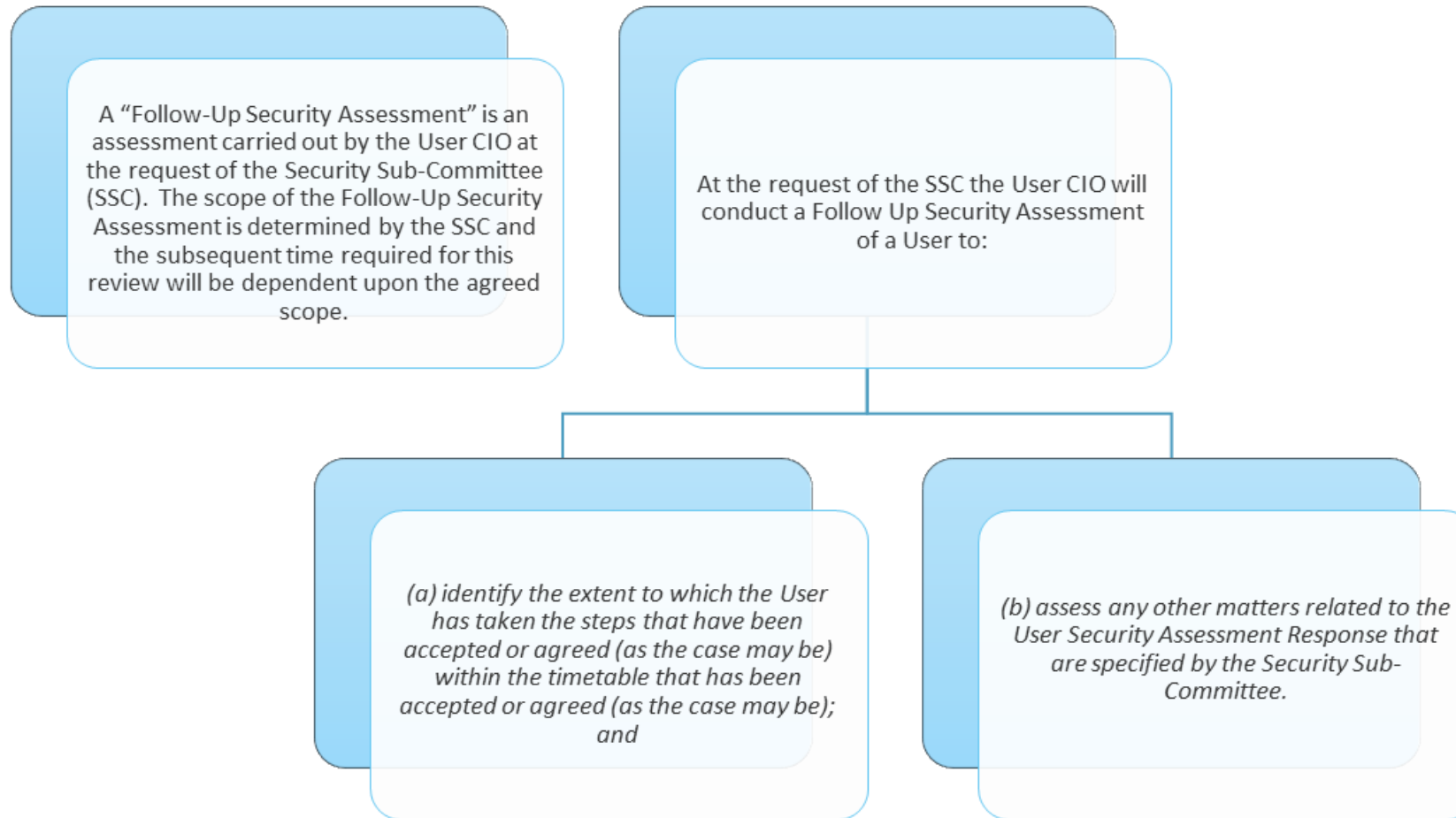
3. How do you consider the risks have changed, if at all, since your last Full Assessment?

- i. Have there been any changes to the Risk Management processes?
- ii. How has the threat landscape changed?

4. How has your approach to risk mitigation changed, if at all, since your last Full Assessment?

- i. Have you modified the security controls used to mitigate risk?
- ii. Has there been a shift in your organisation's risk appetite?

During a Follow-Up Security Assessment



After the assessment



Following the completion of an Assessment the User CIO will produce a written report.



The User CIO will submit a draft copy of the report to the User for review. The User shall have 5 working days to request changes for consideration and a further 10 working days to produce a Management Response to the findings.



This Management Response will be validated by SECAS to ensure that the responses provided adequately address the observations raised, with the User having an opportunity to update the response in line with any comments received.



The User CIO then performs a final validation ahead of the consolidated documented being presented to SSC.



Controls frameworks: Overview

Nick Blake, Senior Security Analyst,
SECAS

What are the SCF and PCF?



- The Security Controls Framework (SCF) and Privacy Controls Framework (PCF) are documents developed by the User CIO with the support of the Security Working Group (User CIO, BEIS, SECAS), and SSC (through review).
- **The controls frameworks serve a number of functions:**
 - Describing the type of evidence the CIO would seek to receive to demonstrate compliance with the SEC.
 - Describing the assessment protocols, regarding how the assessments will work.
 - Creating a consistent approach to the way in which Users are assessed for compliance.

Assessment logistics



- The SCF & PCF set out (amongst other topics):
 - When and how to engage the CIO;
 - What to expect during the assessment, and requirements on the User;
 - Indicative timescales, and how to manage changes to these;
 - Who the CIO would expect to meet with;
 - How to achieve an efficient review;
 - Minimising disagreements;
 - The approach taken to ensuring data confidentiality;
 - Assessment variations.

Control descriptions



The controls frameworks describe:

- The different types of User Assessment including the applicable assessment criteria and frequency of assessment.
- The activities and requirements of each stage of the assessment lifecycle: prior to an assessment, during an assessment and post-assessment.
- Key information and logistical requirements around how a User should engage with the User CIO, as well as indicative timetables and example schedules for the assessments.
- The questions the User CIO might ask, and the evidence it might expect to see from a User to support the assessment.

The controls frameworks will not be:

- Overly prescriptive.
- A replacement for the regulation.
- Exhaustive in their description of the questions / evidence that the CIO may seek to support its work.

Summary



- Users will be subject to Security assessments upon User Entry (and each year thereafter) which are proportionate to the risk they introduce into the system.
- Other Users will also be subject to Privacy assessments, to verify their compliance with relevant SEC obligations.
- Early engagement with the User CIO will be beneficial to Users in securing their desired assessment date.
- The SCF and PCF are documents which have been produced to guide the assessments – they provide clarification of the protocols applying to the assessment process and examples of the types of evidence the CIO may wish to see, and questions which are likely to be asked of the User.



Questions?

Nick Blake, Senior Security Analyst,
SECAS