Session A: Introduction to the SEC

SEC Party Engagement Day – 12th July 2018

Welcome

Gemserv

Afternoon Talks

Time	Session A: Introduction to the SEC
13:30 – 13:45	Introduction to the SEC and SEC Governance - Courtney O' Connor, SECAS
13:45 – 14:00	DCC Onboarding and Overview - Verity Blake, DCC
14:00 – 14:15	DCC User Entry Process - Marco Brunone, SECAS
14:15 – 14:30	Introduction to Security and Privacy, Nick Blake - SECAS
14:30 – 14:45	Prepayment Meters: Current Trends and Issues - William Wilson, Global 365

15:00 - Tea, Coffee and Network!

Introduction to the SEC and SEC Governance

Courtney O’ Connor, Party Support and Operations Delivery Manager, SECAS

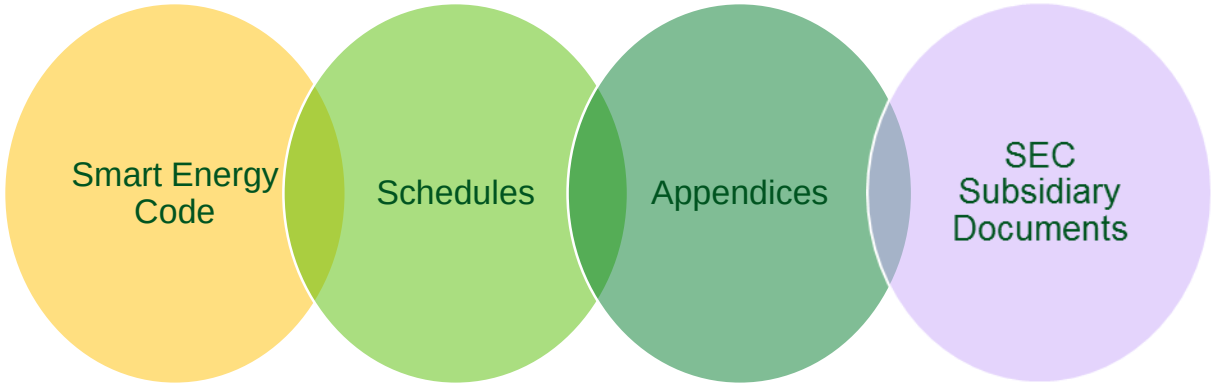
Introduction

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

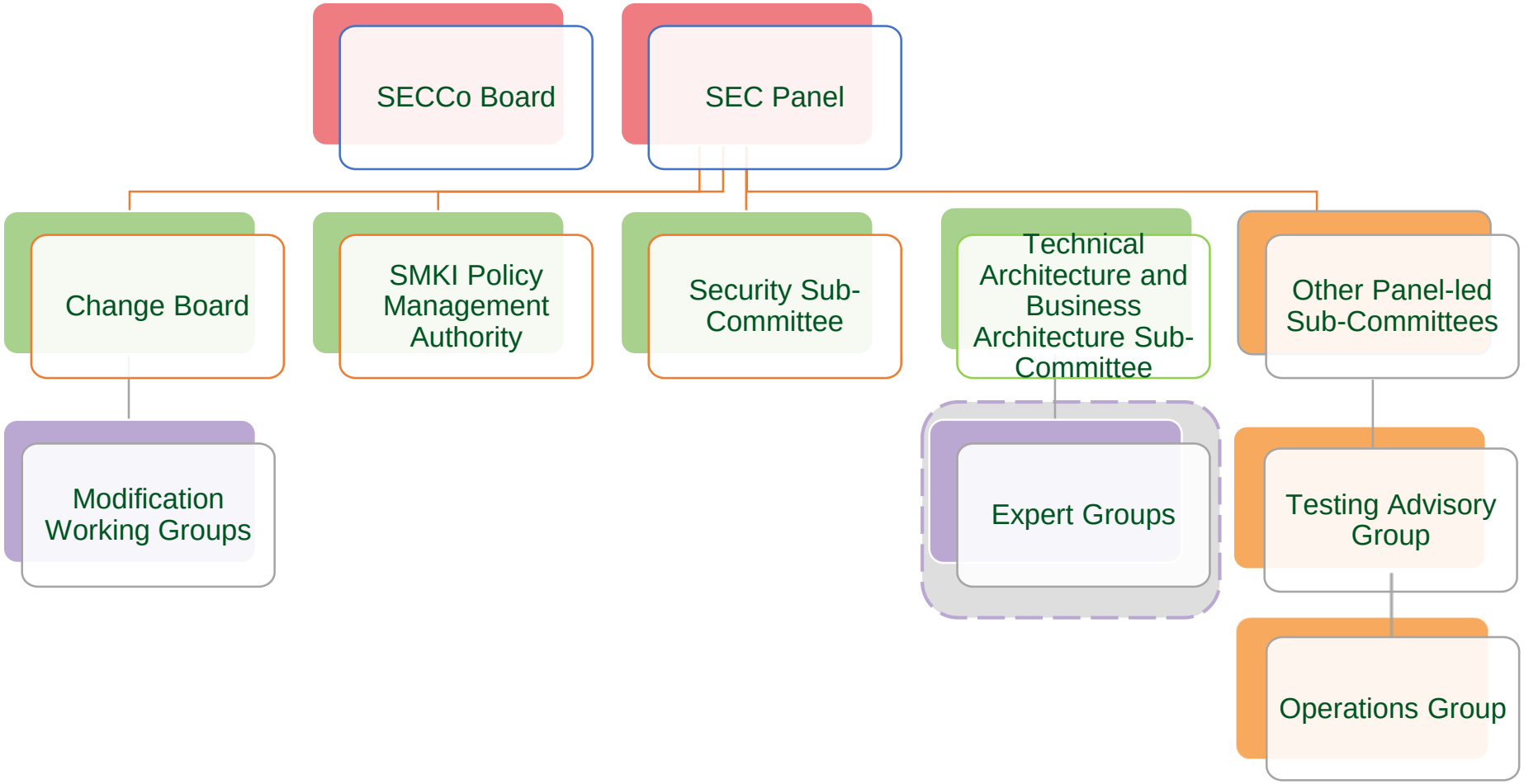
The Smart Energy Code (SEC)

