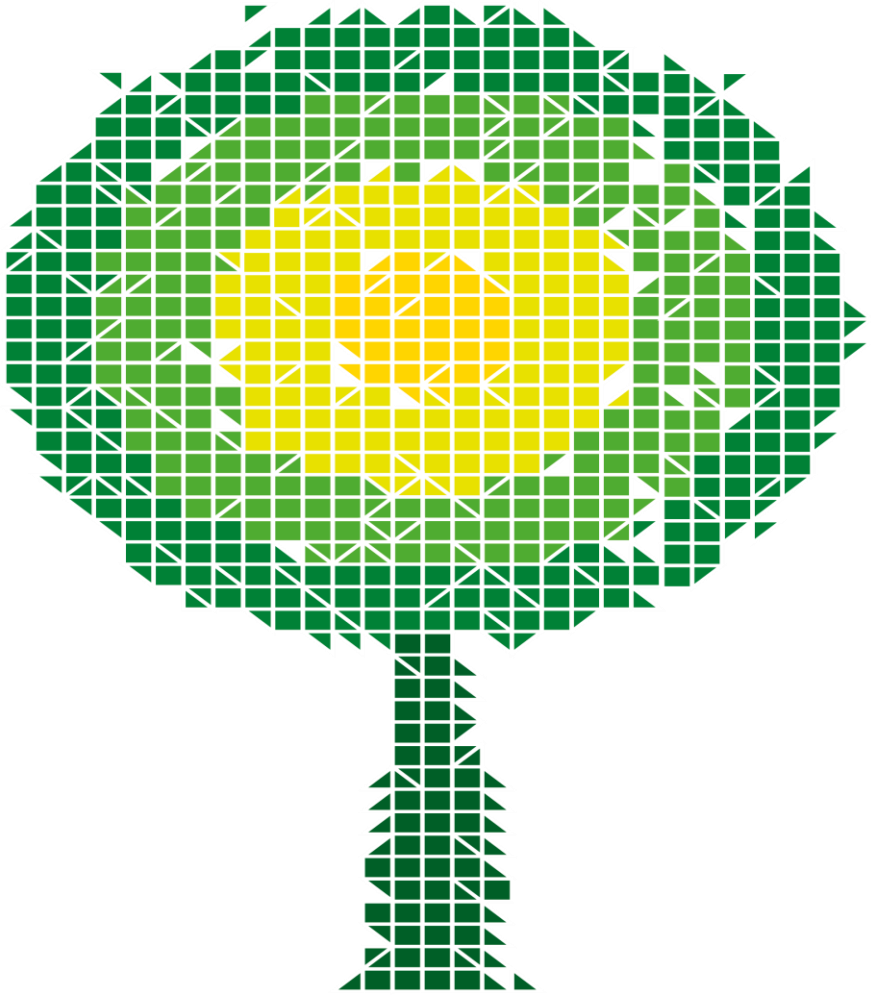
Spotlight on the SEC

Thursday, 8th March 2018



Gemserv

SEC Smart Energy Code

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

Global GROUP ISO 14001 UKAS 0039

Global GROUP ISO 50001 UKAS 0039

ISO 9001 UKAS 001

CYBER ESSENTIALS PLUS

Spotlight on the SEC: Security and Privacy Assessments

Alistair Grange,
User Competent Independent Organisation (CIO)

Agenda

1. Overview of the controls frameworks
2. Types of assessment
3. Using the controls frameworks
4. Summary

CONTROLS FRAMEWORKS: OVERVIEW

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.

TYPES OF ASSESSMENT

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.

DURING AN ASSESSMENT

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’ AIs 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

- A “Follow-Up Security Assessment” is an assessment carried out by the User CIO at the request of the Security Sub-Committee (SSC). The scope of the Follow-Up Security Assessment is determined by the SSC and the subsequent time required for this review will be dependent upon the agreed scope.
- At the request of the SSC the User CIO will conduct a Follow Up Security Assessment of a User to:

  (a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

  (b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

AFTER AN 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.

USING THE CONTROLS FRAMEWORKS

Organisation

- The SCF and PCF are ordered in alignment with the SEC obligations, with guidance supplementing each obligation.

SEC Obligation #	SEC Text
What the CIO may take into consideration	Description
What evidence the CIO might expect to see	Description

Security Controls Framework

SEC Obligation G3.5	**Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, promptly notify the Panel and the Security Sub-Committee.**
What the CIO may take into consideration:	• How have you interpreted the definition of a 'Major Security Incident'? • How do you classify Security Incidents to determine which are Major Security Incidents? • Upon the occurrence of a Major Security Incident, what process do you follow for notifying the SEC Panel and the Security Sub-Committee, and within what timeframe do you aim to provide this notification? • What level of detail do you provide as part of that notification (e.g. does it include the incident type, number of affected users within your organisation etc.)?
What evidence the CIO might expect to see:	• Security Incident Management policy and procedures, including documented incident triage and classification criteria. • Evidence of testing of the security incident management procedure, technical solution and reporting mechanism. • Detailed roles and responsibilities including who is responsible for notifying the Panel and Security Sub-Committee in the event of a Major Security Incident.

Security Controls Framework

SEC Obligation G3.16	**Each Supplier Party shall:** **(a) use its reasonable endeavours to ensure that its User Systems detect all Anomalous Events; and** **(b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.**
What the CIO may take into consideration:	• What steps does your User ISMS specify you follow upon the detection of an Anomalous Event? • How do you ensure these steps are followed and enforced? • How does this relate to your incident management processes?
What evidence the CIO might expect to see:	• The inclusion of Anomalous Event management within the User ISMS. • Evidence of testing the detection of Anomalous Event capability. • Evidence of the live operation of the Anomalous Event detection capability, including the completion of the steps set out in the User ISMS.

Privacy Controls Framework

SEC Obligation I1.2 (Reproduced partially)	**Each User undertakes that it will not request, in respect of a Smart Metering System, a Communication Service or Local Command Service that will result in it obtaining Consumption Data, unless:** **(a) the User has the Appropriate Permission in respect of that Smart Metering System; and** **(b) the User has […] notified the Energy Consumer in writing of:** **(i) the time periods […]; (ii) the purposes for which that Consumption Data is, or may be, used by the User; and (iii) the Energy Consumer's right to object or withdraw consent […]**
What the CIO may take into consideration:	• What procedures and controls are in place to capture consent and opt out preferences from Energy Consumers? Do these apply across all mediums used to initiate collection of energy consumption data? • Is consent gathered prior to accessing, or issuing each request to access energy consumption data?
What evidence the CIO might expect to see:	• Documented procedures to obtain a clear an indication of Energy Consumers' explicit consent to the collection and processing of energy consumption data. • Ability to provide evidence that consent has been gathered prior to, or at the point of collection of energy consumption data from Energy Consumers.

Privacy Controls Framework

SEC Obligation I1.5	**Each User shall put in place and maintain arrangements designed in accordance with Good Industry Practice to ensure that each person from whom it has obtained consent pursuant to Section I1.2 to I1.4 is the Energy Consumer.**
What the CIO may take into consideration:	• What do you consider to be good practice and how have you made this assessment? • What procedures are in place to verify that the individual that has provided consent is the energy consumer? If yes, how is this achieved? • Do these procedures apply across all mediums through which consent is collected form Energy Consumers? • How do you keep this approach under review?
What evidence the CIO might expect to see:	• Documented procedures to confirm the identity of the person from whom consent has been obtained for the processing of energy consumption data. • Implementation of these procedures/consent verification mechanisms across all mediums used to initiate collection of smart metering data from consumers - for instance, online, telephone, mobile applications. • Documented procedures in the event of a change of energy consumer at a premises at which consumption data is collected.

SUMMARY

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.

User CIO Engagement Sessions – March 2018

- SECAS and the User CIO will again be holding one-on-one Engagement Sessions for all Users interested in asking questions about their Security Assessment.
- This will allow SEC Parties to raise specific concerns or questions directly with SECAS and the User CIO. Each session can involve up to 3 representatives from each Party, and the sessions can be held in person or via teleconference.
- Dates available are:
  - **Tuesday 20th March 2018**
  - **Tuesday 27th March 2018**
  - **Thursday 12th April 2018**
- Bookings are now open for all engagement sessions, on a first come first served basis. If you are interested please email the SECAS helpdesk (secas@gemserv.com) your preferred date, and we will come back to you with more information shortly.

The User Entry Process (UEP)

Nick Blake, Small Supplier Party Support Analyst

Introduction

The SEC establishes **pre-conditions** to be eligible to become a DCC User – the **User Entry Process.**

What are you required to do?

SEC Section H1.10 sets out the requirements on SEC Parties for the User Entry Process, and in a nutshell…

UEP in a nutshell

User Entry Process Tests (UEPT)

In accordance with the Common Test Scenarios (CTS)

User ID

Obtained from Panel via SECAS

EUI-64 Compliant

Notified to DCC

User Security Assessment

Carried out by the User Independent Security Assurance Service Provider – the CIO procured by Panel

Section G3-6 requirements

SMKI & Repository Entry Process Tests (SREPT)

In accordance with the SR Test Scenarios

Credit Cover

If applicable, lodged with DCC

Privacy Audit

Carried out by the Independent Privacy Auditor – the CIO procured by the Panel

Section I2 requirements

User ID – SEC Panel

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 they wish to operate in.

User ID Checklist

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

Credit Cover - DCC

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 (SREPT) - DCC

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) - DCC

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 – SEC Panel

Security Assessments: SEC Sections G3 – G6
Privacy Assessments: 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.

- Note: If the assurance status is set to 'Approved subject to steps', those steps MUST be completed prior to going live in the DCC Systems. This is evidenced through a Director's letter.

Checklist

- ✓ Has completed the Initial Full User Security Assessment with an Assurance Status of 'Approved' or 'Approved subject to…'
- ✓ Has completed the Full Privacy Assessment with an Assurance Status of 'Approved' or 'Approved subject to…' or 'provisionally approved subject to…'

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) *Note: RDPs are not a DCC User Role*	**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)

**Note: Licensees have privacy conditions in their licences. However, if you also operate in the role of 'Other User' the SEC privacy audit arrangements apply*

UEP Evidence Form

Link to form

SEC
Smart Energy Code

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	☐
Export Supplier	☐
Gas Supplier	☐
Electricity Distributor	☐
Gas Transporter	☐
Registered Supplier Agent	☐
Other User	☐

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.

SEC
Smart Energy Code

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

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.

SEC User Entry - Guidance

SEC Guides and other useful materials are currently available on the SEC Website at the below hyperlinks:

[User Entry Process Guidance and UEP Evidence Form]

[SEC UEP Checklist for Small Suppliers]

[Small Supplier Security Assessment Guidance]

Becoming a Live DCC User

Mike Gibson

SEC Panel
Small Supplier Representative

What I'm going to cover

1. 'Qualified Status'
2. End to End testing
3. Nominated Contacts
4. SMKI RAPP
5. SMKI Gateway Connection Forms
6. DCCKI RAPP
7. DUIS/SSI/DCCKI Gateway Connection Forms
8. Threshold Anomaly Detection
9. Technical Live Test
10. SECAS Approval

To meet the DCC User Mandate, the following steps should already have been completed:

- SMKI and Repository Entry Process Testing (SREPT);
- User Entry Process Testing (UEPT); and
- User Independent Security Assurance Service Provider (CIO) Audit (Full User Security Assessment - FUSA).

