Data Communications Company

Smart Metering Implementation Programme

Consultation on additional SEC content

DCC response

24th December 2014

Contents

1 Executive Summary

1.1 Introduction and background

Smart DCC Ltd (DCC) was granted the Smart Meter Communication Licence and acceded to the Smart Energy Code (SEC) on 23rd September 2013.

DCC provides the shared communications infrastructure allowing energy suppliers, network operators and other authorised users to operate Smart Meters. The Smart Meter communication service will enable consumers to manage their energy usage with near to real-time information of their energy consumption. Consumers will benefit from energy savings and reduced emissions as a result of more accurate information, bringing an end to estimated billing.

1.2 DCC's response

This document sets out DCC's response to the consultation on additional SEC content published on 17th November 2014 for:

- Additional Public Key Infrastructures and SMKI-related changes
- Security-Related requirements & Post-Commissioning Obligations legal drafting
- Movement of some Technical Arrangements into Subsidiary Documents and Providing for Some SEC Milestones to be Turned into Dates
- Test Services to Support System Providers and Shared Systems, and Possible DCC Gateway Connection Requirements for Remote Testing.

We broadly agree with the proposals set out in the consultation, subject to specific areas for further consideration which we set out in the main body of this response.

DCC looks forward to continuing to work with DECC and stakeholders to build a fit for purpose regulatory framework within which the benefits of Smart Metering can be realised.

If you have any questions regarding any part of this response please address them to [redacted]. DCC plans to publish this response on its website.

2 Additional Public Key Infrastructures and SMKI-related changes

Additional Public Key Infrastructures and SMKI-related changes	
Q1	Do you agree with the proposed approach and legal drafting in relation to Infrastructure Key Infrastructure?
A1	DCC broadly agrees with the proposed approach and legal drafting related to Infrastructure Key Infrastructure subject to the following observations: *SMKI RAPP* The Infrastructure Key Infrastructure (IKI) will be responsible for receiving and processing Certificate Signing Requests, which is a function of the Registration Authority. DCC will be required to make changes to the SMKI Registration Authority Policies and Procedures (SMKI RAPP) to reflect the issuing of Certificates in accordance with the IKI Certificate Policy. L3.20 states 'Any party or RDP which is an Authorised Subscriber in accordance with the IKI Certificate Policy will be an Eligible Subscriber for an IKI Certificate'. DCC are currently making amendments to the SMKI RAPP to accommodate the proposed changes. *ICA Certificates* L3.23 of the SMKI Repository includes both the Root ICA Certificate and the Issuing ICA Certificate and L5.1 (f) refers to "all ICA Certificates" as part of the SMKI Repository. However L3.21 states that the DCC is the only Eligible Subscriber of an ICA Certificate according to the IKI Certificate Policy. Therefore the only 'Relying Party' of an ICA Certificate is the DCC. DCC considers amendments should be made to L3.23 and L5.1 (f) to exclude the ICA Certificates as part of the SMKI Repository.
Q2	Do you agree with the proposed approach and legal drafting in relation to DCC Key Infrastructure?
A2	DCC broadly agrees with the proposed approach and legal drafting in relation to DCC Key Infrastructure subject to the following observation. The content within the DCCKI Interface Design Specification and the DCCKI Repository Interface Design Specification are relatively small SEC Subsidiary documents. Therefore both documents have been produced as a single SEC Subsidiary document. All DCCKI SEC Subsidiary documents were published for consultation 22nd December 2014 on the DCC website.

