Data Communications Company

DCC Production Proving Options Analysis & Recommendation

V1.0

Date: 14 February 2018

Classification: DCC Public

Table of Contents

1 Introduction

The Data and Communications Company (DCC) wishes to undertake production proving; to conduct tests using production meters and other Devices in the live production environment ('production'). The key benefit of this activity is to provide additional assurance of DCC systems, providing DCC and Users with increased confidence in its systems in readiness for roll-out at scale.

The purpose of this document is to set out the reasons why it is necessary for the DCC to implement Production Proving capability and set out an analysis of the alternative options that the DCC has evaluated in recommending the proposed solution.

The principal objectives of production proving are to enable the following:

- releasing new software into production seamlessly, where Service Requests (SR) have been tested against all Device types;
- prove the DCC Total Systems end-to-end, where SRs are exercised daily;
- proactively identify issues in the production environment before they impact Users;
- speedily triage User issues to minimise disruptions and loss of service to Users; and
- prove fixes following implementation.

DCC would be better able to meet these objectives if it is able to undertake proving activities in the production environment and therefore under realistic conditions as would be experienced by DCC Users. DCC continues to undertake rigorous testing of DCC Systems in the Pre-Integration Testing (PIT), Systems Integrating Testing (SIT) and User Integration Testing (UIT) environments. However, due to the differences between the test environments and the production environment, if DCC is to fully prove live systems it needs to undertake production proving in the production environment (details of the differences are provided in section 1 of the annex).

Under the existing regulatory and security arrangements, DCC is permitted only limited capability to test with real Devices in the production environment. For DCC Live (Release 1.2, November 2016) DCC worked with BEIS to introduce changes to the Smart Energy Code (SEC) to enable proving of production Communication Hubs. This has enabled DCC to undertake some proving activity in the production environment, but not using meters.

DCC has conducted a detailed analysis of the options available to implement production proving capability. The options are as follows:

- Option 1 - build a pre-production environment (with sub options for the types of pre-production environments built);
- Option 2 – utilise an energy supply company to undertake production proving (with sub-options for partnering model);
- Option 3 - DCC itself implements a Production Proving Function;
- Option 4 – early roll-out of DCC releases to a set of DCC Users (early adopters); and
- Option 5 – do nothing.

DCC has undertaken a detailed evaluation of the options and option 3 is recommended - DCC implements a Production Proving Function. This would give DCC the ability to install, commission and interact with production devices in the live environment. This would be limited to devices

deployed for production proving purposes only – there will be security controls in place which stop DCC from successfully communicating with non-production proving devices in the live DCC environment.

Changes are required to the SEC to enable DCC to implement its recommended option.

2 Summary of Options

DCC has identified a number of options to enable it to undertake production proving. It has conducted a review of each option to help it identify the best solution. This has entailed DCC evaluating each option in terms of its strengths and weaknesses and the extent to which the option meets DCC's production proving objectives (as set out in section 1 to this paper). DCC has also assessed each option against the following set of criteria - estimated cost, security impact, time to implement, regulatory impact, stakeholder impact, and risks. A high-level summary of the DCC analysis is provided in the table overleaf with the detailed analysis provided in section 2 of the annex to this paper.

The costs provided are high level estimates, and should be regarded as indicative at this stage. The firm costs will be arrived at through the process of competitive procurement and further informed by the detailed design of the solution. It is conceivable that this may result in the costs increasing or potentially decreasing. Clearly once the actual costs are known they may vary from the indicative costs summarised in this paper. Our objective in carrying out the competitive procurement will be to obtain the best available value for money.

RAG: Green-Low Impact to Criteria; Amber- Medium Impact to Criteria; Red-High Impact to Criteria				Key Criteria			
Title	**Option**	**Key Benefits**	**Key Constraints**	**1Security Impact**	**2Estimated Cost (high-level and indicative)**	**3Time to Implement**	**4Risk/ Effectiveness**
Pre-production environment (*different usage to live environment)	**1a – Pre-production with infrastructure a close replica and same code base to production**	Provides high confidence for new releases and can triage functional faults and some non-functional.	The biggest constraint in using a pre-production is the fact that live Service Request monitoring of the production system cannot be carried out, and therefore DCC will still be behind Users in becoming aware of environmental issues. Costs significantly higher than other options (£50m+) and time to implement 12 months +.		Design & Build - £50m+ Ongoing - £5m per year (approx). Significantly higher than other options.	Lead time longer than other options.	Considered red based on criteria 2 & 3 and because the option is not effective in meeting production proving objectives.
	1b - with the same code base as production, but different infrastructure (cloud based solution)	Provides high confidence for new releases. A cloud based pre-production would have the benefit of not being restricted by Service Levels that are currently in place for User Integration Testing A (UIT-A) (Option 1c).	As a hybrid, cloud environment would not enable proving of environment configuration / implementation issues for certain sub-sets of the solution (core IT stack). Would not be an exact replica of production (different infrastructure) and it would not therefore be possible to run full diagnostics against this option. Code based issues could be diagnosed, but not environmental issues. Costs significantly higher than other options (other than 1a) (£40m-£45m) and time to implement 12 months +.		Design & Build - £40-45m +. Lower than 1a due to solution being cloud based. Ongoing - £5m per year (approx.). Significantly higher than other options.	Lead time much longer than other options.	Considered red based on criteria 2 & 3 and because the option is not effective in meeting production proving objectives.
	1c – utilise UIT-A	UIT-A is capable of acting as a pre-production environment. It already exists therefore implementation costs and lead time to implement are not a concern.	It carries the same limitations as option 1b in terms of offering very limited capability to prove the live environment. UIT-A cannot be considered a true reflection of production for performance and resilience issues.		N/A – already exists.	N/A – already exists.	Option not effective in meeting production proving objectives.