The Security Sub-Committee (SSC) will review the Management response following the FUSA, this review must result in a “Approved” or “Approved subject to...” rating.

Once this has been confirmed, an H1.10 form must be submitted to SECAS.
SECAS will then review this and set User status to Live User (although you are not really ‘Live’ at this point!).

These steps mean you are ‘Qualified’ (as per the DCC User mandate requirement), but there are now another series of steps you need to take in order to actually go ‘Live’. Until then you are unable to communicate with any SMETS2 meters gained from another Supplier, and are unable to install any.

The following slides cover some of the activities that are required in order to achieve this.

NB The following steps can currently take anything upwards of 3 months to complete.

Why is this needed?

In achieving Qualified status, you have potentially not undertaken any End to End testing. Although this is not mandated by the SEC, it is advisable that a degree of End to End testing is undertaken before you go live.

When does this need to be done?

- Any time after you have completed UEPT.

How is this completed?

- End to End testing can be undertaken in one of the DCC test labs, or in your own or a 3rd party 'Remote Test Lab'.
- You will need to work with the DCC, your User System Shared Resource provider and any other third parties such as CRM/billing providers, Meter Operators, Meter Manufacturers on your approach and timescales for End-to-End testing.

Why is this needed?

Some of your Users (including your User System Shared Resource provider if using one) will need to be able to access the DCC SharePoint site. You are likely to have set some up for Test, but you need to confirm access for Live.

Here is a sample of some folders users will need access to:

- Incident Contact
- DCCKI Contact
- Quarterly Forecasts
- Major Incident
- Gateway Connections
- Testing Services
- Operational Reports

When does this need to be done?

Prior to going live in order to submit Forecasts and Threshold Anomaly Detection Procedures (TADP) values.

How is this completed?

Users must complete the Nominated Contacts form, and this must be emailed to the DCC Service Desk by either the Lead Contact or a Backup Contact

Why is this needed?
This notifies to the DCC who will be your Nominated Officer (NO), Senior Responsible Officer (SRO) and Authorised Responsible Officer (ARO) for LIVE. Again, you will have done this for test, but you need to separately confirm the people undertaking these roles in Live. There are a number of SMKI Registration Authority Policies & Procedures (RAPP) forms that must be completed.

Once DCC have processed SMKI RAPP forms, the ARO (usually your Shared Resource provider) will collect IKI credentials which are used to generate further Certificate Signing Requests (CSRs).

When does this need to be done?
Anytime after SREPT & UEPT is complete.

N.B. DCC will only process these once H1.10 has been accepted by SECAS. There is then a lead time for DCC to review and approve the forms. It is recommended that you start this process as soon as possible in order to prevent any delays to Go Live. Most subsequent steps are dependent on completion of the SMKI and DCCKI RAPP.

How is this completed?
Once all forms are complete they must be uploaded to the SMKI folder on SharePoint and the DCC Service Desk must be informed.

Why is this needed?

DCCKI RAPP process results in receiving Live DCCKI Authorised Subscriber status. Thereafter, DCCKI certificate can be produced and DCCKI Admin Users can be appointed.

When does this need to be done?

After the Live SMKI RAPP process is complete and SMKI Authorised Subscriber status approved.

How is this completed?

Once all forms are complete they must be uploaded to the DCCKI folder on SharePoint and the DCC Service Desk must be informed.

Why is this needed?

SMKI Gateway Forms are required to open the Live connection between the DCC and the User System.

DUIS Gateway Connection Forms must be submitted to allow the User System to send DUIS Service Requests to the DCC.

Self Service Interface (SSI) gateway connection forms allow access to SSI.

DCCKI gateway connection forms allow access to the DCCKI repository.

When does this need to be done?

Once the Live SMKI RAPP has been confirmed as completed. Although your Shared Resource provider is likely to be completing the SMKI Gateway Connection form, they cannot do this until the Live SMKI RAPP and Live DCCKI RAPP are complete (which is a dependency on you – see previous slides).

How is this completed?

Once all forms are complete they must be uploaded to the Gateway folder on SharePoint and the DCC Service Desk must be informed.

Why is this needed?

Service Request forecasts and Threshold Anomaly Detection forecasts must be submitted prior to go live. Threshold Anomalies are to detect and prevent anomalous events. This will ensure DCC and the User System can implement warning and quarantine checking. SR forecasts are for DCC planning and finance purposes. These are also monitored via monthly report to SEC Panel, for actuals being within 10% of forecast.

When does this need to be done?

Prior to go live.

How is this completed?

Threshold Anomaly Detection Procedures (TADP) values must be created in the defined DCC format, signed with the ARO key and uploaded to the DCC SharePoint site.
SR forecasts must also comply with the defined DCC format and must be submitted via Sharepoint.

Why is this needed?

Just prior to Go Live a simple check can be performed to ensure the connectivity between DCC and the User System is working as expected. Typically your User System will send a ‘Read WAN Matrix’ service request in order to prove this connectivity.

When does this need to be done?

Before go live.

Pre-requisites

Gateway Connection (DUIS) configured by DCC/DSP.
Service Request forecast submitted.
Threshold Anomaly Detection Forecast processed by DCC.

Why is this needed?

The second stage of SSC authorisation is, following completion of all required remediations, to submit a Directors Letter (confirming all actions complete).

This is reviewed by SECAS and the SSC. If SSC accept Directors Letter in full, SECAS will approve final Go Live

When does this need to be done?

Prior to Go Live.

Having completed all of the above, you can start using the live DCC services to gain and install SMETS2 meters!

Data Communications Company

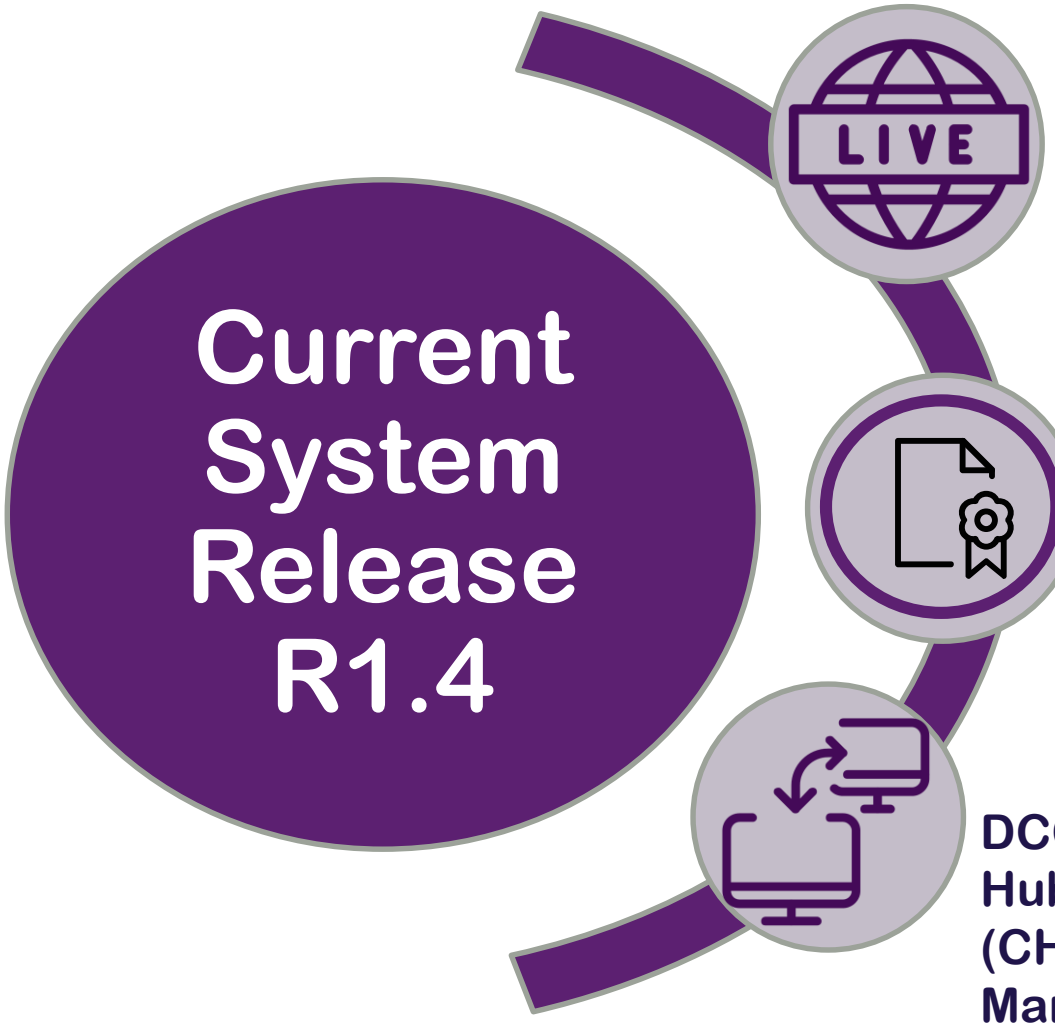
DCC Programme and Business Update

Verity Thenard
Industry Partnership Manager
08 March 2018

Agenda

1. DCC Business and Programme Update
   - Operational Update
   - Release 2.0
   - SMETS1
2. Upcoming Events and getting in touch

Operational Update



Current Comms Hub FW:

- S&C: Toshiba - 11.24
- S&C: WNC - 2.13 & 2.16
- North: EDMI - 1.37.7

Re-test of DSP Business Continuity Disaster Recovery (BCDR) on 3rd/4th Feb was successful at <4hrs.

DCC is providing Comms Hub Antenna Stimulators (CHAS) to support device Manufactures' noise testing.

Release 2

Background and Scope:

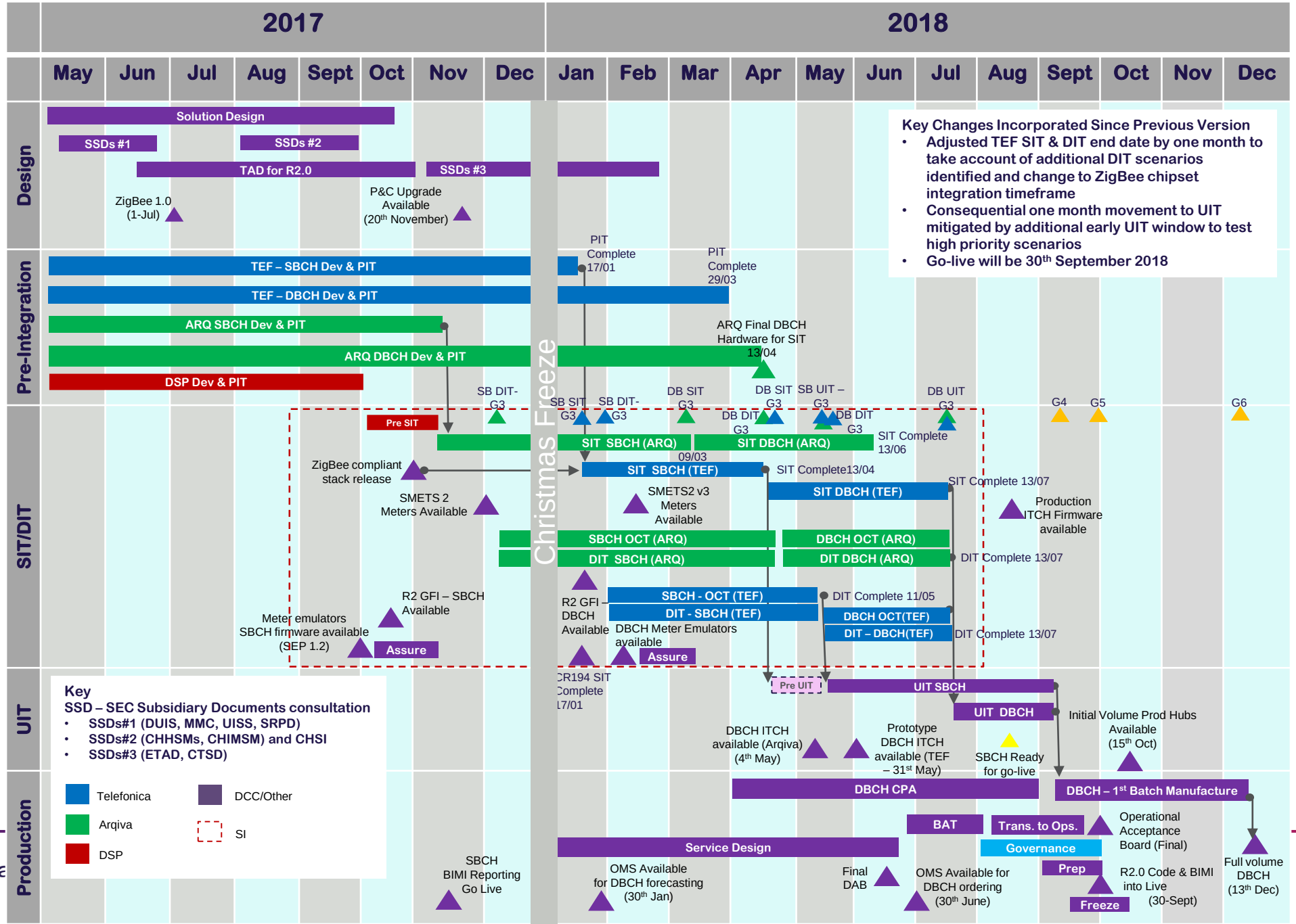
- The HAN frequency (2.4GHz) used by Single Band Comms Hubs (SBCH's) works in around 70% of premises – the rest require another solution.
- R2.0 introduces Dual Band CH (DBCH's), using HAN frequencies of 868MHz & 2.4GHz – to reach other area's and therefore better coverage.
- Part of the SMETS2 Programme – a significant step to enable the installation of Smart Metering Systems for an increased proportion of Great Britain homes.
- Changes to the DCC test (UIT) and production systems to support DBCH as well as making DBCH available to customers.
- This includes – 8 New Service Requests, 13 updated service requests, 6 new DCC Alerts and 3 new response codes.

Release 2.0

Release 2.0 Update	Status*
Programme Status:	Overall RAG Status Amber
Next Milestones	ZigBee Certification Complete - 28/03/18 DIT DBCH commence - 16/04/18
UIT Available	UIT SBCH Commences - 21/05/2018 UIT DBCH Commence - 19/07/2018
DBCH Available	Initial volumes available from 13 October 2018 full volumes available form 13 December 2018.
Go Live	Go live on 30 September 2018.

*Status – at time of issue, on 2 March 2018.

R2.0 Plan on a Page Version 3.6 (NON Contingent)



Data Communica Company

SMETS1: Programme Objectives

Primary Objective:

The overall aim for the SMETS1 Service is to ensure interoperability for SMETS1 meters, so that smart functionality is retained when a customer switches supplier.

Underlying objectives:

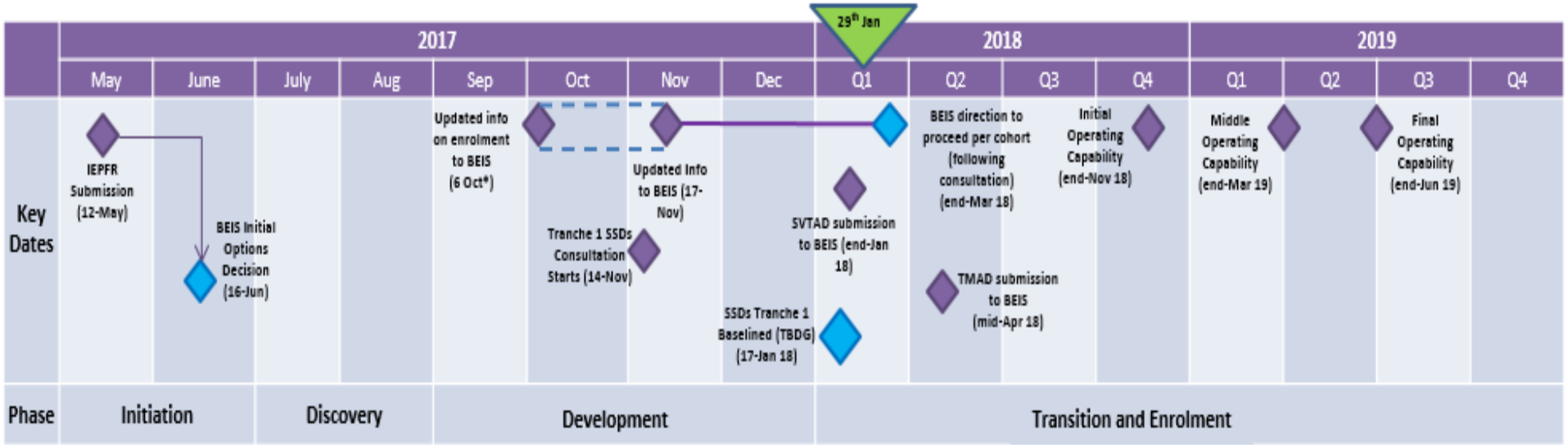
1. To make interoperability and smart benefits available quickly and reliably for all stakeholders;
2. To do so in a cost-effective manner, taking account of the impact on businesses and consumers; and
3. To ensure an acceptable level of security for the Smart Metering System, prioritising high impact risk mitigations from the outset.

To help deliver the best solution, to date we have carried out over 50 industry engagements delivered and supported 4 public consultations.

SMETS1 Key Milestones

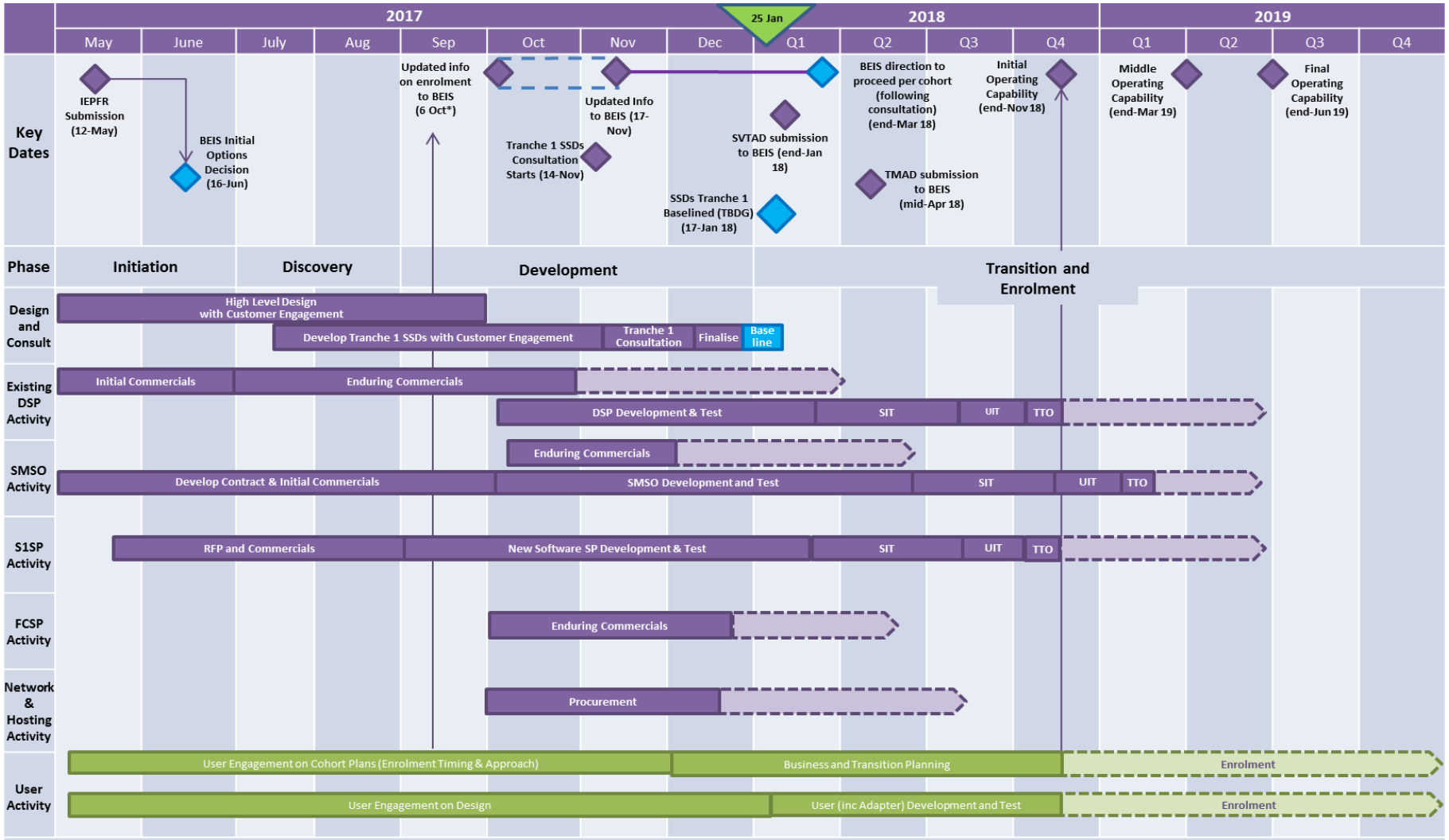
DCC are now in the build phase of the SMETS1 Programme, the next key decision will be on the Integration Path (IP), which is now pending.

The milestone haves are underpinned by a set of risks, assumptions and dependencies., which have been formed primarily through the Initial Enrolment Project Feasibility Report (IFPER) and subsequent Industry and Stakeholder engagement.



*Status – at time of issue, on 2 March 2018.

SMETS1 LC13 POAP



KEY

- DCC Activity
- BEIS Activity
- User Activity
- DCC LC13 Milestones
- Proposed BEIS Decision Milestones
- Activity Duration TBD

NOTES

- This plan is not stand alone and is to be read in conjunction with the Consultation on DCC's delivery plan for SMETS1 Services.
- The available information was provided to BEIS on 24 August 2017, and formal sign-off on 6 October 2017.
- All contingency has been removed from this plan to provide a pure delivery timescale on key elements.
- The delivery plan will continue to be subject to regular reviews of SMETS1/R2.0 programmes; may be revised as a result of a direction from BEIS.
- Timescales in relation to testing assume readiness for IOC Nov 18.
- Enrolment of cohorts at MOC and FOC will be subject to additional testing phases, with exact dates TBC.

Upcoming Events

DCC Operations Customer Forum (previous COBI)
8 March 2018
This is a regular meeting for DCC, our customers and other industry parties to discuss key aspects of Service Management. The forum focusses on how our customers interact with the DCC solution.

DCC Design Release Forum
14 March 2018
This monthly forum focuses on DCC User-facing System Design. The typical agenda focuses on discussion and points of clarification on completed design, but also sharing information on forthcoming design changes

DCC Comms Hub & SM-WAN Design Forum
28 March 2018
The "Comms Hub & SM-WAN" forum is for DCC, Energy Suppliers, SEC Parties, and Device Manufacturers to discuss CH & SM-WAN issues and developments according to the priorities of the attendees.