Q3	Do you agree with the proposed approach and legal drafting in relation to allowing RDPs to become Authorised Subscribers for Organisation Certificates?
A3	DCC agrees with the proposed approach and legal drafting to allow RDPs to become Authorised Subscribers for Organisation Certificates.
Q4	Do you agree with the proposed approach and legal drafting in relation to the checks the DCC must apply when deciding if a Subscriber is an Eligible Subscriber?
A4	DCC agrees with the proposed approach and legal drafting in relation to Device checks when deciding if a Subscriber is an Eligible Subscriber. The SMKI Device Certificate Policy Appendix A 1.4.1 (b) states that "the DCA may treat either a Supplier or the DCC for Devices that are either 'Commissioned' or 'Installed not Commissioned'." as an Eligible Subscriber. This aligns the policy intent that although DCC has no provisions to check Device Types, DCC will now be required to undertake additional checks in accordance with Appendix A 1.4.1 (b) when deciding if a Subscriber is an Eligible Subscriber.
Q5	Do you agree with the proposed approach and legal drafting in relation to the size restrictions on a number of fields in Device and Organisation Certificates?
A5	DCC broadly agrees with the proposed approach to place an explicit value on size restriction in the Issuer and Subject fields in Device and Organisation Certificates. In future, further changes to the field size specification in a Device and Organisation Certificate will require a Change Request to the Trusted Service Provider (BT). This would be followed by an impact assessment with potential time and cost implications. *Certificate Issuance* Appendix B 4.3.1 E (iii) states that the OCA shall not issue "any Certificate containing a Public Key if that Public Key is the same as that contained in any other Certificate that was previously issued by the OCA". The probability that two separate Service Providers generate the same Public Key pair for their Organisation Certificates is relatively low due to the algorithms used to generate Organisation Certificates as well as the high volume of Organisation Certificates required. DCC has explained the need to have this check in place is significantly low and is not supported by the TSP's solution. Should this text be concluded a Change Request would have to be issued to the TSP. This would delay the delivery of the SMKI service and have time and cost implications. *Organisation Certificate Profile* Annex B of Organisation Certificate Profile states that the subjectUniqueID field should contain "64 bit Entity Identifier for the Organisation that is the subject of the Certificate". DCC has interpreted this as a requirement for a stand-alone field outside of the normal Distinguished Name (DN) fields that are used to identify the subject of the Certificate. This requirement is not supported by the TSP solution as it is contrary to RFC Type RFC5280. DCC

	suggest the subjectUniqueID should be amended to Unique Identifier and the value column amended to "This attribute within the subject shall be populated with the 64 bit Entity Identifier (compliant with EUI-64 standard – see Great Britain Companion Specification) of the subject of the Certificate" this is because the RFC recommendation does not support subjectUniqueID which is aligned with the TSP solution reflected in the SMKI contract.
A6	Do you agree with the proposed approach and legal drafting in relation to the clarified Independent SMKI Assurance Scheme?
Q6	DCC broadly agrees with the policy intent to clarify who can be a member of the Independent SMKI Assurance Scheme subject to the following observation. In the marked up track changes of SEC4A, the legal drafting appears to have reversed the intended position back to the previous legal drafting in SEC4. SEC4A Appendix C 2.4 states "no director of the DCC (or of any such DCC Service Provider) is or becomes a director or employee....the provider of the scheme". The proposed legal drafting does not reflect the policy intent set out in Paragraph 263 of the SEC4A consultation. DCC consider the legal drafting position is reversed back to the tracked changes this reflects and the policy intent as set out in Paragraph 263 of the SEC4A consultation.