- 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 Governance Structure



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

Smart Metering Key Infrastructure Policy Management Authority

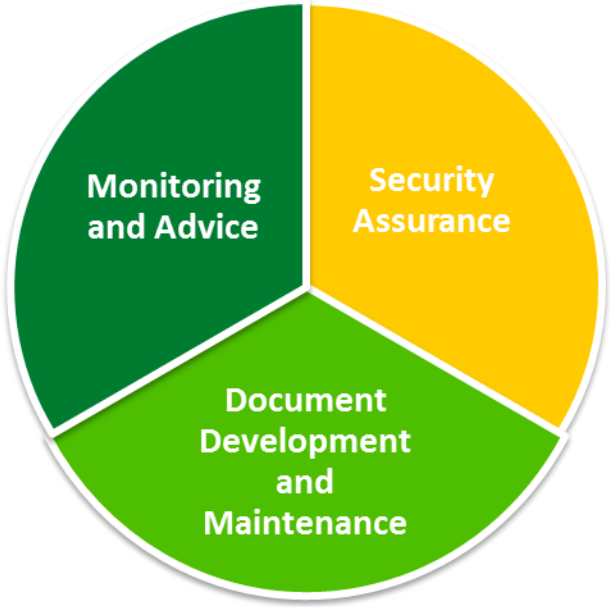
Sub-Committee	Function	Membership
SMKI Policy Management Authority (PMA)	Governs the SMKI Document Set and to monitor and gain assurance of the DCC operation of SMKI services	3 Large and 1 Small Suppliers, 2 Network, 1 SSC & 1 TABASC Representative, PKI Specialist, DCC, Ofgem, SoS and independent Chair

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

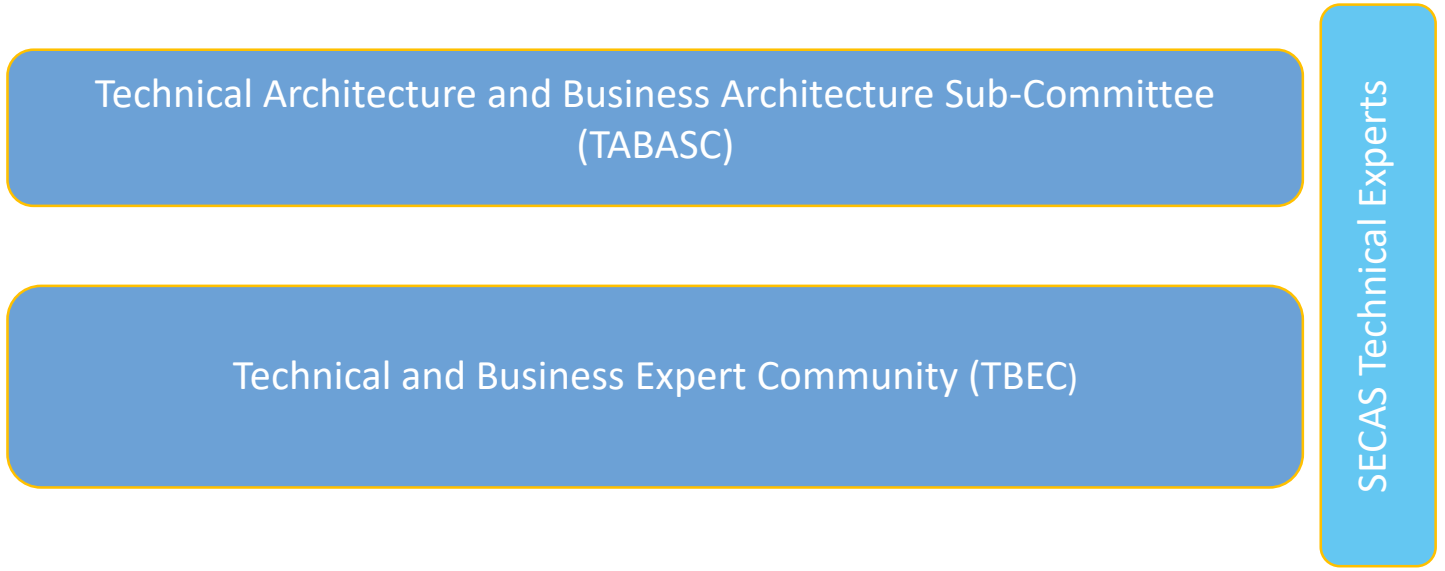
Security Sub-Committee

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



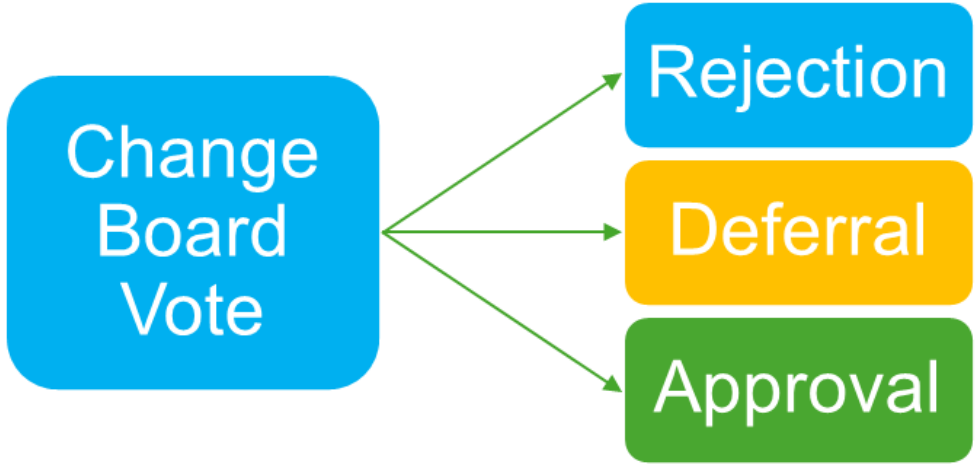
Technical Architecture and Business Architecture Sub-Committee