Comms Hub Train the Trainer (CH TTT) Courses
Dates TBC
Upcoming training sessions to be released and communicated by DCC's Service Desk.

How to engage and get support

Speak to your Industry Partnership Manager

- Or alternatively email contact@smartdcc.co.uk

Industry Test Team

- Available to support you through testing Testing.Notices@smartdcc.co.uk or E2ETestingNotices@smartdcc.co.uk

DCC Service Desk

- For live services ServiceDesk@smartdcc.co.uk

DCC Website and DCC SharePoint

- Contact Service Desk for access to SharePoint

DCC monthly newsletter

- Sign up here!

DCC CHARGING STATEMENT

In accordance with the Charging Methodology the Charging Statement sets out the Charges applicable for each regulatory year additionally an explanation of these charges is also given.

THANK YOU

Any questions? Please email contact@smartdcc.co.uk

Smart Metering - Alternative Home Area Network Update

Spotlight on the SEC

8th March 2018

Colin Sausman

Chair, Alt HAN Forum

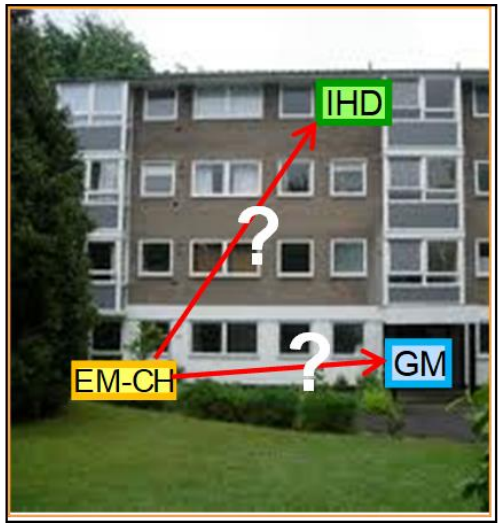
Agenda

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

What is Alternative HAN?

1. A service to Suppliers that solves a problem:

- “Missing piece of the jig-saw”, where:
- Meter + DCC services ≠ 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



What is Alternative HAN?

1. A “regulated co-operative” of Suppliers

- Empowered by the SEC to make commercial decisions
- Underpinned by licence obligations on Suppliers
- Costs recovered via DCC charges
- Alt HAN Forum as decision-maker
- Alt HAN Company as contracting vehicle

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

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. Vendor engagement – positive
4. Issued ITT – requested coverage of all use cases
5. Now closed – a number of tenders received
6. Decision pending on moving into Stage 2A

Key Developments

Data Pilot

1. Sample of 6 data areas
2. To “prove concept” of a data-driven propensity model and proactive approach to Alt HAN premise identification
3. Building survey work and data analysis ongoing
4. Input from individual suppliers and other industry parties
5. Findings being reviewed currently

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. Further Supplier engagement will be invited in 2018
4. Consultation planned for Q4 2018
5. Accession Q1 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. Supplier engagement points coming up in 2018.

Key upcoming Planning Milestones

From Alt HAN Forum High-Level Plan

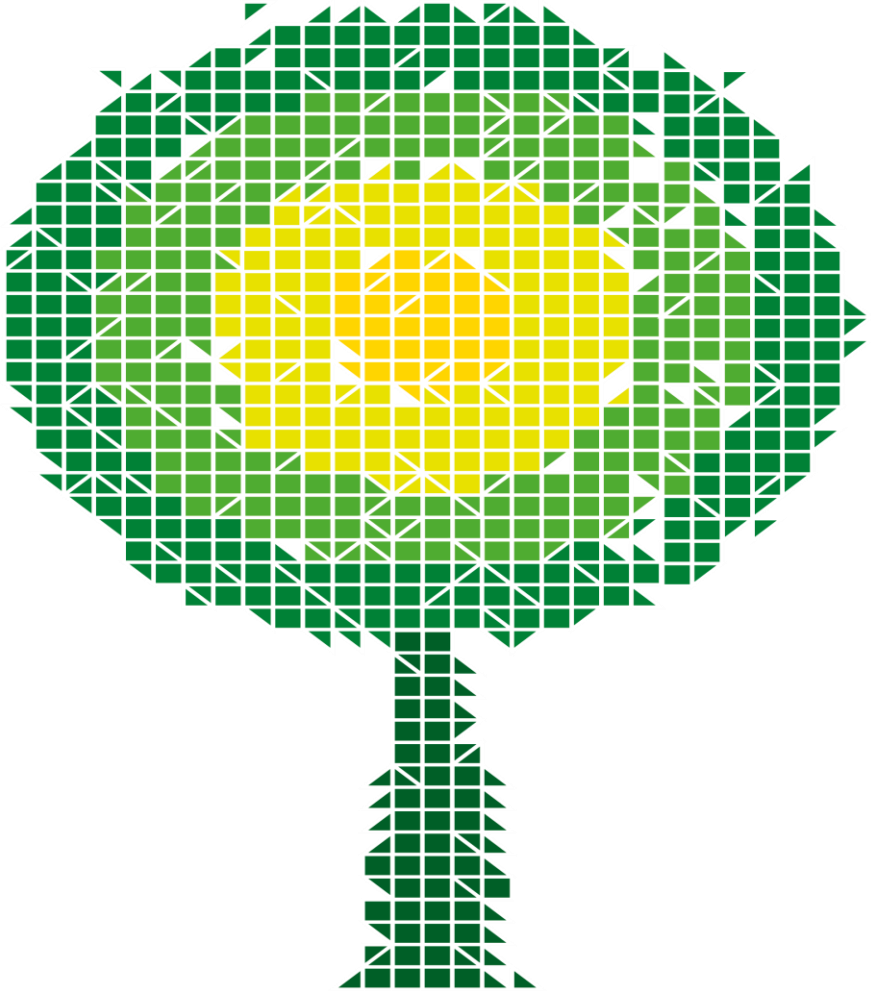
1. Decision to take forward vendor(s) to Detailed Design: **Apr 2018**
2. Operational Services requirements set: **Feb 2018**
3. Operational Services RFP issued: **Apr 2018**
4. Phased move to Programme Structure: **Q1-Q2 2018**
5. Alt HAN Co/Supplier Contract Accession: **Q1 2019**
6. Alt HAN services “safe launch”: **Q2 2019**
7. Exempt Premises List Approval: **Q2 2019**

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

althan@gemserv.com or 0207 090 7766.

SEC Governance Update

Courtney O'Connor,
Operations and Party Support Consultant, SECAS



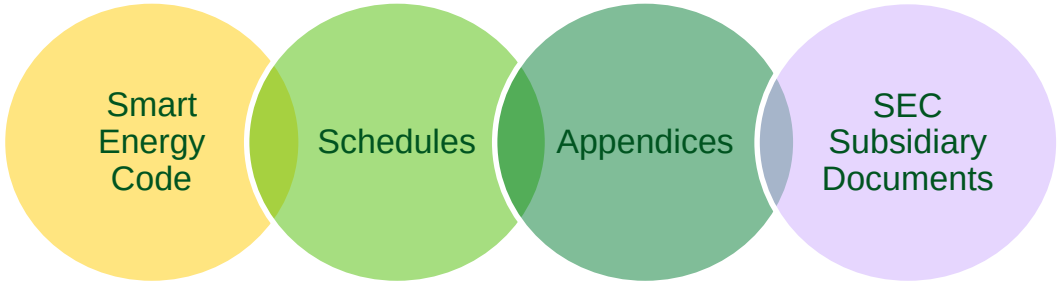
Smart Energy Code Administrator And Secretariat (SECAS)

- 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, and 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

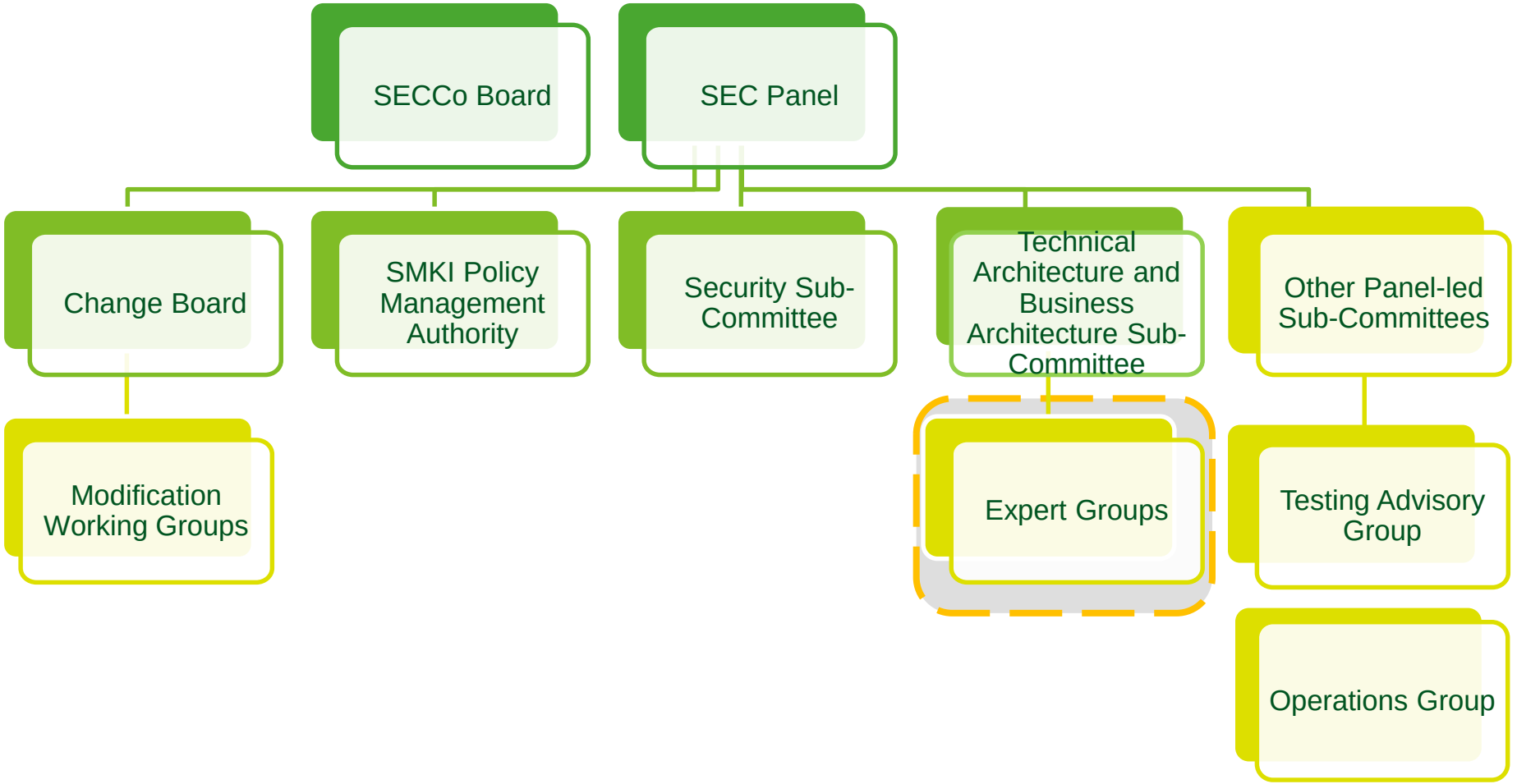
The Smart Energy Code (SEC)