3 Security-Related requirements & Post-Commissioning Obligations legal drafting

Security-Related requirements & Post-Commissioning Obligations legal drafting	
Q7	Do you agree that the proposed changes are necessary and proportionate to protect DCC Systems?
A7	DCC broadly agrees that the proposed changes and legal drafting are proportionate to protect the DCC Systems. DCC may be exposed to security risks as a result of Parties connected to the DCC systems. The proposed security controls not only prevent imminent threat to the DCC systems but potentially mitigates the impact of further risks to all other connected Parties. Therefore implementing additional security controls to detect and prevent such security risks is supported by DCC. This agreement is subject to the following observations: *Security obligation for Testing* There are currently no SEC arrangements for DCC to apply security controls to the Test Participants within a testing environment. DCC suggests that the SEC permit the scope of a new Subsidiary document to include obligations on Parties, RDPs and DCC relating to the Issuing and use of Test Certificates for the purposes of Testing over a DCC Gateway Connection. This would place obligations on Parties and RDPs in relation to the security that they must adopt on their systems as part of such testing. *Systems vulnerability assessments* The policy intent in Paragraph 271 of the SEC4A consultation proposes an obligation on Network Parties and Other Users to complete system vulnerability assessments in accordance with their organisation risk assessment. The legal drafting in Section G3.8 excludes Network Parties and Other Users from carrying out system vulnerability assessments. If the proposed changes are concluded they will not align with the DSP contract and will therefore have time and cost implications. DCC suggest the legal drafting is amended to reflect the policy intent set out in Paragraph 271 of the SEC4A Consultation. *Party Signifier* DCC is required to provide an interim Incident Management process set out in X7 of SEC4A including a live Service Desk once SEC4A is designated. Once Section H15 is effective in January, Parties will be able to order DCC Gateway Connections. This process is intended to use the Party ID (now changed to Party Signifier) to identify SEC Parties that request a DCC Gateway Connection. The obligation on the Panel to provide Party Signifiers was not included in the SEC4A conclusions, which means that DCC will need to use an interim placeholder for this information. DCC would prefer that this obligation is concluded and designated as soon as possible to facilitate the transition to the enduring arrangements.

Q8	Do you agree with the proposed changes to the post commissioning obligations and associated limitation of liabilities?
A8	DCC disagrees with the proposed approach to the post commissioning obligations H5.33-39 and associated limitations of liabilities subject to the following observations: DCC are currently progressing the proposed changes to the post commissioning obligations set out in the SEC4 consultation aligned to GBCS v0.8.1 as the agreed solution design. DCC has no provisions in place to process the additional obligations set out in H5.33-39 of SEC4A as this functionality was not considered when proposing changes to the DCC Plan in the consultation published on 17th November 2014. DCC considers that the number of meters that will process a Device suspension would be very low immediately after DCC Live. In order to avoid further delays to the delivery of the programme, DCC suggest that the new obligations set out in H5.33-39 are implemented in a later release as part of our proposed Release Management Strategy. *SECA4 post commissioning obligations changes* H5.33 proposes that where a Communication Hub Function (CHF) fails to re-generate its Private Keys or one of the Organisation Certificates is compromised within 7 days of the event, Users must notify DCC in order to set the Smart Metering Inventory (SMI) Status to 'Suspended' until the CHF Device is replaced. H5.37 proposes that where a Smart Meter or a Gas Proxy Function (GPF) fails to re-generate its Private Keys or one of the Organisation Certificates is compromised within 7 days of the event Users must notify DCC in order to set the Smart Metering Inventory Status (SMI) to 'suspended' until the Device is replaced. Suspending Devices impacts all Users, including the User that has failed to complete their obligation. The User that fails to comply with their obligation is also obliged to replace the Device. The current design does not enable Users to initiate a Device suspension to DCC. Therefore DCC has no provisions to govern the process to fulfil a Device suspension request by Users. In order to meet such obligations a Change Request would need to be issued to the CSPs and the DSP. This would invalidate the current change DCC is in the process of implementing which would give rise to additional costs and delay delivery timescales. *Section M Limitations of Liability* M2.7 states that where the DCC or a Supplier Party breaches obligations set out in H5.34 - H5.35 (DCC) and H5.37 (c) and (e) (Supplier Party), a Party may recover costs as set out in M2.8. As outlined above DCC has no provisions in place to govern this process. DCC or a Supplier Party could not be in breach of such obligations if the current solution design does not support this, and as such the proposed legal drafting would need to align with the changes DCC are currently implementing. *DCC reporting service* DCC is currently working with Parties to consider DCC providing a number of operational reports to support all Parties, and discussing with DECC the need for the inclusion of a DCC reporting service within the SEC (to provide reports