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, DCC, an independent Chair, SoS and Authority representative



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

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

Questions?

Courtney O’Connor, Party Support and Operations Delivery Manager, SECAS

Data Communications Company

DCC CUSTOMER ON BOARDING

Verity Thenard, Head of Regulatory Stakeholder Management, Smart DCC

Agenda

Scope

1. DCC On Boarding Steps
2. DUIS and Service Requests
3. Timelines and Useful Links

Data Communications Company

1

DCC Customer On Boarding Steps

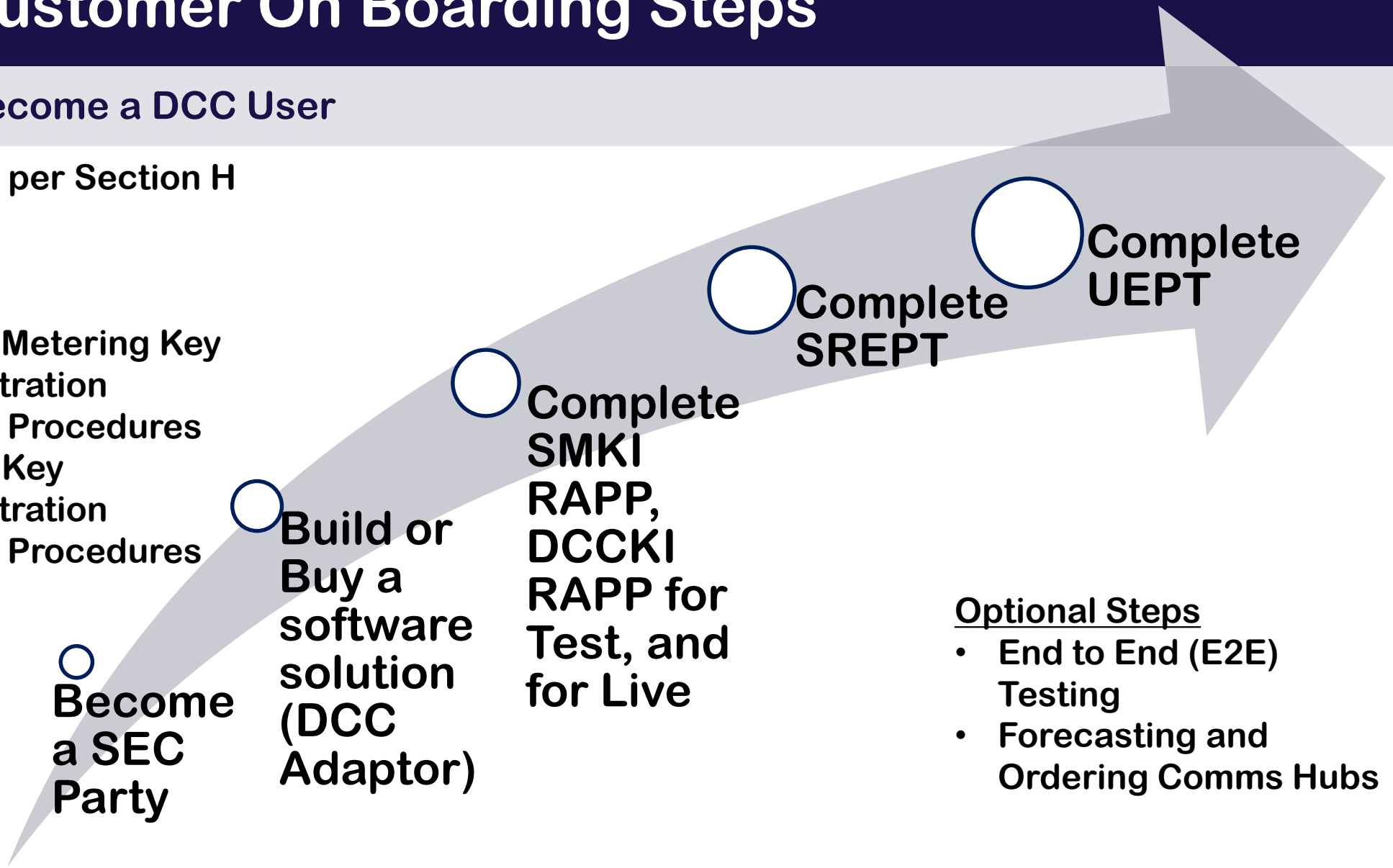
1 DCC Customer On Boarding Steps

Steps to become a DCC User

- Mandatory steps, as per Section H of the SEC

Acronyms

- **SMKI RAPP** – Smart Metering Key Infrastructure Registration Authority Policy and Procedures
- **DCCKI RAPP** – DCC Key Infrastructure Registration Authority Policy and Procedures