A multi-Party agreement:

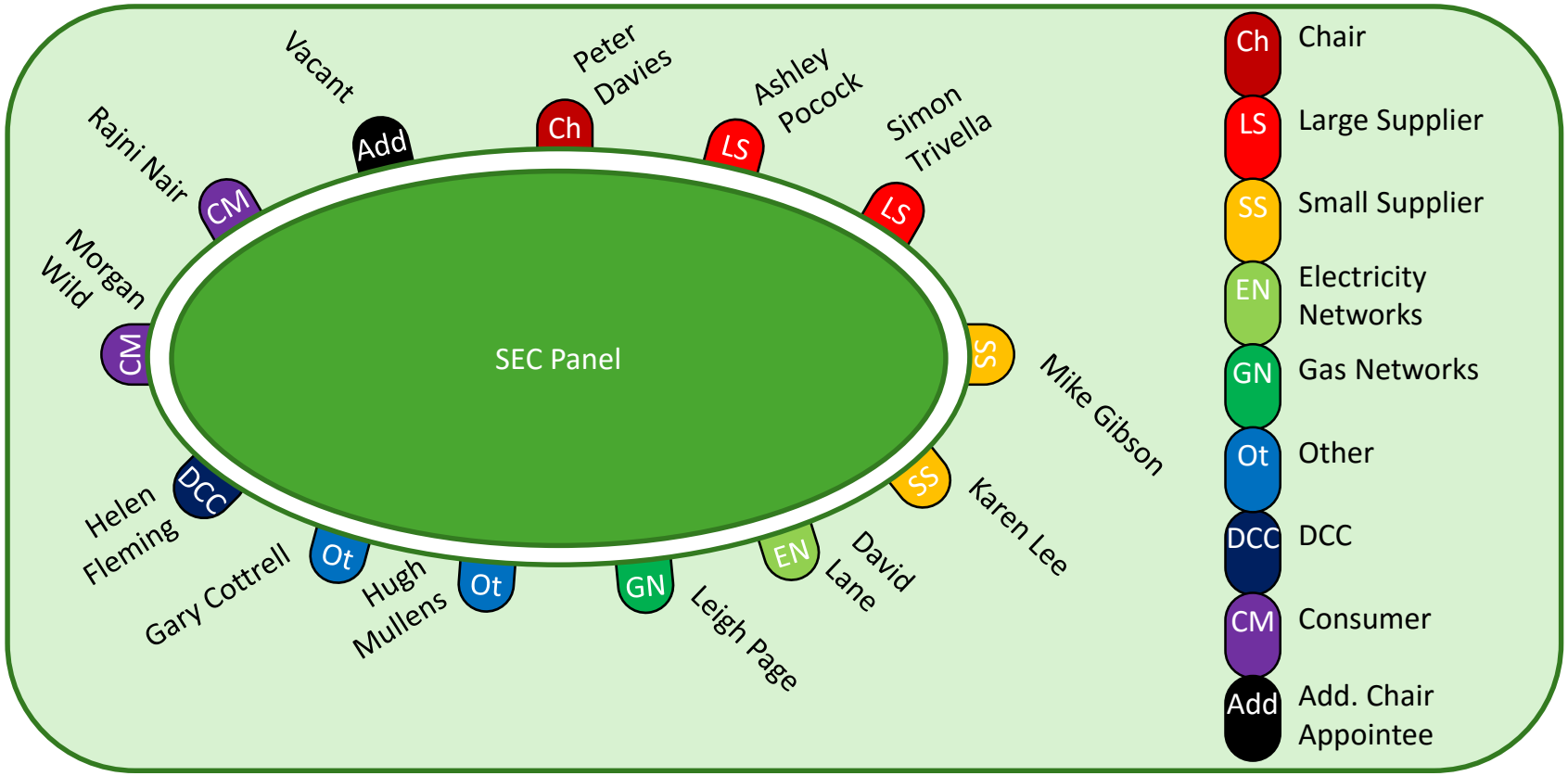
- DCC licence obligation for the SEC
- Defines the rights and obligations between the DCC and the Users of the DCC Services
- Specifies other provisions that govern the end-to-end management of Smart Metering in GB



SEC Governance Structure



SEC Panel


SEC Panel
Vacant
Add
Peter Davies
Ch
Ashley Pocock
LS
Simon Trivella
LS
Mike Gibson
SS
Karen Lee
SS
David Lane
EN
Leigh Page
GN
Hugh Mullens
Ot
Gary Cottrell
Ot
Helen Fleming
DCC
Morgan Wild
CM
Rajni Nair
CM
Ch Chair
LS Large Supplier
SS Small Supplier
EN Electricity Networks
GN Gas Networks
Ot Other
DCC DCC
CM Consumer
Add Add. Chair Appointee

SEC Panel and SECCo Board

Panel — Pursue the Panel Objectives and Panel Duties using the powers set out in the SEC (SEC Section C2)

- 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 — Act as the corporate vehicle to support Panel business

- 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

Current Priorities

- At the February 2018 Panel meeting, the Panel approved the Draft Budget for the next three Regulatory Years. The Draft Budget has now been published on the SEC Website, and will remain the Draft Budget until 8th March 2018, after which it will become the Approved Budget 2018-2021 to become effective on 1st April 2018.
- The SEC Panel Release Management Policy has been approved for use, following updates to the documents as a result of the responses received to the Release Management Policy consultation.

SMKI PMA

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

Duties

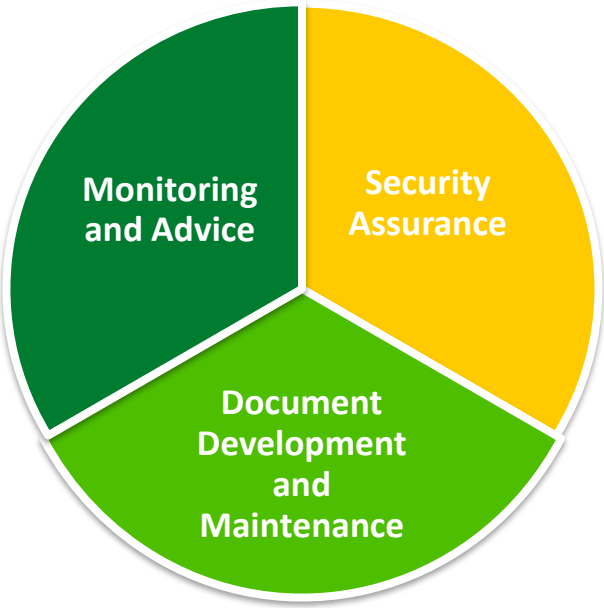
- Approve Assurance Scheme and Service Provider
- **Contribute** to Design Activities
- Review and Approve SMKI Documentation
- Produce guidance documents e.g. Recovery Key Guidance
- Monitor testing reports in relation to SMKI
- Review and Approve DCCKI Documentation

Current Priorities

- The DCC have expressed their concerns about the current number of key Custodians. The DCC plan to contact the SMKI PMA chair in regards to call for nominations. The DCC does not believe this is an immediate concern, but could become an issue if replacements can't be found.

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



Current Priorities

- The SSC has been liaising with the organisation that won the bid to complete the end to end Security Risk Assessment. The SSC has provided their views on the proposed approach. The scope and assumptions for the Risk Assessment will be discussed at the Risk Assessment Workshop on the 13th March.

Technical Architecture and Business Architecture Sub-Committee

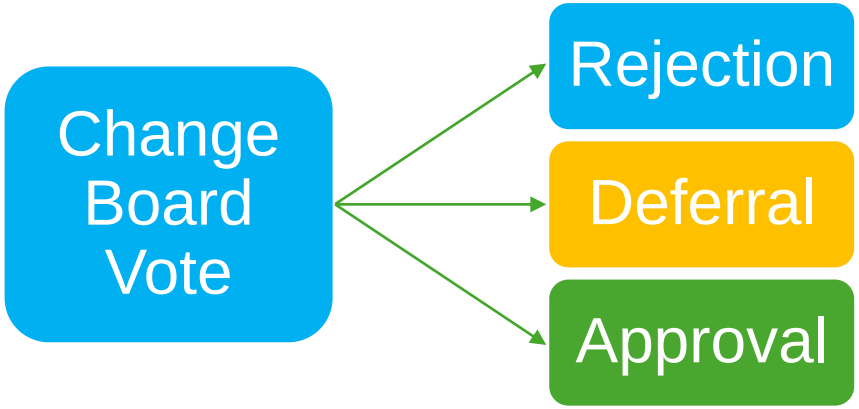
Sub-Committee	Function	Membership
Technical Architecture and Business Architecture Sub-Committee (TABASC)	Provides support & advice on the Technical Specifications and end-to-end Technical Architecture	8 Suppliers (6 Large and 2 Small), 2 Networks (1 Gas and 1 Electricity), 2 Other Parties, DCC, an independent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

Current Priorities

- Draft changes of the Business Architecture Document and Technical Architecture Document for Release 2.0 content to be issued to the TABASC, the TBEC and other interested SEC Parties for review in March 2018 (at least 20 Working Days)
- Issuing the Effectiveness Review Survey to SEC Parties and Users at the end of April 2018.

Change Board

Sub-Committee	Function	Membership
Change Board	Review the Modification Report Consultation responses and vote on whether to Accept/Reject or defer a Modification Proposal	Large Suppliers from Voting Group of that Category, 3 Small Suppliers, 3 Other, 3 Networks, Consumer, DCC, Ofgem, SoS and SECAS Chair



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 and has weekly calls with the DCC to understand testing progress.	1 person appointed by Large Supplier, 3 persons from the Small Suppliers, 3 Persons from the Electricity and Gas Networks, 3 persons from the Other SEC Parties, 1 Consumer member

Current Priorities

- Reviewing each phased Testing Approach Document for Release 2.0 and SMETS1 to inform Panel recommendations to BEIS on the associated entry and exit criteria.

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 person appointed by Large Supplier, 3 persons from the Small Suppliers, 3 Persons from the Electricity and Gas Networks, 3 persons from the Other SEC Parties, 2 persons appointed by the DCC, TABASC representative, Authority and SoS representative

Current Priorities

- Gaining an insight into the DCC Ready to Scale work and costing within the DCC Budget.
- Reviewing DCC reporting and its operational relevance.
- Reviewing the DCC's business continuity and disaster recovery tests.

Keeping Parties Updated

- All non-confidential meeting documentation provided on the SEC Website
- Meeting Headlines provided one Working Day after each meeting
- Transitional Governance Update provided to the Panel each month
- Monthly newsletter – [sign up on the SEC website]

SEC Version 5.13

SEC 5.13 came into effect on the 1st February 2018

BEIS concluded on a consultation on the renaming of SMETS documents, the incorporation of various schedules and subsidiary documents and related transitional variations to the SEC

Changes to the Smart Metering Equipment Technical Specifications (SMETS) naming conventions;

Introducing additional SEC Schedules in order that SEC Party Modification Proposals can be raised against them for implementation in future SEC Releases.

Introducing a suite of new Schedules and Subsidiary Documents to the SEC in advance of Release 2.0, in order support the introduction of Dual Band Communication Hubs. Related Transitional Variations* are also being introduced to support the early introduction of Release 2.0 documents;

SEC Version 5.14

SEC Version 5.14 came into effect on 22nd February 2018. The Secretary of State has directed changes to SEC Section A and designated a new SEC Appendix AJ.