	to Parties as agreed with Parties from time to time). One of the reports being considered is to identify a list of Devices where no attempt to change any of the credentials has been received within 7 days of installation (noting that this report could be run within a shorter elapsed time period e.g. a report could also be generated identifying Devices where no attempt had been made within 5 days to allow Suppliers to update their credentials in time). This proposal could be of value in this case as it may provide support to enable Users to identify or track meters where they may have not met their obligations. However, in order to manage the volume of data and costs, the emerging design proposals mean: • the reports are currently intended for early life support only (i.e. DCC would extract data only for new Users to constrain the volume of data) • the reporting process will be subject to a 24 hour delay as it will be based on an overnight extract of the DSP Service Audit Log • the scheduled time taken to run these extracts and reports has yet to be agreed • the reports will not be linked to any Service Management notification mechanism; it will therefore be the responsibility of Users to actively check the SSI to see what reports are available • the reports will only reflect the meter status and will not provide any information relating to Communications Hub security credentials • the reports are based on a limited period of data (currently intended to be 2-3 months), so meters left with unchanged certificates longer than this period would not be identified • the reports will identify where no attempt has been made to change credentials. Where a request has been attempted DCC would not correlate the request with the response message, nor would DCC validate which credentials have been changed. As a result, this approach may not identify all meters that have not successfully had all their required credentials changed.
Q9	At what point should the Recovery Key on a meter be validated?
A9	DCC proposes the point at which a Recovery Key on a meter should be validated is 'as soon as reasonably practicable (and in any event within 7 days) following the Commissioning on a meter'. The Recovery Key is an Organisation Key associated with a Public Certificate stored on Devices and should therefore align with the 7 day period the SEC requires for all other Device Certificates to be validated within. There is a risk that a Recovery Key that is not validated within this period may be compromised and therefore Could not be used to recover other credentials stored on the Device.

4 Movement of some Technical Arrangements into Subsidiary Documents and Providing for Some SEC Milestones to be turned into Dates

Movement of some Technical Arrangements into Subsidiary Documents and Providing for Some SEC Milestones to be turned into Dates	
Q10	Do you agree with the proposal to move four Section s of the SEC (H4, H5, H6 and O3) from the SEC into SEC subsidiary documents, and the proposed changes to the legal drafting accommodate this?
A10	DCC broadly agrees with the proposed approach subject to the following observations. *Section O3* DCC agrees with the rationale to move Section O3 from the SEC into a SEC Subsidiary document. For the avoidance of doubt, DCC assumes Section O3 will move into the Non-Gateway Interface Specification that DCC are obliged to produce in accordance with Section X9 of the SEC. *Section H* DCC agrees with the rationale to move content from H4, H5 and H6 into SEC Subsidiary documents, on the basis that the following are considered: *Changes to Obligations* a) The DCC solution design currently aligns to the drafting in H4, H5 and H6 set out in the SEC4 consultation. Any further changes made to the current drafting may have significant impact on the DCC delivery plan. This has not been factored into the DCC plan recently consulted on in accordance with Condition 13 which would have further time and cost implications. *Timing* b) There are currently no indicative timescales as to when the proposed content in H4, H5 and H6 will be moved from the SEC and developed into SEC Subsidiary documents. This may introduce new challenges to DCC being able to finalise related designs and documentation. For example the DCC User Interface Specification (DUIS) documents are scheduled to be concluded by March 2015.
Q11	Do you agree with the proposed approach to amending the legal drafting to provide for the Secretary of State to direct that an activity is required to be carried out in advance of a specified date instead of a milestone?
A11	DCC broadly agrees with the proposed approach for the Secretary of State to direct that an activity milestone can be replaced with a specified date subject to the following observation. DCC published a consultation on the DCC plan in accordance with Condition 13 in November 2014. Following the consultation DCC are set to submit a new plan to the Secretary of State in early 2015. DCC is concerned that prior to the approval of the new plan, if all activity milestones are replaced with a

specified date, they would not align with the delivery timescales of the new plan. DCC therefore suggest that the replacement of activity milestones with a specified date should not occur prior to this point.