Optional Steps

- End to End (E2E) Testing
- Forecasting and Ordering Comms Hubs

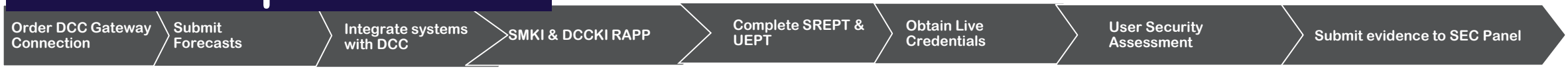
Data Communications Company

1 DCC Customer On Boarding Steps

Prepare to be a DCC User by User Role

Supplier

Network Operator



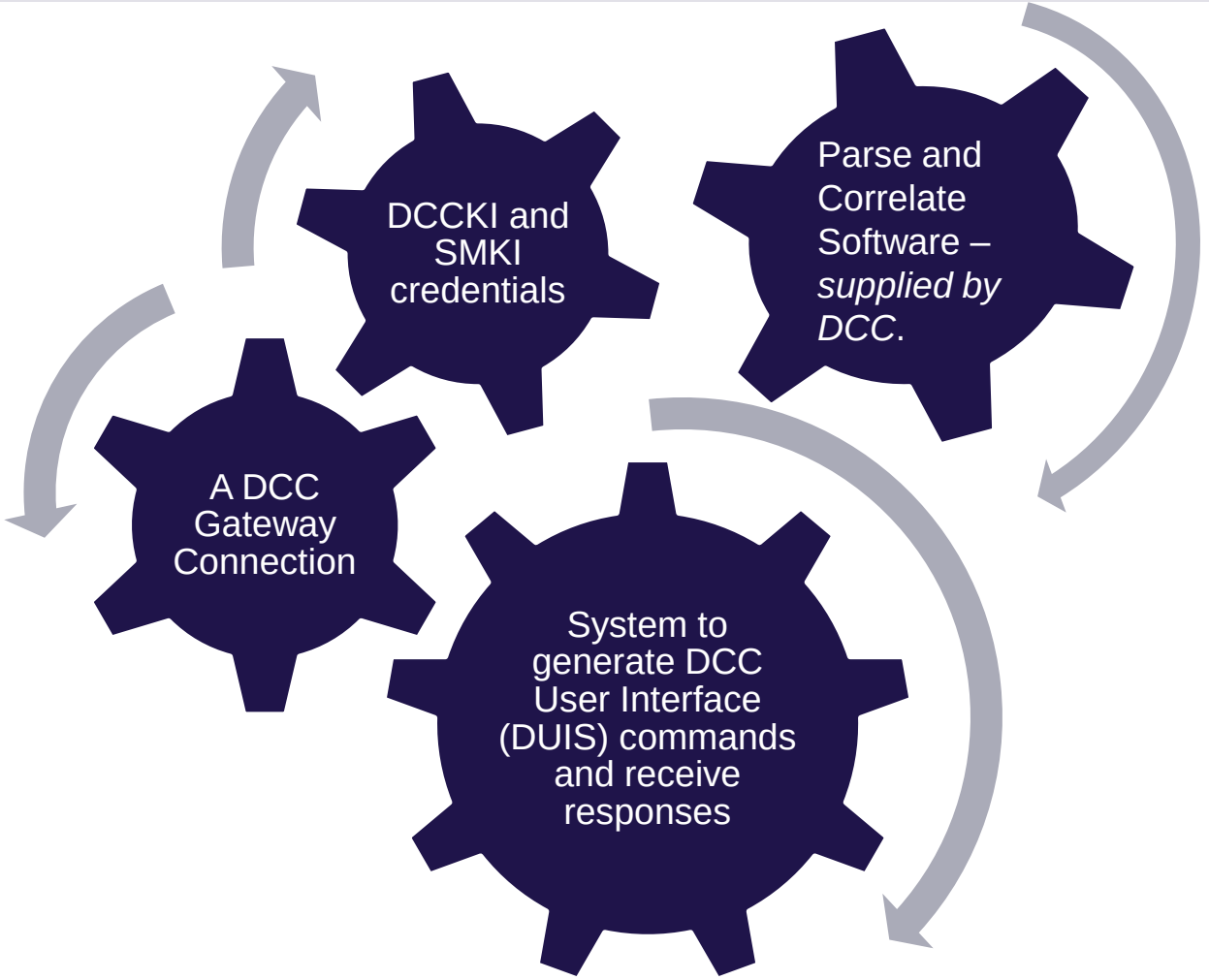
Other Users

Responsible Supplier Agent (RSA)

Data Communications Company

1 DCC Customer On Boarding Steps

What do you need to communicate with Meters?



Data Communications Company

1 DCC Customer On Boarding

User Roles and Services Available

All Roles

- Service Management
- Self Service Interface
- WAN Coverage Checker
- Smart Metering Inventory
- SMKI Services
- Reports

Import, Export and Gas Supplier

- Able to Install and Commission of devices in consumer homes
- Update device firmware
- Access to consumption data
- Billing
- TOU tariffs

Electricity Distributor and Gas Transporter

- Access to alerts including power outages & power restore and network information
- Able to check Supply Status and Event or Security Log
- Able to configure some alerts on devices
- GT able to initiate the recording of gas consumption data

Registered Supplier Agent

- Able to access services in their own rights and on behalf of Suppliers
- Able to read Device Configuration, Event or Security Log, Read Supply Status and read Firmware Version

Other User

- Need consumer consent to access data
- Access to Consumption Data
- Can add devices to HAN
- Read tariff Information
- Request Customer Identification Number

2

DCC User Interface Specification (DUIS)

2 DCC User Interface Specification (DUIS)

DUIS is the DCC User Interface Specification, is the communications interface designed to allow the communications referred to in Section H3.3 of SEC – the Communications to be sent via the DCC User Interface, which are sent between the DCC and DCC Users.