The changes to Section A introduce a new Section A4 to cover the provisions for derogations from the SMETS1 General Installation End Date. Derogations may be granted to Suppliers by the Secretary of State. Consequential amendments to other parts of Section A have also been made in response to this.

The new SEC Appendix AJ 'SEC Variation Testing Approach Document' has been produced to explain how testing will be conducted by DCC as directed for Release 2.0.

SMETS1 and AME end dates

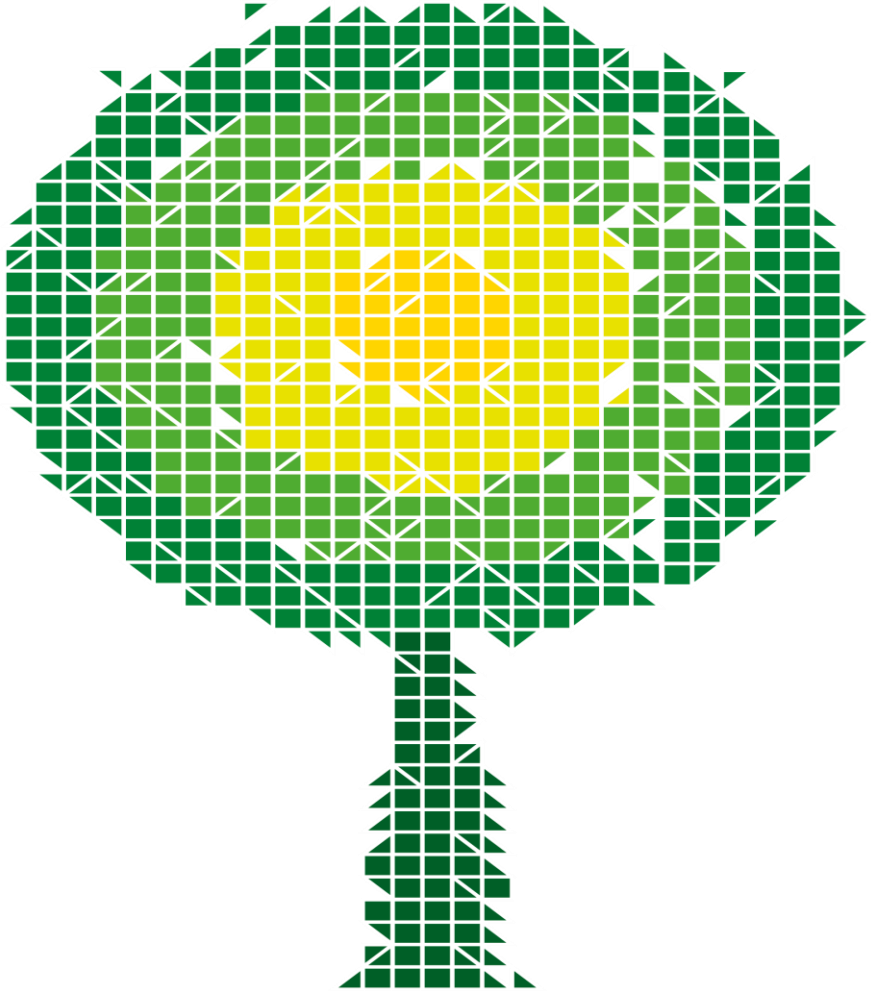
- On the 18th January 2018, the Smart Metering Implementation Programme (SMIP) Senior Responsible Officer (SRO) announced their decision in regards to the SMETS1 and Advanced Meter Exception (AME) end dates.
- The SMETS1 end-date will now be **Friday 5th October 2018**. It is expected that all SMETS1 capable meters will be made compliant by this date.
- The AME end-date will now also be **Friday 5th October 2018.**
- SEC Section A4 has been introduced to cover the provisions for derogations from the SMETS1 General Installation End Date. Derogations may be granted to Suppliers by the Secretary of State.

Non-Domestic Mandate

- While we can't pre-empt the outcome of the consultation, it is reasonable to expect that most non-domestic suppliers will be required to become DCC Users by 31 August 2018.
- BEIS have advised that, in general, responses to the consultation were also supportive of the policy proposal to exempt I&C suppliers with advanced meters installed at in-scope sites from the DCC User mandate.

TABASC Effectiveness Review

Kayla Reinhart
Operations Senior Analyst, SECAS



Gemserv

The **Who**, **What**, **When**, **Where** and **Why**?

- **Who?**
  - The TABASC is engaging with SEC Parties and Users
- **What?**
  - A survey is being issued to SEC Parties and Users
  - Those with a technical/operational background are encouraged to respond
- **When?**
  - The survey will initially be issued at the end of April 2018
- **Where?**
  - The survey will be accessible via link that will be issued via email and also accessible via the SEC Website
- **Why?**
  - On direction from the SEC Panel, the TABASC is required to review the effectiveness of the Technical Architecture, Business Architecture and the HAN requirements
  - The survey findings will help inform the effectiveness analysis
  - The initial findings will also inform if the survey questions are appropriate to inform enhancements when the survey is reissued or followed up, once installed meter volumes increases

Detailed Supplementary Materials – For Information

- The following slides, provide more detail on the reasons for the Effectiveness Review

Briefing Pack

TABASC Reviews of:

- **The Effectiveness of the End-to-End Technical Architecture;**

- **The Effectiveness of the Business Architecture;**

- **The Effectiveness of the HAN Requirements.**

Background: The SEC Section F1.4 puts obligations on TABASC to undertake three reviews on behalf of the SEC Panel.

SEC F1.4:

"The Technical Architecture and Business Architecture Sub-Committee shall undertake the following duties on behalf of the Panel: ……

(e) to review (where directed to do so by the Panel) the effectiveness of the End-to-End Technical Architecture (including so as to evaluate whether the Technical Code Specifications continue to meet the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate)."

(f) to review (where directed to do so by the Panel) the effectiveness of the Business Architecture (including their assessment against the SEC Objectives), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate);

(g) to review (where directed to do so by the Panel) the effectiveness of the HAN Requirements (including their assessment against the SEC Objectives), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), and report to the Authority and the Panel on the outcome of such review;"

The SEC Panel meeting on 12 August 2016 approved the Panel directions for TABASC to undertake the three reviews described in F1.4 (e), (f) and (g).

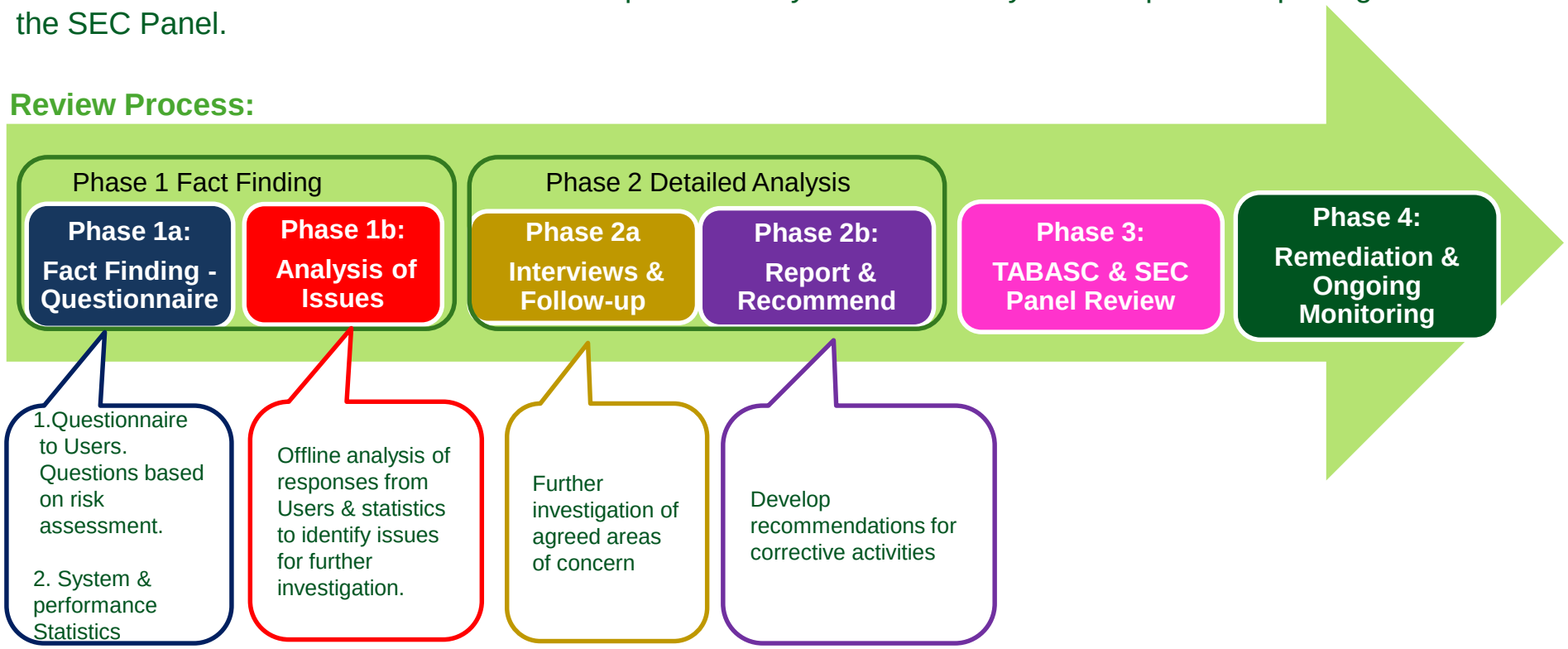
TABASC identified strategic risks to be addressed in the reviews

Review Area	ID	Strategic Risk
Technical Architecture	1	DCC technical solution doesn't work effectively and adversely impacts DCC User rollout
	2	High number of (SMETS2) smart meters require fault resolution following installation
	3	High number of Comms Hubs require fault resolution following installation
	4	Smart Meter device specification problems, inconsistencies and time to market delays cause initial problems
	5	Technical problems prevent Network Operators meeting industry SLAs on receipt of alerts on loss of supply
	6	DCC system performance, availability and reliability affects installation processes and rollout rates
	7	DCC service management function not capable of supporting volume and severity of reported incidents affecting rollout
	8	Technical scalability problems affect installation and rollout rates
	9	Technical interoperability problems require meters to be replaced
	10	DCC change and release processes do not support prompt and agile improvements to functionality to address problems
	11	BCRD processes are inadequate to maintain business operations at scale
Business Architecture	12	DCC User business and operational processes cause problems (e.g. time or resource related) affect installation rates
	13	'Clunky' processes / workarounds cause large numbers of consumer transactions to be conducted 'offline'
	14	Inadequate interoperability prevents a smooth change of supplier process for consumers
	15	Processes affect the consumer experience (e.g. requiring consumer contact for readings, billings, change of circumstances) leading to consumer resistance which affects rollout profiles
	16	Supplier rollout strategies do not adequately support vulnerable and fuel poor consumers during rollout
HAN Requirements	17	HAN performance (e.g. in the absence of non-functional requirements) affects business operations
	18	Difficulties experienced with implementing firmware upgrades remotely affects business operations
	19	Difficulties experienced with the HAN integrating with CADs and other in-home consumer equipment
	20	The performance of 2.4GHz HAN does not meet the 70% assumed deployment capability
	21	868 and Alt HAN delays affect rollout timescales

A Phased Approach to the reviews

The process uses a factfinding phase, which can be iterative, and uses a questionnaire to focus on the areas identified in the risk assessment to identify any areas requiring further investigation. TABASC propose the use of a Survey Monkey questionnaire as an economic, efficient and readily available tool that can be issued by SECAS on behalf of TABASC and can also have the responses analysed in-house by SECAS prior to reporting to TABASC and the SEC Panel.