RAG: Green-Low Impact to Criteria; Amber- Medium Impact to Criteria; Red-High Impact to Criteria				Key Criteria			
Title	**Option**	**Key Benefits**	**Key Constraints**	**1Security Impact**	**2Estimated Cost (high-level and indicative)**	**3Time to Implement**	**4Risk/ Effectiveness**
Utilise energy supplier	**2a – utilise existing energy suppliers**	Allows for end to end systems proving, post release proving and can triage faults.	Incident resolution slowed down due to reliance on 3rd party. Increases DCC's risk of non-compliance with its Licence - working with energy supplier may increase the risk of unforeseen market distortions and discrimination.		Set up cost - £200k. Ongoing cost - £50k per year+ £25k for a release.		Due to regulatory risks and reliance on 3rd party.
	2b – supplier in a box (via MSP)	Allows for end to end systems proving, post release proving and can triage faults.	Incident resolution slowed down due to reliance on 3rd party. Potentially raises wider regulatory concerns as DCC will need to restrict the supplier's ability to supply energy and compete in the supply market. Potentially long lead time in comparison to other options, setting up a supply company may be time consuming.		Set up cost - £500k - £700k. Ongoing costs – £350k - £400k per year.	Potentially long lead time (associated with setting up a new supplier).	Possible regulatory barriers and reliance on 3rd party.
DCC Production Proving Function	**3 – DCC Production Proving Function**	Allows for end to end systems proving, post release proving and can triage faults at speed as the Production Proving Function will be an internal DCC function (within DCC Technical Operations) and there is no reliance on a 3rd party.	Regulatory and security amendments required. Greater DCC investment (in comparison to other options).	After controls implemented.	Set-up costs £600k - 870k. Operating costs £300k - 500k per year.	Capability delivered in stages.	Achieves proving objectives.
Early roll out of releases to some Users	**4 – early rollout of releases to some DCC Users**	Provides high confidence for new releases.	Proving capability is limited to releases, this option does not enable daily proving of DCC systems and does not enable DCC to triage faults occurring in live.		Considered similar to 2a.		Limited proving capability.

RAG: Green-Low Impact to Criteria; Amber- Medium Impact to Criteria; Red-High Impact to Criteria				Key Criteria			
Title	**Option**	**Key Benefits**	**Key Constraints**	**1Security Impact**	**2Estimated Cost (high-level and indicative)**	**3Time to Implement**	**4Risk/ Effectiveness**
Do nothing	**5 – do nothing**	No investment, security impact or regulatory changes required.	Does not provide the additional assurance and capability DCC believes is desirable. Increased risk of issues that result in loss of service and so direct costs to Users, and potentially also increased DCC charges due to release failures, slower fixes and higher volume of Incidents that require additional resources to handle the cascading problems. Potential impacts on roll-out progress, and DCC meeting operational performance targets.		Risk of costs to Users from delays, loss of service and increased DCC charges. .		No proving capability in live environment.

3 Recommendations & Justifications

DCC recommends that option 3 is implemented subject to the solution being competitively tendered.

DCC considers the recommended option as the option that meets the principal production proving objectives i.e. it provides a secure and reliable service for end to end systems proving, post release proving and for triaging faults at speed.

Option 3 would impact the existing security arrangements. After careful assessment of the risks, in discussion with the Department for Business, Energy & Industrial Strategy (BEIS), appropriate security controls have been identified. The security impact after implementing additional controls is considered to be low because:

- The integrity of the security architecture is maintained;
- There will be separation between the Production Proving Function and Production Proving Systems, and other parts of the DCC Live Systems; and
- Controls will be put in place to ensure that the Production Proving Function cannot carry out any critical service requests on live Devices in consumer premises even if the other parts of DCC Live Systems are compromised.