This machine-to-machine interface enables authorised Users to call Service Requests to interact with Devices and Services within the DCC, and to receive Responses to those requests, in addition to Device and DCC Alerts.

Use of the DCC User Interface enables Users to manage installed Smart Metering and make use of the wider DCC Services supporting the rollout, enrolment and management of Smart Metering Devices.

2 DCC User Interface Specifications

DCC User Interface Services Schedule

Full list available here: [SEC Appendix E - DCC User Interface Services Schedule]

Service Request Name	Service Reference	Service Reference Variant	Critical	Modes of Operation				Eligible User Roles						
				On Demand	Future Dated Response Pattern	DCC Scheduled	Non-Device Request							
Update Import Tariff (Primary Element)	1.1	1.1.1	Yes	Yes	Device	No	No	IS	GS					
Read Active Import Profile Data	4.8	4.8.1	No	Yes	DSP	Yes	No	IS	GS	ED	GT		OU	
Read Reactive Import Profile Data	4.8	4.8.2	No	Yes	DSP	Yes	No	IS		ED			OU	
Read Export Profile Data	4.8	4.8.3	No	Yes	DSP	Yes	No			ED		ES	OU	
Read Tariff (Primary Element)	4.11	4.11.1	No	Yes	No	No	No	IS	GS				OU	
Read Tariff (Secondary Element)	4.11	4.11.2	No	Yes	No	No	No	IS					OU	
Retrieve Daily Consumption Log	4.17	4.17	No	Yes	DSP	Yes	No	IS	GS	ED	GT		OU	
Create Schedule	5.1	5.1	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	
Read Schedule	5.2	5.2	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	
Delete Schedule	5.3	5.3	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	
Read Device Configuration (Identity Exc MPxN)	6.2	6.2.4	No	Yes	No	No	No	IS	GS	ED	GT	ES	OU	RSA
Read Device Configuration (MPxN)	6.2	6.2.7	No	Yes	No	No	No	IS	GS	ED	GT	ES	OU	RSA
Read Auxiliary Load Switch Data	7.7	7.7	No	Yes	DSP	No	No	IS					OU	
Read Boost Button Details	7.11	7.11	No	Yes	DSP	No	No	IS					OU	
Read Inventory (Current and Future Suppliers may use this Service Request)	8.2	8.2	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	RSA
Update Inventory	8.4	8.4	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	RSA
Join Service (Non-Critical)	8.7	8.7.2	No	Yes	No	No	No	IS	GS				OU	
Unjoin Service (Non-Critical)	8.8	8.8.2	No	Yes	No	No	No	IS	GS				OU	
Read Device Log	8.9	8.9	No	Yes	DSP	No	No	IS	GS				OU	
Update HAN Device Log	8.11	8.11	No	Yes	DSP	No	No	IS	GS				OU	
Request Customer Identification Number	9.1	9.1	No	Yes	No	No	No						OU	
Read Firmware Version	11.2	11.2	No	Yes	DSP	No	No	IS	GS	ED	GT	ES	OU	RSA
Request WAN Matrix	12.1	12.1	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	RSA
Device Pre-notification	12.2	12.2	No	No	No	No	Yes	IS	GS	ED	GT	ES	OU	RSA

Data Communications Company

3

Timelines and Useful Links

3 Timelines and Useful Links

SMKI Repository and Entry Process Tests (SREPT)

- SMKI Registration (RAPP) In order for parties to start SREPT you need to have completed the SMKI registration (RAPP) process and configured a connection. Refer to: Guide to SREPT and SMKI RAPP.
- SMKI RAPP forms need to be uploaded to SharePoint (forms processed then DCC initiates a verification meeting). Organisation verification with Director/Company Secretary via webex/skype
- ID verification for Senior Responsible Officer (SRO) and Authorised Responsible Officers (ARO) – only AROs receive a USB token at DCC's office with test (& live) certificates

SMKI Repository and Entry Process Tests (SREPT)

- SMKI & Repository Test Scenarios Document (SRTSD) sets out the test scenarios that must be completed by each category of test participant, and the test artefacts that must be produced for review by DCC
- Customers need to provide 60 working Days notice of their intention to start SREPT – this is provided to Testing.Notices@smartdcc.co.uk

3 Timelines and Useful Links

DCC Gateway Connection

- DCC gateway connection - low volume ~90 working days, high volume ~7.5 months
- Costs and charges for the DCC Gateway connection vary depending on the connection volume ordered. Each connection ordered will have an associated installation cost as well as an annual charge. Charges are published in our Indicative Charging Statements and Indicative Budgets, which are published on our website here. Guidance on charges can be found here.
- DCC has published FAQs and Guides on Gateway connections here.
- Gateway connections are ordered from the DCC Service Desk, servicedesk@smartdcc.co.uk, the forms that need to be submitted are on SharePoint here. A site visit will need to be conducted as part of the ordering process, to determine the work required.

3 Timelines and Useful Links

DCC Adaptor

- All the SEC documents are available on SECAS's website here. Use of DUIS is also available on the Developing the SEC Page.
- DCC's DUGIDS is on DCC's Design Release Forum page of SharePoint here. Older versions are also on DCC's website. The Message Mapping Catalogue is a SEC Document, and available on the SECAS Website.
- Great Britain Companion Specifications (GBCS), Government document that details the requirements for communications between the Home Area Network (HAN) and DCC. The latest version is available on the Developing the SEC Page.

3 Timelines and Useful Links

User Entry Process Test (UEPT)

- To become a DCC User, a Party must undertake User Entry Process Tests (UEPT) - refer to the Common Test Scenarios Document. This sets out the test scenarios that must be completed by each category of test participant, and the test artefacts that must be produced for review by DCC.
- During UEPT, a DCC Industry Test Analyst will be allocated to you to assist with the process.