Review Process:



An Iterative Questionnaire

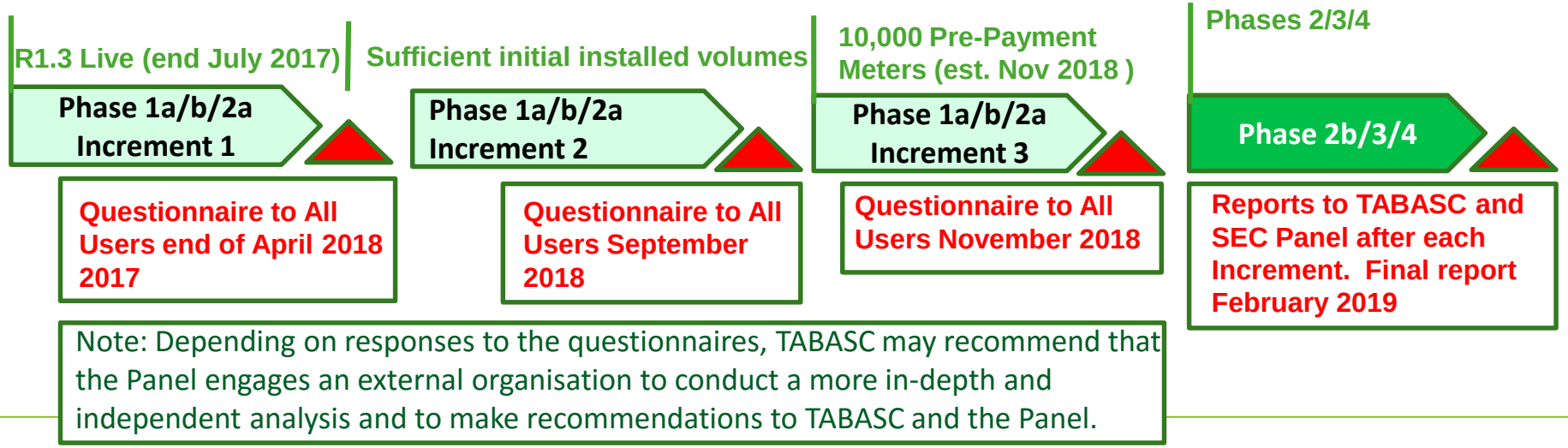
The questionnaire is intended to be proportionate and not too onerous for Users to complete. The questionnaire can be re-issued iteratively (amended as appropriate in the light of experience) at various points in the deployment lifecycle to identify any emerging problems associated with the technical and / or business architecture and / or HAN requirements.

TABASC will consider factors such as the volume of installed devices (including Pre-Payment Meters) when proposing the exact timing for the issue of a questionnaire. Reports and recommendations will be provided to TABASC and the Panel following each incremental questionnaire with a final report planned for January 2019.

TABASC believes there is value in conducting early surveys to identify emerging problems, therefore the survey is being issued at the end of April 2018. Any feedback will inform survey improvements or analysis on problems preventing installations.

TABASC estimates that effective live operations can only be measured when Large Suppliers are operating around 10,000 Pre-Payment Meters, therefore the survey will be reissued once installed volumes increase, subject to any amendments in light of the initial survey period.

Potential Incremental Timetable (to be adjusted by TABASC as appropriate)

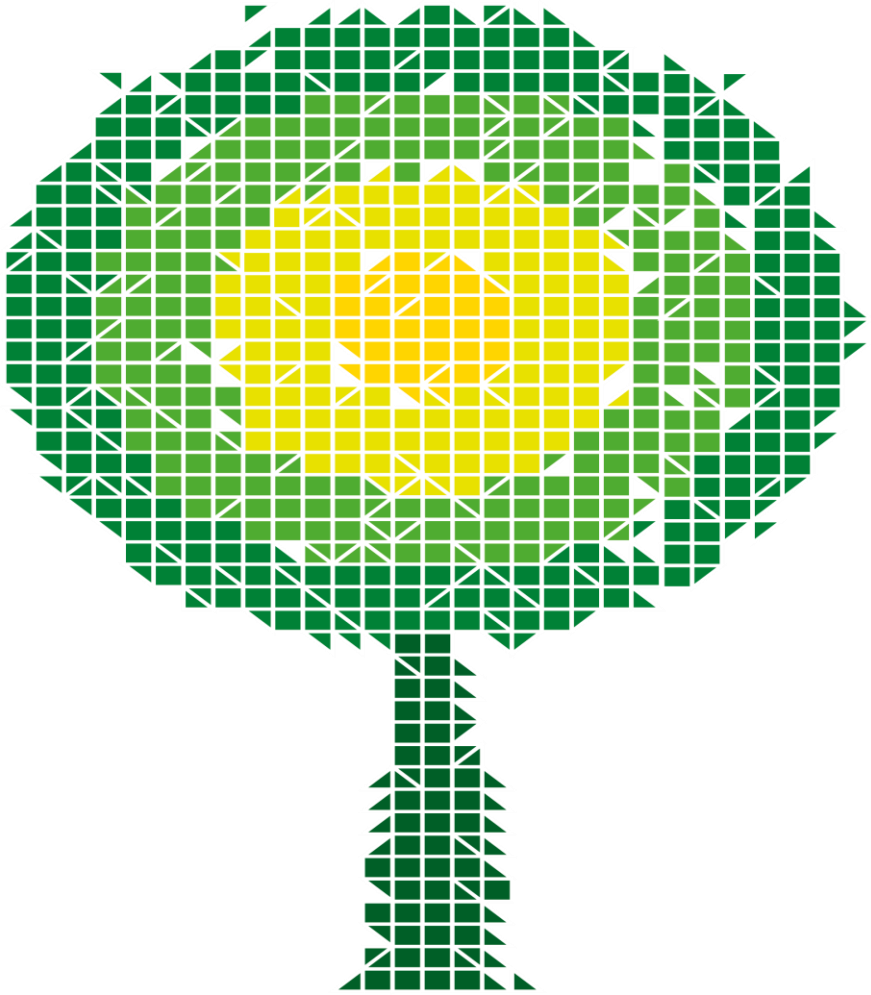


Questionnaire

A copy of the questionnaire will be sent to SEC Parties at the end of April 2018.

Release 2.0

Courtney O’Connor,
Operations Consultant, SECAS



Release 2.0 Fact Sheet

- **When? -** DCC Release 2.0 is expected is September 2018.
- **Why? –** To support new functionality and ensure Secretary of State changes are implemented.
- **What? –** Changes to support DBCH and Technical Specifications changes. Additionally the implementation of SECMP006 -Specifying the number of digits for device display and SECMP008 - Provision of a DCC Alert (formerly Service Request Error Response) for Quarantined Service Requests
- **Progress -** Release 2.0 is making good progress against the current plans in the lower-risk phase of regression testing single functionality.

Time to prepare

- SEC V5.13 introduced a suite of new Schedules and Subsidiary Documents to the SEC in advance of Release 2.0, this will support the introduction of Dual Band Communication Hubs:
  - SMETS2 V3, CHTS V1.2, GCBS V.20, CHHSM V1.2,V1.3, DUIS V2.0 and MMC V2.0.
- This early incorporation into the SEC will facilitate SEC Parties who wish to raise a SEC Party Modification Proposal for a later release, by giving them easy access to the documents for use as a reference.
- DUIS V2.0 and MMC V2.0 have been designated and incorporated into the SEC, but no Party shall be entitled to exercise the rights set out in them, nor obliged to comply with the obligations set out in them.

Testing Approaches for Release 2.0

SEC Designation v5.14 introduced the new SEC Appendix AJ – SEC Variation Testing Approach Document (SVTAD). The purpose is to explain how testing will be conducted by the DCC for Release 2.0.

To successfully test the content of Release 2.0 two Testing Approach Documents have been produced (so far) which set out how the testing will be undertaken (supporting Appendix AJ). They are the:

- Systems Integration Test Approach Document (SIT) and;
- Device Integration Test Approach Document (DIT)

Implementation Managers Forum Identified Potential Risks for Release 2.0

- Unacceptable number of defects present at the point of SIT/DIT exit, if an extension was needed this could lead to delay of R2.0.
  - DCC are going to ensure transparency and will highlight R2.0 impacting issues as they arise.
- A delay of R2.0 would increase the proximity to delivery of the SMETS1 Service.
  - The DCC propose to submit a Change Request to the JIP if necessary
- Sub GHz Meters, Comms Hubs, IHD and PPMIDS, not being available for R2.0 DIT.
  - DCC have contingency planning in place and BEIS have been reassured that they will be available.

Key Release 2.0 Testing dates (via JIP)

System Integration Testing DBCH Commences – 12/3/18

Device Integration Testing for DBCH Commences – 16/4/18

System Integration Testing DBCH Completion – 13/7/18

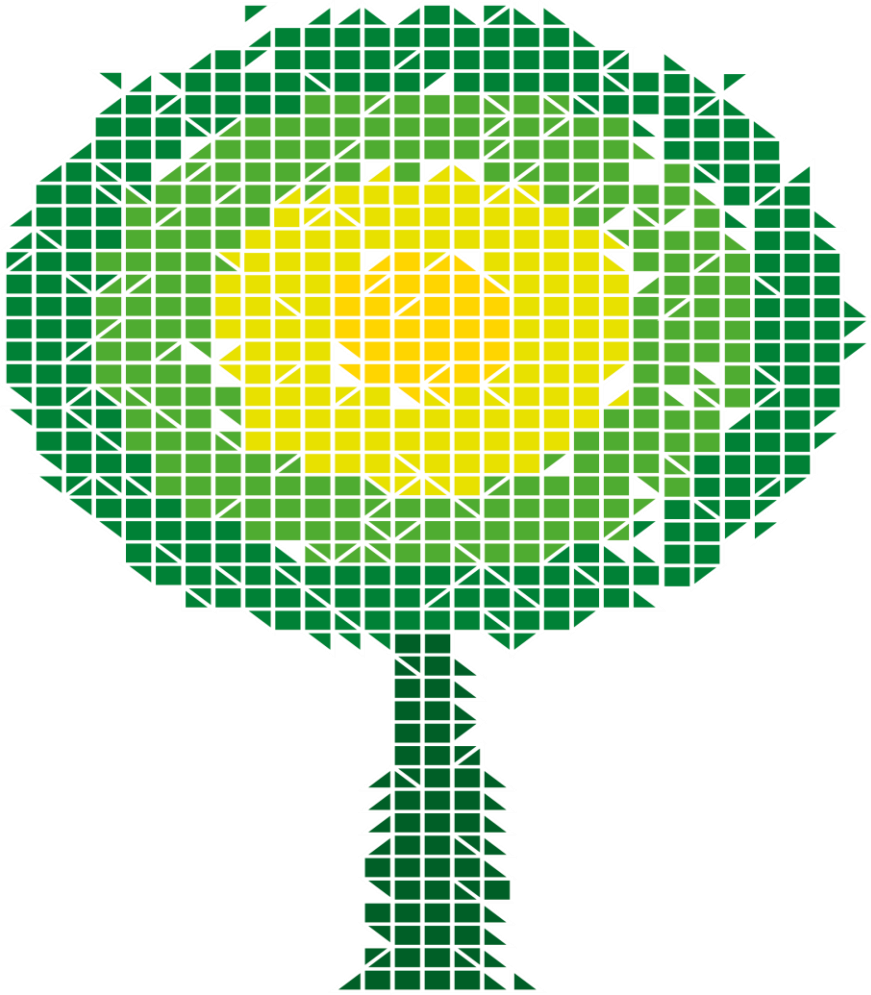
Device Integration Testing Completion – 13/7/18