The high-level solution for Option 3 is set out in Section 4.

3.1 Other Options Considered

Options 1a and 1b have been dismissed on the basis that the implementation lead times and costs are significantly higher in comparison to the other options. DCC's proving ability would be limited (in comparison to option 3) and the high investment is therefore not considered economic and efficient. Whilst option 1c (utilise UIT-A) is readily available, DCC would not be able to prove live systems as it would in production. The option is therefore dismissed due to the limited capability it offers.

Option 2a is dismissed on the basis that DCC has concerns that contracting with energy suppliers (and certain energy suppliers having early access to new DCC releases) could increase the risk of unforeseen market distortions and discrimination and therefore increase DCC's risk of non-compliance with its Licence.

Option 2b is dismissed on the basis that setting up an energy supply company would entail considerable work (and potentially long lead times) although this would be reduced by procuring a Supplier in a Box. Furthermore, DCC does not have absolute certainty at this stage that the solution does not give rise to wider regulatory concerns given that under this arrangement DCC would need to restrict the supply company's ability to supply energy and compete in the supply market.

Option 4 is dismissed on the basis that it provides very limited proving capability; it would only enable post release proving. DCC would not be able to prove systems on a daily basis or undertake diagnostics, the option therefore does not meet DCC's production proving objectives.

Option 5 is dismissed on the basis that it does not provide the additional assurance that DCC services will operate satisfactorily in the live environment, and there is therefore a higher risk of Incidents arising, delays, and additional costs.

4 Option 3 – DCC Production Proving Function (high level solution)

4.1 DCC Production Proving Function – Regulatory Principles

Following discussions with BEIS the following assumptions have been agreed with regards to the regulatory changes required to implement this option. The Production Proving Function will be a DCC function that has the capability to do the following:

- Become a subscriber for Organisation Certificates for the purpose of DUIS XML signing and PP Registration Data File Signing;
- Become a subscriber for Device Certificates that may include any type of Device as the Subject of the Certificate;
- Be permitted to act as if it were a User in a number of User roles;
- Install and commission Devices as part of a Smart Metering System (SMS);
- Send Service Requests that result in the sending of Commands (both Critical and Non-Critical) to PP Devices comprising those SMSs and receive responses and Alerts from the same;
- Have self-generated MPXNs in the PP Registration Data for which it is the Registered Gas Supplier and Registered Electricity Supplier. This will be achieved by DCC being permitted to create dummy Registration Data for the purpose of production proving (and for such purposes be treated as a Registration Data Provider); and
- Communicate only with PP Devices installed for production proving purposes.

4.2 DCC Production Proving Function – Detailed Solution

In this option, DCC implements a Production Proving Function, under the existing security architecture that would allow DCC when acting as the Production Proving Function to interact with the other part of the DCC Live Systems in the way that DCC Users would interact with DCC Live System. To maintain the integrity of the security architecture, a number of soft and hard controls will be implemented in the PP Function, PP Systems and PP devices.