Forecasting and ordering

- DCC has published a Forecast and Order Information Pack which provides an overview of the various forecasts DCC asks parties.
- There is a 10 month lead time for Forecasting, with orders being placed at the 5 month mark. As an example, if you require Communications Hubs to be delivered in March 2019 a forecast must be submitted by the May 2018 deadline. If you do not submit a forecast by the deadline, a nil return will be assumed. Forecasts must be submitted through the Order Management Systems (OMS). Information can be found here: DCC Operations SharePoint site.

3 Timelines and Useful Links

End-to-End Testing

- Provides an opportunity for Parties to test the interoperability of meters and back office systems. Refer to: End to end testing approach document.
- Can be undertaken against meters that are installed in a CSP Test Lab, or against meters that are installed in a remote test lab which has been established in a location chosen by the Party. Parties can use their own meters during end-to-end testing, or can ask the DCC to obtain meters on their behalf.

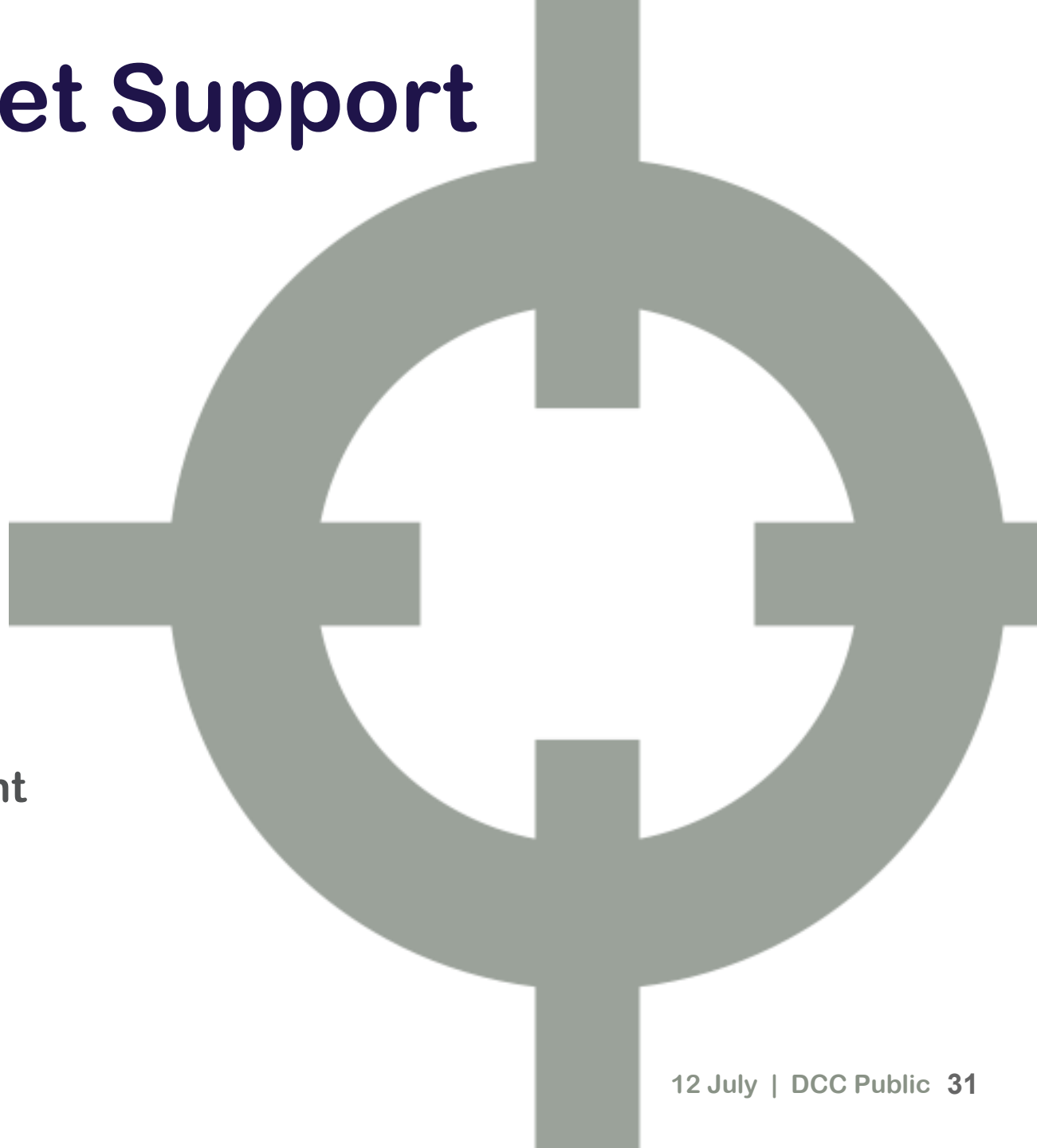
Security assessment

- Parties are required to undergo an Initial Full User Security Assessment as part of the User Entry Process – Contact SECAS for more details.

How to Engage and Get Support

Industry Test Team
Available to support you through testing
Testing.Notices@smartdcc.co.uk
Service Mangers
Our customers key contact at DCC
opsuserservice@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
General Questions?
Contact@smartdcc.co.uk



Data Communications Company

Thank you

Data Communications Company

User Entry Process - Becoming a DCC User

Marco Brunone, Party Support Senior 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

User ID

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

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

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) *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)

UEP Evidence 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.