User Integration Testing DBCH Commences – 19/7/18

User Integration Testing Completion – September 18

Modifications Update

Caroline Gundu, Senior Modifications Analyst



Gemserv

Agenda

- Overview of Modifications process
- Review of Modifications process
- Status of Open Modification Proposals
- Individual updates on four modifications impacting all SEC Parties
- The SEC Modifications Register
- Upcoming Meetings & Consultations
- Where to find more information

Modification Process

- The SEC and SEC Subsidiary Documents can be modified in accordance with the processes set out in SEC Section D.
  - SEC Parties and a number of interested bodies are entitled to raise Modification Proposals
- Guidance is provided to simplify and to clarify provisions in the SEC

1) Modification Proposal Raised

2) Initial Modification Report

3) Refinement Process

4) Modification Report

5) Change Board Vote

6) Authority Decision (Path 1/2 only)

Progression Paths

Path Type		Description
Path 1	Authority-Led	Significant Code Review led by Authority
Path 2	Authority Determination	a) Material effect on Energy Consumers b) Material effect on competition in Supply c) Material effect on: • the environment, • access to or privacy of Data, • security of the Supply of Energy, • security of Smart Metering Systems; d) Changes to arrangements in: • Governance (SEC Section C) • Modification Process (SEC Section D) e) Unduly discriminate between Parties
Path 3	Self Governance	None of the Path 2 Criteria
Path 4	Fast Track	Correct typos / minor inconsistencies

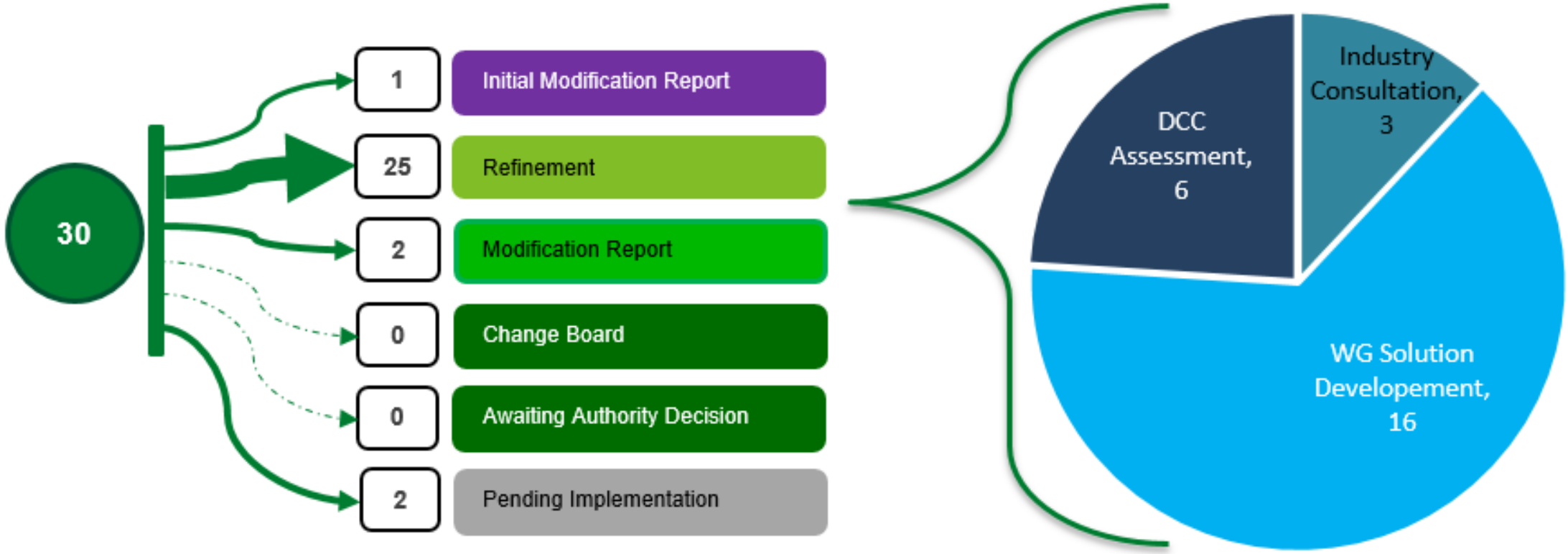
Review of the Modifications Process

- Strengths
  - Good Critical Friend support provided by SECAS
  - A knowledgeable in-house team able to provide technical guidance

- Challenges
  - Lack of quoracy for Working Group Meetings and lack of engagement on consultations
  - Complexity and lack of clarity in the modifications process

- Next steps
  - Section D is currently under view.
  - February 2018 SEC Parties were invited to an engagement workshop
  - An industry consultation will be issued in March 2018

Status of Open Modification Proposals



Overview Modifications impacting all SEC Parties

Modification ID Number	Modification name
SECMP0012	Channel selection to support Shared HAN solutions
SECMP0041	Amending the Change Board decision making rules for Modification Proposals
SECMP0042	Amendment to SMKI Services to provide DCC Users and/or SMKI Participants with Authorised Responsible Officer (ARO) Statistics and Information
SECMP0044	User Security Assessment of a Shared Resource

SECMP0012 - Channel selection to support Shared HAN solutions

- **Summary**
  - Seeks to enable channel selection at the 2.4GHz frequency in the SEC and the associated technical specification documents.
  - This will enable shared HAN infrastructure to be deployed cost effectively and efficiently in high density housing, using standard 2.4GHz equipment.

SECMP0012 - Channel selection to support Shared HAN solutions

- **Impact**
  - This modification seeks to provide greater flexibility at the installation and commissioning process for Smart Metering Systems. If implemented, it is expected to have a positive impact large suppliers, small suppliers and other SEC Parties, and the DCC.
  - Modest amendments to the SEC, The Great Britain Companion Specification (GBCS), The Communication Hub Technical Specifications (CHTS) and The DCC User Interface Specification (DUIS).

SECMP0012 - Channel selection to support Shared HAN solutions

- **Progress Update**
  - The PA and technical options will be discussed at the next Working Group (WG).
  - SECAS sought a perspective from the Alt HAN Forum, to identify if there is a crossover between this modification and some of the technical solutions coming out through tenders.
  - It was advised that the solution proposed provides a network plan for Alt HAN and noted that the Alt HAN Forum would be interested in how this solution would develop.
  - Implementation cost of £9,872,000 provided in the PA was steep but not unexpected.

SECMP0041 - Amending the Change Board decision making rules for Modification Proposals

- **Summary**

  Seeks to change SEC Section D ‘Modification Process’ to ensure:

  - Each SEC Party is entitled to vote on SEC variations; and
  - SEC Change Board Members’ votes will be bound by views/votes put forward by their Party Category.

SECMP0041 - Amending the Change Board decision making rules for Modification Proposals

- **Impact**
  - All Parties are expected to be impacted by SECMP0041 as the introduction of SEC Party voting will allow all Parties the opportunity to formally feed into the final decisions on SEC Modification Proposals.
  - This modification is proposing to change the Change Board voting system, and if implemented, it is expected to have a positive impact on all future modifications.
- **Progress Update**
  - The first WG was held on Wednesday 18th October 2017.
  - SECAS are addressing the action items that came out of this meeting.
  - The second WG meeting will be arranged at a date in mid March 2018.

SECMP0042 - Amendment to SMKI Services to provide DCC Users and/or SMKI Participants with Authorised Responsible Officer (ARO) Statistics and Information

- **Summary**
  - Seeks to place an obligation on the DCC to develop a reporting mechanism which can be used by DCC Users and/or Smart Metering Key Infrastructure (SMKI) Participants to obtain up-to-date information on the use of ARO credentials for SMKI related services.
- **Impact**
  - All SEC Parties who are (or wish to become) DCC Users and/or SMKI Participants

SECMP0042 - Amendment to SMKI Services to provide DCC Users and/or SMKI Participants with Authorised Responsible Officer (ARO) Statistics and Information

- **Progress Update**
  - SECMP0042 was presented at September 2017 Panel meeting. It was agreed that this modification does not require further assessment and/or development by a WG as the SMKI PMA had already developed a set of business requirements to deliver the proposed solution.
  - The Panel agreed to submit SECMP0042 to the Refinement Process to allow for a full DCC assessment to be undertaken. The Preliminary Assessment request was submitted on 1st December 2017, and the DCC will be confirming the delivery date shortly.

SECMP0044 - User Security Assessment of a Shared Resource

- **Summary**
  - SECMP0044 seeks to improve the User Security Assessment process where a User has engaged in a Shared Resource to provide the User System on their behalf.

SECMP0044 - User Security Assessment of a Shared Resource

- **Impact**
  - This modification affects all Users who are using a Shared Resource to provide their User System.
  - Small Suppliers will benefit the most from this Modification as it will remove the need for a Full User Security Assessment in the second and third years following the first User Security Assessment.
  - Large Suppliers will still be required to have a Full User Security Assessment if they supply energy to more than 250,000 Domestic Premises, but they will be assessed independently of their Shared Resource.
  - Network Operators who use a Shared Resource will benefit in a similar way to Small Suppliers.

SECMP0044 - User Security Assessment of a Shared Resource

- **Progress Update**
  - The first Working Group meeting took place on Monday 22nd January. The WG requested for amendments to the draft legal text and agreed to meet again to discuss the new legal text.
  - SECAS are awaiting the draft legal text from legal advisors.

SEC Modifications Register

- Presents an overview of all SEC modification proposals
- Accessing the SEC Modifications Register
- SECAS refreshed the modifications register in March 2018.

Upcoming Meetings & Consultations

Working Group Meetings

- **SECMP0012** ‘Channel selection for Shared HAN solutions’ - **April 2018 (TBC)**
- **SECMP0025** ‘Electricity Network Party Access to Load Switching Information’ – **March/April 2018 (TBC)**
- **SECMP0041** ‘Amending the Change Board decision making rules for Modification Proposals’ – **March 2018 (TBC)**

Upcoming Meetings & Consultations

Industry Consultations

- **SECMP0002** ‘Add New Command to Reset Debt Registers’ – due **April 2018**
- **SECMP0019** ‘ALCS Description Labels’ – due **April 2018**
- **SECMP0023** ‘Correct Units of Measure for Uncontrolled Gas Flow Rate’ – due **20th March 2018**
- **SECMP0027** ‘Amending Service Request Forecasting’ – due **21st March 2018**

Industry Consultations

- **Industry Consultations**
  - **SECMP0029** ‘Business Continuity and Disaster Recovery Testing Amendments’ – due **April 2018**
  - **SECMP0034** ‘Changes to the SEC Section D for DCC analysis provisions’ – due **9th March 2018**
  - ****SECMP0043** ‘Modification to Services Force Majeure Provisions’ – due by **15th March 2018**
  - **SECM0045** ‘GDPR Modification’ – due **9th March 2018**

Where to find more information

- Guidance on the SEC Website
- Modification and Release Content Status Report
- Monthly SEC Modification Proposal Question Hour
- Email us: SEC.Change@Gemserv.com