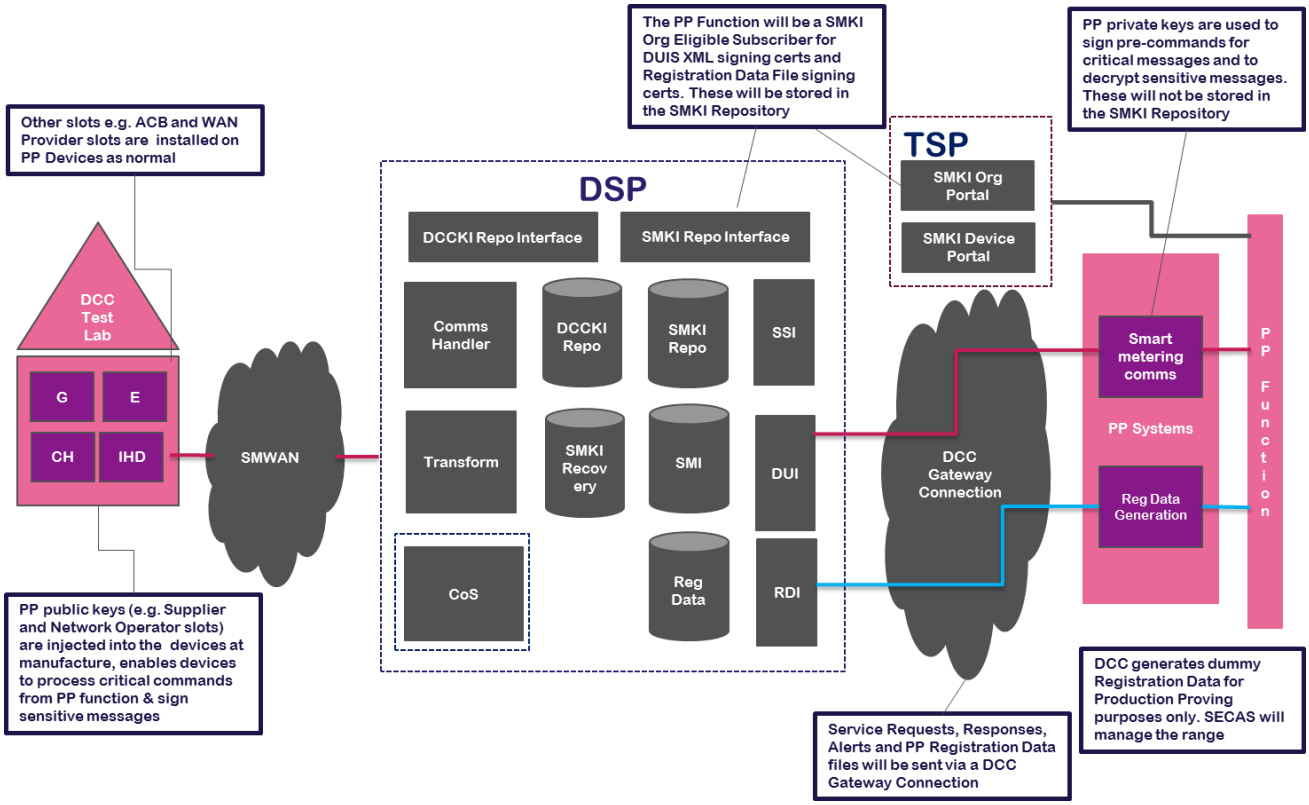

Figure 1 - Option 3, DCC implements a Production Proving Function

The implementation of the solution would be as follows:

- The Production Proving Function will be a DCC function that has the capability of sending Service Requests to the DCC and commands to Devices installed and commissioned by DCC for production proving purposes only; the Production Proving Function will be restricted to only do so to production proving Devices and will not do so to non-production proving Devices;
- The Production Proving Function will have the ability to interact with the DCC Live Systems under specific User roles for the purpose of production proving only. The Production Proving Function will submit Service Requests over the DCC User Interface as if it were a User and receive Signed Pre-Commands, Alerts and Responses;
- DCC would not inherit supplier obligations generally and would not act as a supplier outside of production proving. This would be achieved through SEC changes to describe a new SEC party role (DCC Production Proving Function) that would have the right to act in the various DCC User roles (i.e. IS, GS, ES/ NO and OU);
- The Production Proving Function will be an eligible SMKI subscriber under the Organisation Certificate Policy for a remote party role of XML Signing and Registration Data File Signing certificates;
- The Production Proving Function will be an eligible SMKI subscriber under the Device Certificate Policy for Device certificates;
- The PP Systems will send Service Requests over the DCC User Interface as if it were a User. The PP Systems will be Separate from the DSP and will use a Gamma connection to connect to the other parts of the DCC Live Systems;

- The Production Proving Function will install and commission bespoke production smart metering systems (SMS) in a suitable environment under the above roles (the Devices will be in a controlled, non-consumer environment). The SMS will not be installed at real meter points as they will be behind a settlement meter. The SMS will be reserved for production proving purposes only and Production Proving Function will only be permitted to communicate with these specific SMS; specific cryptographic controls will be implemented to ensure this;
- The Production Proving Function will also submit dummy registration data specific to the production proving via the Registration Data Interface. The Registration Data will be the same format as live User Registration Data, however, the values will fall outside of the existing industry ranges; and
- The Production Proving Systems will be separate from the rest of the DCC Total System.

To ensure the implementation of the solution is secure, additional security controls will be implemented (although not all of these would necessarily be explicitly set out in the SEC). Details of the cryptographic controls and non-cryptographic controls which would be implemented are provided in section 3 of the annex.

This solution does however, limit the activity and business / User processes that can be proven in production.

Specifically:

- Install and commission: Installation and Commissioning can be achieved via two approaches. By submitting Service Requests to Devices with pre-injected public keys in the supplier and network operator slots (injected at point of manufacture) or by populating the supplier and network operator slots with the access control broker key, which is then swapped during Installation and Commissioning for the supplier / network operator public keys. The latter approach is intended to stop supplier keys being compromised during the manufacturing process. Under this solution, the Production Proving Function would not be able to prove the latter Installation and Commissioning process.

- Change of supply: as the PPF would be restricted from accessing the DCC COS function, it would not be able to swap certificates on PPF Devices and prove / test this process.

Solution benefits:

- Production proving is under full DCC control.
- There is minimal / no change to the existing DCC total systems.

Solution issues:

- Not all User processes could be tested / proven.
- Bespoke devices are required.
- Longer lead time to implement (due to bespoke device manufacture lead times).
- Higher cost than volume production Devices (due to bespoke device manufacture requirement).