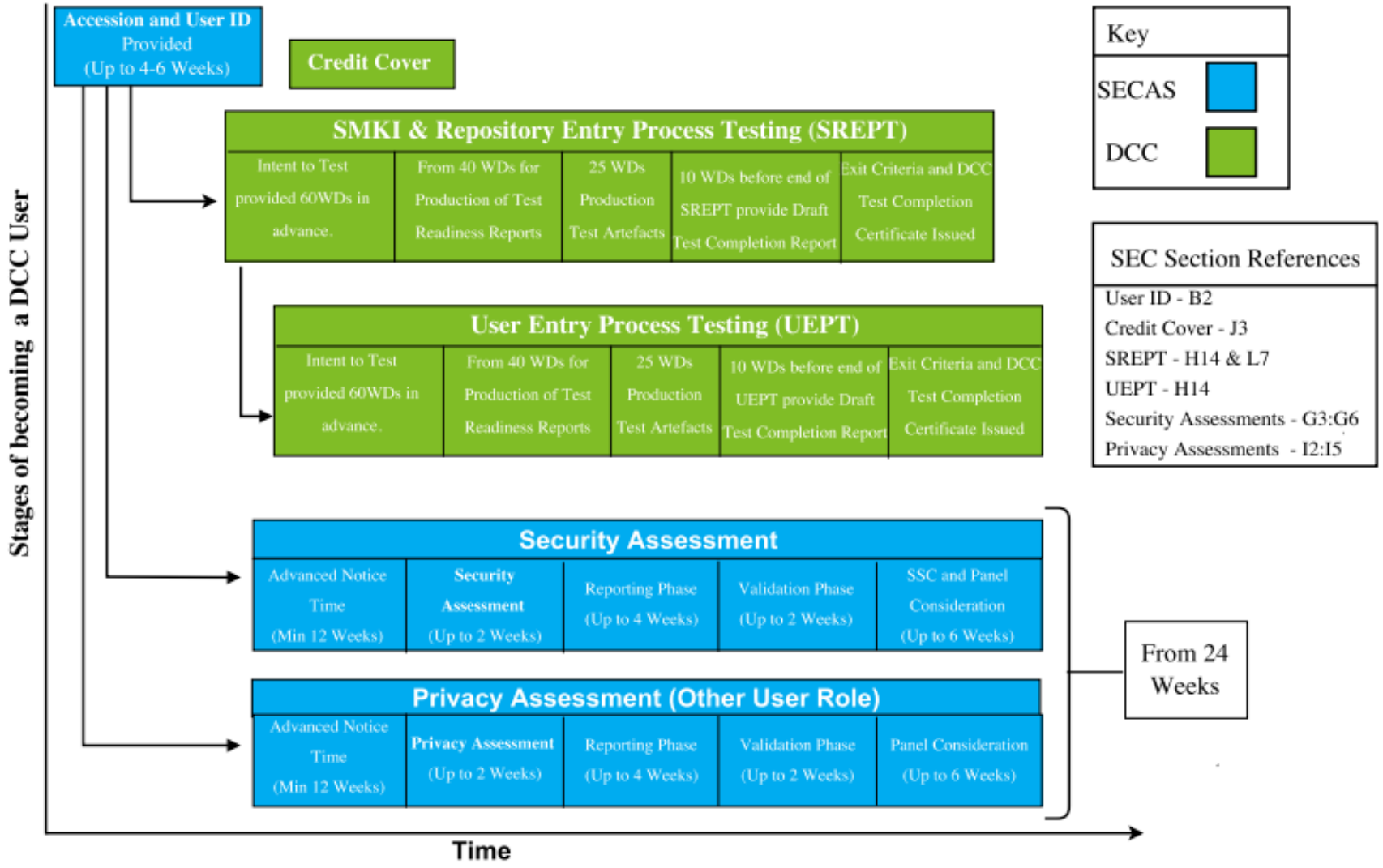
SEC Section H1.10 Clauses	Date Received	Evidence
SEC Section H1.10 (a) *Receive confirmation from the DCC that a User ID for the User Role has been accepted*		
SEC Section H1.10 (b) *Complete the required User Entry Process Tests for the User Role*		
SEC Section H1.10 (c) *Demonstrate the applicable 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.

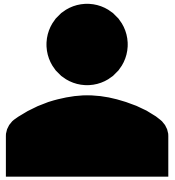
Estimated Timeline for Becoming a DCC User



Points of Contact

SECAS Helpdesk Tel: 020 7090 1000

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

Questions?

Marco Brunone, Party Support Senior Analyst, SECAS

Security and Privacy Overview

Nick Blake, Senior Security Analyst, SECAS

Agenda

- Types of assessment
- Overview of the controls frameworks
- 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.

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 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.

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.