5 Test Services to Support System Providers and Shared Systems, and Possible DCC Gateway Connection Requirements for Remote Testing

Movement of some Technical Arrangements into Subsidiary Documents and Providing for Some SEC Milestones to be turned into Dates	
Q12	Do you agree with the approach and proposed legal drafting supporting Parties undertaking tests equivalent to UEPT and SREPT on their own account?
A12	DCC agrees that a Party can place reliance on the tests conducted by Third Parties on the condition that: a) DCC can review the results of previous tests that have been undertaken; b) DCC can request that additional testing should be undertaken before the organisation can be deemed to have passed its UEPT and SREPT; and c) DCC understands the relationship between Parties and Shared Service Providers. The proposed legal drafting set out in L14.20, L14.29 and L14.33 of the SEC supports this approach.
Q13	Based on our understanding of the DCC's remote testing offering, it may be that a DCC Gateway Connection is required, which would mean that remote testing would only be available to SEC Parties. We welcome views from prospective testing participants on the impact this may have on their plans?
A13	DCC broadly agrees with the proposed approach to remote testing subject to the following observations. Section H14.31 and H14.9 of the SEC require that DCC provides a service and related facilities to enable Test Participants, including non-SEC Parties, to conduct Device Testing and User System Testing. We set out requirements for a Test Participant to undertake remote testing as discussed with DECC below: a) Service Requests are sent to a Device via the DCC User Gateway, which would allow the participant to fulfil the basic tenet of proving interoperability between the Device and the DCC Systems; b) any organisation wishing to test the interoperability of Devices with the DCC will need to obtain a Communications Hub for Testing as part of the Testing Services and are likely to require the ability to generate Service Requests in accordance with the DCC User Interface Specification (DUIS), previously known as DCC User Gateway

Interface Specification (DUGIS)

c) any organisation that would like to send a Service Request to its own Devices via the DCC User Interface (whether installed in a remote test lab or a CSP test lab) must first complete the relevant User Entry Process Tests and SMKI & Repository Entry Process Tests, or other entry criteria as set out in the Enduring and End-to-End Test Approach Document;

d) the organisation must have the capability to place SMKI Certificates on the Devices.

We consider this to be the default solution, which is described in Option 1 below. DCC firmly considers that this is the preferred Option for all Test Participants.

DCC recognises that, there are certain categories of Test Participants who are neither prospective DCC Users nor SEC Parties (e.g. test houses, assurance scheme operators and device manufacturers). We agree with DECC's statement that it is not onerous to become a SEC Party or to access testing services via the DCC Gateway. However, we do recognise that it may be more difficult for these categories of Testing Participant to generate Service Requests.

Additionally, regardless of whether these Test Participants establish a DCC Gateway Connection they will need to meet the security requirements demanded by SEC of DCC Users if they wish to interact with the DCC Systems. For example, DCC Users must comply with ISO27001 ISO27005 and undergo a Security assessment. It is likely that there would need to be equivalent obligations on non-SEC Parties through a Bilateral Agreement.

Remote Testing Solutions

In discussions with the DSP and CSPs, DCC has considered three options that would enable Testing Participants who are not DCC Users or SEC Parties to test different elements of their solution in a remote testing environment.

1. No central development
2. Limited enhancement to Service User Emulator
3. Hosted or Distributed Testing Solution

Option 1 – No central development:

This solution has no impact on the DCC programme, but the Test Participant needs to develop or acquire testing software to generate Service Requests for which they must use a DCC Gateway Connection.

Outline solution:

Under this option a Test Participant would be required to develop their own systems capable of generating Service Requests (or procure these from a commercial (service provider) or collaborate with other Test Participants and

send them to DCC using a DCC Gateway Connection.

DCC would make available the test environments to the Test Participant, to ensure that test data can be configured for their use (security credentials, for example), offer support to these Test Participants and support resolution of Testing Issues raised.

Relative benefits:

This solution would require least central development of the solution, thus minimising the risk of using resources without any benefit if there is no demand for the service. It would provide the greatest level of assurance as this testing solution imitates closely the full requirements for Users to test and use the DCC solution. There would be very few operational constraints such as time availability, bandwidth and responsiveness. It is therefore less manually intensive than Option 2.

This solution is, however, more onerous on Test Participants to develop necessary systems (or procure relevant services) especially if a significant number of participants wish to solely test Devices.