5 Next Steps

- DCC presents the Production Proving Function solution to the SEC Panel Subcommittees (SSC, TABASC, SMKI PMA, Operations Group).
- Following the outcome of the consultation, DCC carries out the necessary activities to implement the Production Proving Function.

Annex – Further Information

1 Background

1.1 Essential Background

The test environments are purposely designed to be more dynamic and fluid as a result of fixes being tested in support of Incident and defect resolution, and are generally a release ahead of production due to defect fixes being applied to support end to end test defect resolution. For example, DCC's UIT-A environment is functionally equivalent to live, but also functionally ahead as it is a test environment where new functionality/ fixed are tested, meaning the code base will often be different. Therefore, the test environments will never be an exact replica of the live environment. Detailed examples of the specific differences between the test and live environments are provided in section 1.2 of the Annex.

1.2 Examples of the specific differences between the test and production environments are as follows

- the test environments use a different Smart Metering Key Infrastructure (SMKI) repository and SMKI certificates. This means that faults and upgrades relating to this functionality can only be identified in the live environment;

- the extant test environments are not built to production scale and are only functionally equivalent to production. This means that the end to end production environment performance and performance related issues can only be predicted via these environments rather than definitively identified;

- the test environments are not always at the same configuration baseline as production. This is because workarounds are often applied in this environment to enable successful testing (e.g. manual configuration changes may be applied in the test environments that would be implemented as automated configuration once implemented in production); and

- pre-production (option 1b) will be a hybrid cloud solution. It will therefore not be an exact replica of production until production is also a hybrid cloud solution.

2 Detailed Options

2.1 Option 1 – build a pre-production environment

There are three sub-options for building a pre-production environment:

- Option 1a - build a pre-production environment which is identical to production, using an on-premises solution;
- Option 1b - build a pre-production environment with the same code base as production, using a hybrid cloud environment; or
- Option 1c- utilise the existing UIT-A (test) environment.

Option	Benefits	Constraints	Estimated Costs (High Level and Indicative)	Implementation Timescales	Impacts (Security, Regulatory, Stakeholder)	Risks
Option 1a - Pre-production with infrastructure a close replica and same code base to production **(different usage to production)**	• Provides high confidence for new releases and can triage functional faults and some non-functional. Examples of non-functional faults that can't be triaged are where an environmental failure on production is not known, although the symptoms are, and therefore cannot be replicated in pre-production, i.e. a process is not functional in production. Performance and resilience tests will be possible in this environment.	• Costs significantly higher than other options (£50m+). • A new (expensive) environment will need to be built which although it will be a functional replica of the production code set, the environment will be different and experience has shown that production Incidents are as likely to be environmental issues as code defects. • The biggest constraint in using a pre-production is the fact that live Service Request monitoring of the production system cannot be carried out, and therefore DCC will still be behind Users in becoming aware of environmental issues. • Upon upgrading production, it is key that any environmental installation issues are detected and this can only happen in production.	Design & Build - £50m+ Ongoing - £5m per year (approx.) Devices in pre-production would not be the same/ real Devices as in Production.	Minimum 12 – 24 months.	Security – none expected on the basis that controls in a pre-production environment are no different to other test environments. Regulatory - low impact. Provisions may need to be introduced into SEC in respect of the operation of the environment. Stakeholder – significant cost to Users and ultimately energy consumers. DCC Service Provider (SP) impact is also high in respect of work required to design and build and therefore lead time to deliver will be 12month +.	DCC is unable to deliver within a reasonable timeframe as a significant amount of work is required and DCC SPs will have to manage delivery alongside existing commitments.

Option 1b – with the same code base as production, but different infrastructure **(Cloud based solution)**	• Provides high confidence for new releases.	• As a hybrid cloud environment would not enable proving of environment configuration / implementation issues for certain sub-sets of the solution (core IT stack). • Would not be an exact replica of production (different infrastructure). • Would not enable DCC to test or triage production SMKI certificates related functionality or issues. • It would not be possible to run full diagnostics against this option as it would be a different environment. Code based issues could be diagnosed, but not environmental issues. • Assuming a 10-20% reduction in implementation costs for a hybrid cloud solution would cost between £40-45M + which is still	Design & Build - £40-45m + (assumes a 10-20% reduction in comparison to Option 1a due to the solution being cloud based). Ongoing - £5m per year (approx.)	Minimum 12-24 months.	Security – none expected on the basis that controls in a pre-production environment are no different to other test environments. Regulatory - low impact. Provisions may need to be introduced into SEC in respect of the operation of the environment. Stakeholder – significant cost to Users and ultimately energy consumers. DCC SP impact is also high in respect of work required to design and build and therefore lead time to deliver will be 12month +.	DCC is unable to deliver within a reasonable timeframe as a significant amount of work is required and DCC SPs will have to manage delivery alongside existing commitments.

		significantly high.				
Option 1c – utilise UIT-A	UIT-A is capable of acting as a pre-production environment. It already exists therefore costs and lead time to implement are not a concern.	It carries the same limitations as option 1b in terms of offering very limited capability to prove the live environment. UIT-A cannot be considered a true reflection of production for performance and resilience issue.	n/a – already exists.	n/a – already exists.	Security – none expected. Regulatory – non- expected. Stakeholder – none expected.	None expected.