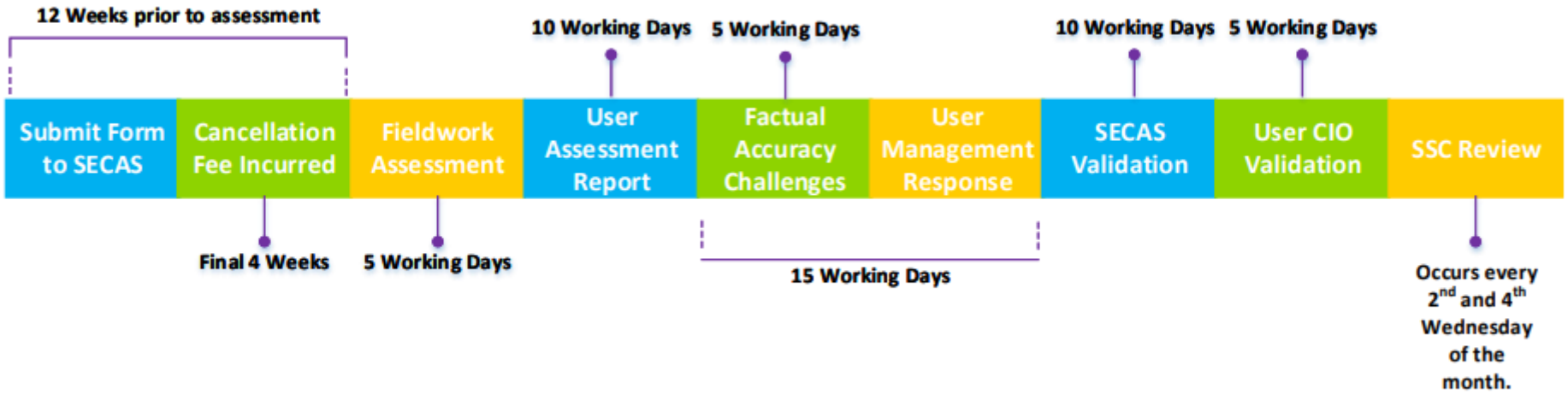
Control descriptions

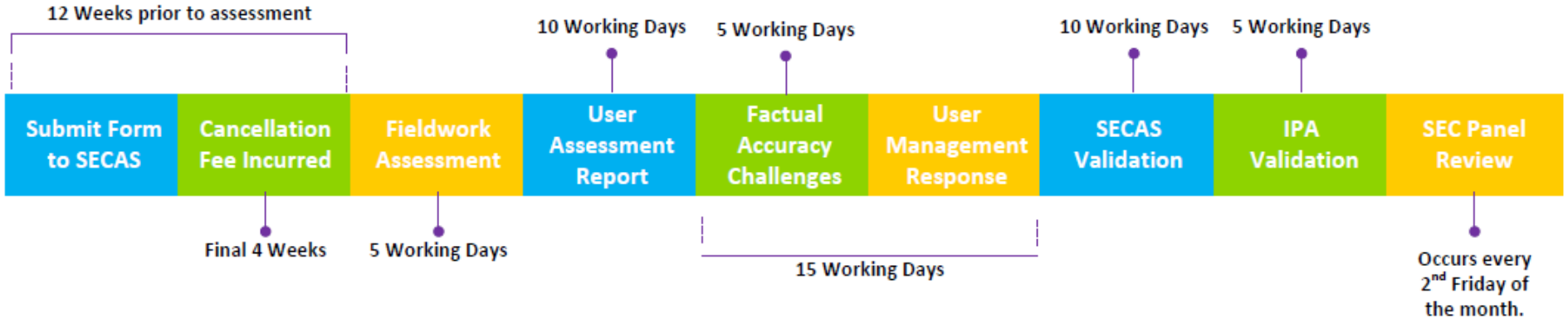
- The controls frameworks describe:
  - The different types of User Assessment including the applicable assessment criteria and frequency of assessment.
  - The activities and requirements of each stage of the assessment lifecycle: prior to an assessment, during an assessment and post-assessment.
  - 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.

Security and Privacy Assessment Timeline





Questions?

Nick Blake, Senior Security Analyst, SECAS

Prepayment Meters: Current Trends and Issues – GLOBAL-365

GLOBAL-365®

AGENDA

Questions!

Who is GLOBAL-365?

Terminology

Current trends and issues – legacy meters

Current trends and issues – smart meters

More questions

Questions!

Who is GLOBAL-365?

World Leaders in Innovative Business Process Automation

company purpose

We are a commercial organisation with a very serious social justice agenda.

Since the introduction of prepayment meters in the 1980s, those already living in fuel poverty have had to pay more than credit customers for their energy.

This means the most vulnerable in our society have to pay the price for a costly and inefficient service.

The Department for Business, Energy & Industrial Strategy's programme to install smart electricity and gas meters in every household in Great Britain by 2020 has created the opportunity for a new type of prepayment system to be developed.

Our SMARTprepay is the first system with the technology and sophistication to finally offer price parity between prepayment and credit customers.

smart® prepay


smart®
prepay

Terminology

Current trends and issues – legacy meters

Current trends and issues – smart meters

The following ways will be available for customers to make prepayments

Channel	Tender types
ATM	Credit card & debit card
Bank	Direct Debit & Standing Order
Card issuer	Recurring Payments
In Home Display	Credit card & debit card
Mobile phone - SMS	Credit card & debit card
Online	Credit card & debit card
Phone - DTMF/IVR	Credit card & debit card
Smartphone & tablet- app	Credit card & debit card
Smartphone & tablet- Pingit	Faster Payment
Retailers	Cash, credit card and debit card

smart prepay

Meter types supported

SMETS1

Manufacturer	SMSO
Aclara	CGI
Elster	CGI
Itron	CGI
L+G	Trilliant
Secure	CGI

SMETS2

Manufacturer	DCC adaptor
All	All

smart prepay®

Funds Splitting

Part of each top up can be used to make payments for other purposes such as paying off an energy debt or saving for Christmas

The customer chooses either a percentage of each top up or an amount per day, week or month and this will be automatically credited to a separate account

Minimum payments towards topping up energy are ring fenced

All payments and balances appear in the customer's online SMARTprepay account in real time

Renewable Energy Credits

UTRNs generated for prepayment customers immediately upon receipt of a file allocating the value of renewable energy generated by a community energy scheme in the previous 24 hours between the members of the scheme

smart® prepay

Warm Home Discount Scheme & Cold Weather Payments

UTRNs generated for prepayment customers immediately upon receipt of a file listing supplier's customer fuel specific account numbers and the value of payments

More questions

Any more questions

William Wilson

07785 393 576

william.wilson@global-365.com

Thank You For Listening

SEC Engagement Day – 12th July 2018

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 0039

LLOYD'S REGISTER LRQA ISO 9001 001

CYBER ESSENTIALS PLUS