Option 2 – Limited enhancement to Service User Emulator:

The Service User Emulator is a tool that tests the DSP solution during Pre-Integration Testing. It is being developed by the DSP and could potentially be used to emulate the interaction of Service Users with the DSP solution. This solution has limited impact on the DCC programme but is highly constrained in the service it provides to a Test Participant and we are concerned that this would not be a viable option for high volumes of testing. It may be a more suitable solution for any Test Participant that wishes to use the service on an ad hoc basis.

Outlined solution:

The DCC may be able to provide an extension to the tools being developed to support DCC testing during Pre-Integration Testing to Test Participants as follows:

a) the Test Participant sends the required information to the DSP via a suitably-secured means, which would need to be considered;
b) this request provides the information required by the DSP to generate Service Requests on behalf of the Test Participant;
c) the DSP will generate Service Requests via a Service User Emulator as agreed with the Test Participant;
d) the DSP will send these Service Requests to the Devices that have been installed in the CSP Test Lab or Remote Test Lab;
e) the Service Responses and Alerts will be received by the Service User Emulator and provided to the Test Participant by the DSP.

The applicable charges associated with the Testing Services will be set out in the guide for Testing Participants as required by section H14.3 of the SEC, which we anticipate to publish on the DCC Website Q1 2015. The associated

charges would need to appear on the DCC Charging Statement as an Explicit Charge under K7.5 (i). The addition of these Charges would require a Notice to amend the Service Charges in accordance with Licence Condition 19.11.

Relative benefits:

This service would only be appropriate if there is limited demand – this would have the lowest development cost, but be manually intensive in operation and subject to considerable operational constraints (such as time availability, bandwidth and responsiveness), all of which would need to be fully impact assessed.

This proposal removes the requirement to establish a DCC User Gateway Connection to a Test Participant solely for the purposes of testing Devices in a remote test lab or at a CSP test laboratory.

It is included within the draft End–to-End Testing Approach Document which is currently published on the DCC website for review[1] and which will be developed in conjunction with DCC's Test Design and Execution Group (TDEG) prior to formal consultation, the timing of which is currently being reconsidered in light of the re-planning, but expected in Q2 2015.

Option 3 – Hosted or Distributed Testing Solution:

This solution has a potentially high impact on the DCC programme but enables Test Participants to test without having to develop their own testing software to generate Service Requests and may remove the requirement to use a DCC Gateway Connection. The solution would require DCC to maintain the software on an enduring basis unless it was agreed that the solution could be provided to the industry on an open source basis.

Outline solution:

Under this option DCC would make available an enhancement of the Service User Emulator (as described in Option 2) for use by Test Participants. The enhancement would enable Test Participants to initiate Service Requests, by either:

a) enabling a secure connection via a web service into the Service User Emulator, which would be hosted within the DCC systems; or
b) distributing an enhanced version of the Service User Emulator to Test Participants and enabling them connect to the DCC test environment using a standard DCC Gateway Connection.

We would recommend that any additional development costs would be

[1] http://www.smartdcc.co.uk/media/1673/vt_0003_end-to-end_testing_approach_document_v1_0.pdf

recovered as Fixed Charges and that costs incurred directly as a result of Device testing (such as Test Participant support or costs of providing a DCC Gateway connection) are charged explicitly to a Test Participant. As with Option 2, these Charges would need to be added to our Charging Statement.

Relative Benefits

This solution would balance the level of development required by DCC and by Test Participants, which may be appropriate, depending upon the demand for such a service. There would be very few operational constraints such as time availability, bandwidth and responsiveness it is therefore less manually intensive than Option 2 however, there would be a time and cost impact.

Conclusion

We would anticipate that system development costs would be recovered within Fixed Costs and that costs incurred as a direct result of individuals testing (e.g. Requesting a Communication Hub, Communications Link or DSP operating Option 2) would be charged directly to the Testing Participant as an Explicit Charge. Although no solution has been recommended, the volume of potential users would be the likely determinant for the preferred options influenced by demand for the service. There is no current requirement upon the DCC to implement a specific solution for Test Participants and we envisage this being agreed through the Transitional Governance arrangements, as necessary.

DCC considers that Option 1 is the default option.