2.2 Option 2 – utilise an energy supply company to undertake production proving

DCC has identified two options for how it can work with a supply business, who would undertake production proving for DCC:

- Option 2a – utilise existing energy suppliers to test Devices; and
- Option 2b – 'supplier in a box'; establish a new supply company (procured through a Managed Service Provider) which is set up solely for providing a production proving service to DCC.

Option	Benefits	Constraints	Costs (approx.)	Implementation Timescales	Impacts (Security, Regulatory, Stakeholder)	Risks
Option 2a – utilise existing energy suppliers	• Allows for end to end proving of the solution to real meters / Devices in the production environment and would be useful for post release production proving. • Triage would be possible for functional and environment specific Incidents.	• DCC will need its requirements prioritised to ensure it is receiving a secure and reliable service. I.e. for system releases a supplier will need to ensure their systems are upgraded in a timely manner to undertake proving. DCC anticipates that this option may run into difficulty as a supplier will need to manage competing priorities (including its own delivery programmes) and this tension may result in the supplier not meeting the Service Level Agreement	Set up cost - £200k. Ongoing cost - £50k per year+ £25k for a specific release (to stand up a team for a weekend). Potentially costs to supplier for reprioritising its delivery programme – unknown. *These costs are estimated	6 months to complete regulatory activities (tbc if regulatory changes required) and design / stand up a DCC capability to manage.	Security there is a residual risk that the supplier may attempt to misuse production proving access to attack production systems. Therefore, the production proving supplier will be obliged to comply with security controls equivalent to SEC Section G obligations. Regulatory - this option is low impact. SEC may require a regulatory change to introduce rules for how this would work in practice. Stakeholder - a sub set of suppliers are perceived at being at an advantage due to early adoption of DCC changes.	Risk that supplier is not meeting Service Level Agreement. Raises concerns over DCC's compliance with the requirements of its Licence, in particular the general objective (Condition 5.10(a)[1]) to carry on the mandatory business in the manner that is most likely to facilitate competition, and DCC acting in a manner that is consistent with its special position, the relevant prohibition being not to discriminate between any persons (Condition 11.7(b)[2]). DCC's concern is that contracting with energy suppliers will increase the

[1] 5.10 The Second Enduring General Objective of the Licensee is to carry on the Mandatory Business in the manner that is most likely to facilitate**:**

(a) effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy under the Principal Energy Legislation;

Smart Meter Communication Licence

[2] 11.7 In undertaking each such activity, the Licensee must not**:**

(a) unduly prefer itself or any Affiliate or Related Undertaking over any person or any class or description of persons; or

(b) unduly discriminate between any person or any class or description of persons.

Smart Meter Communication Licence

		placed on it. • Although the option is perceived to be low cost there will be costs to suppliers i.e. upgrading their systems for major DCC releases. • There would be significant impact to DCC operations in managing multiple suppliers simultaneously to deliver this capability on DCC's behalf. • There is potential of delay being added for the triage of functional Incidents having to reach out to the supplier. • Diagnostics could be run against this option, but it would be within the control of the supplier.	by DCC, they have been informally shared with a supply company and are considered a reasonable estimate.			risk of unforeseen market distortions and discrimination, and therefore increase DCC's risk of non-compliance with its Licence.
Option 2b – supplier in a box	• Allows for end to end proving of the solution to real meters / Devices in the production environment and would be useful for post release	• Solution raises regulatory concerns given that under this arrangement DCC will need to restrict the supply companies' ability to supply energy and compete in the supply	Set up cost - £500k - £700k. Ongoing costs – £350k - £400k per	6 – 12 months to become fully operational.	Security – there is a residual risk that the supplier may attempt to misuse production proving access to attack live systems. Therefore, the production proving supplier will be obliged to comply with security controls equivalent to SEC Section G	Regulatory concerns result in DCC being unable to implement the solution.

	production proving. • Triage would be possible for functional and environment specific Incidents.	market. It is un-clear at this stage whether these can be overcome. • Costly to procure and implement with long lead times as the Managed Service Provider has to complete all steps to become a DCC User and meet other regulatory obligations placed on energy suppliers. • Less control for DCC and diagnostic ability diminished due to access. There is potential of delay being added to the triage of functional Incidents having to reach out to the Managed Service Provider. • Unknown regarding how a Managed Service Provider will act as a proxy in the middle.	year.		obligations. Regulatory – no changes required to SEC or Licence. Potentially wider regulatory concerns in relation to the supplier being self-supply. Stakeholder – none.	

2.3 Option 3 – DCC implements Production Proving Function capability

Under option 3 DCC would implement production proving capability (as an internal DCC function); modification to the SEC to introduce the DCC Production Proving Function will be required. This will give DCC the ability to install, commission and communicate with real Devices in the live environment.

Option	Benefits	Constraints	Costs (approx.)	Implementation Timescales	Impacts (Security, Regulatory, Stakeholder)	Risks
Option 3 – DCC Production Proving Function	• Allows for end to end proving of the solution to real Devices in the production environment. • Allows for post release production proving. • Diagnostics can be run against this option. DCC has greater control for diagnostic capability (as no reliance on non-DCC party). • No requirement for purchasing separate diagnostic tools • Triage would be possible for functional Incidents, and within the control of DCC (no reliance on non-DCC party) • Environmental issues would be visible.	• Regulatory changes required. Security architecture amendment required. • DCC will need relationships with device manufacturers. • The solution requires greater DCC involvement (hands on). • Greater integration with adapter and head end costs. • Own RDP feed along with management (lead time and costs to deliver).	Set-up costs £600k - £870k. Operating costs £300k - £500k per year.	4-6months. DCC is looking to implement capability in stages. This includes interim solutions - contracting with a 3rd party to send Service Requests into Production in a managed service capacity.	Security – impact is considered low as mitigations have been identified. The existing security controls prohibit DCC from acting in a User role. This restriction is intended to avoid security breaches resulting from the compromise of one organisation, and reflects that the DCC has functions that are not operated by a User. However, mitigations have been identified and on the basis of this the security impact is considered to be low. The final solution will be presented to the SEC Security Sub-Committee (SSC) and implementation of the solution will be subject to SSC's agreement. Regulatory – impact is high. Changes are required to the SEC to implement the solution. Stakeholder – (medium) impact to Service Provider to deliver the solution.	None

2.4 Option 4 – early roll-out of DCC releases to a set of DCC Users

Under option 4 DCC would roll-out new releases to a set of DCC Users before they are made available to all DCC Users.

Option	Benefits	Constraints	Costs (approx.)	Implementation Timescales	Impacts (Security, Regulatory, Stakeholder)	Risks
Option 4 – early roll out of DCC release to a set of Users	• Provides high confidence that a release is viable prior to deployment in production.	• Provides limited capability (release testing only). • Does not meet diagnostics requirements as capability only enables DCC to prove releases.	Considered similar to 2a.	Can be implemented straight away.	Security – none. Regulatory, Stakeholder – a sub set of suppliers are perceived at being at an advantage due to early adoption of DCC changes.	Raises concerns over DCC's compliance with the requirements of its Licence, in particular the general objective (Condition 5.10(a)[3]) to carry on the mandatory business in the manner that is most likely to facilitate competition, and DCC acting in a manner that is consistent with its special position, the relevant prohibition being not to discriminate between any persons (Condition 11.7(b)[4]). DCC's concern is that contracting with energy suppliers will increase the risk of unforeseen market distortions and discrimination, and therefore increase DCC's risk of non-compliance with its Licence.

[3] 5.10 The Second Enduring General Objective of the Licensee is to carry on the Mandatory Business in the manner that is most likely to facilitate**:**

(a) effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy under the Principal Energy Legislation;

Smart Meter Communication Licence

[4] 11.7 In undertaking each such activity, the Licensee must not**:**

(a) unduly prefer itself or any Affiliate or Related Undertaking over any person or any class or description of persons; or

(b) unduly discriminate between any person or any class or description of persons.

Smart Meter Communication Licence

2.5 Option 5 – do nothing

Under option 5 no further action is taken to prove live systems.

Option	Benefits	Constraints	Costs (approx.)	Implementation Timescales	Impacts (Security, Regulatory, Stakeholder)	Risks
Option 5 – Do nothing	• No investment required. • No change to regulation.	• Significantly higher risk of issues in live environment results in loss of service to Users; cost implications for Users; impacts on roll-out progress; impacts on DCC meeting operational performance targets; impacts DCC's reputation and the reputation of the smart metering programme.	Costs to Users from service disruptions and also greater costs in the form of DCC charges since increased DCC resources will be required to handle the cascading problems.	n/a	Security – none. Regulatory – none. Stakeholder – significantly increased risk of impacts to Users and ultimately energy consumers from issues arising in the live environment which cannot be tested. Greater direct costs and inconvenience for Users, with possible resultant delays and loss of impetus for their rollout plans; and also, greater costs in the form of DCC charges since increased DCC resources will be required to handle the cascading problems.	Smart meter roll-out progress impacted by unforeseen faults in DCC service.

3 Option 3 – Production Proving Function Solution: Security Controls

To ensure the implementation of the solution is secure, non cryptographic security controls will be implemented:

- The Anomaly Detection Threshold (ADT) values for all Service Requests sent from the Production Proving Function would be agreed with the Security Sub-Committee.
- Individuals who can generate production proving Service Request will be DCC employees and specifically not DSP employees. These individuals will be subject to appropriate security vetting. These people will not be employed in identified DCC roles such as SMKI RA or DCC Security assurance team.
- PP Devices will comply with production compliance and certification requirements, as well as being restricted to target Service Requests to only the PP Devices.
- PP Systems will be located at a site other than the one housing production DSP systems and that they should not be administered by DSP staff who have access to the DSP production systems.
- PP Systems and controls will be subject to an independent security assessment.
- The DCC will demonstrate to the SSC on a monthly basis that SRs have not been targeted at non-production proving Devices, and that this evidence be retained and available for an external audit.

The following cryptographic controls would also be applied:

- Production Proving Function would sign DUIS XML with self-generated private signing keys for which it has previously requested and been issued with corresponding SMKI XML signing certs by the TSP. This would enable Production Proving Function to submit valid DUIS Service Requests. However to enable this and to ensure that such keys and certificates cannot be used in relation to any live Device, the TSP would need to add a new Remote Party Role (. pPPXmlSign). The Production Proving Function needs these Certificates only so that it can sign the XML of Service Requests and Pre-Commands to the DCC – such signing is already required to be done with keys that are never used for signing Command for Devices.
- Production Proving Functions would sign GBCS pre-commands with different self-generated private keys for which there must be no corresponding SMKI Certificate (The Production Proving Function must never ask for such Certificates and the TSP must never issue such Certificates to the Production Proving Function). This means that a critical Command signed by the Production Proving Function cannot be successfully executed on any live Device that has had only SMKI Certificates installed on it. This is different to Supplier and Network Parties, who are required to have SMKI Certificates issued in relation to such keys, and have such SMKI Certs installed on all their live Devices (SEC IEWP has requirements to make sure this is the case by no later than 7 days following installation)
- PP Devices would be manufactured and configured before installation as per all other Devices, with only one exception. The exception is that the Production Proving Function would instruct the Device manufacturer to place the Production Proving Function's public keys in the supplier and network Operator Trust Anchor Cells (the Production Proving Function would calculate these public keys from the private keys it has generated – this is how public keys are always calculated). This means that PP Devices would accept Supplier

and Network Operator instructions from the Production Proving Function (all other instructions come from the ACB and the PP Devices would accept these as well)

- The Production Proving Function would be allowed, in common with every other Party and all parts of the DCC, to create its own public / private key pairs including its own Supplier and Network Operator key pairs. It would need to have the Device Manufacturers, from whom it buys PP Devices place its supplier and network operator public keys (along with the valid SMKI ACB, WAN Provider and other Certificates) on the PP Devices it wants to use. The Production Proving Function would not be allowed any SMKI Certificates valid for use on Devices. If commands with Production Proving Function public keys are sent to a Device other than a PP Device, that Device would reject these commands, as the Certificates in them would fail Certificate path validation on the Devices (since the Certificates were not issued by SMKI, and so will not chain back to the SMKI root which is on the Device). This is why the Production Proving Function could never cause a critical action on a 'real' Device
- A consequence of the last point is that the Production Proving Function would not be able to use any DCC functionality to change Certificates in supplier or Network Operator Trust Anchor Cells (including CoS), as it would not be allowed any valid Certificates for such changes. The DCC could, however, test change of ACB and WAN Provider credentials on PP Devices (since those end Certificates are valid, and so the valid SMKI root could load on PPDs). The DCC can already do this as it is already permitted to commission Communications Hub Functions for production proving purposes
- What the above also means is that only a Production Proving Function could control its own PP Devices (since it is using its own Production Proving Function keys) in the role of suppler or network party and those are the only Devices it could control in this capacity. Further, other valid DCC Users could not control these PP Devices in these roles
- SMKI WAN provider, access control broker and SMKI Root and Recovery Certificates would still be injected onto Devices as per the current production solution
- The Production Proving Function will sign PP Registration Data files with self-generated private signing keys for which it has previously requested and been issued with corresponding SMKI file signing certs by the TSP. This would enable Production Proving Function to submit valid PP Registration Data Files. However to enable this and to ensure that such keys and certificates cannot be used in relation to any live Registration Data, the TSP would need to add a new Remote Party Role (pPRDPFileSign).