This document has been redacted to remove any commercially sensitive information and is now classified as DCC Public.

Should you have any queries, please contact Commercial@SmartDCC.co.uk

SCHEDULE 3

DCC REQUIREMENTS

1. INTRODUCTION

1.1 This Schedule 3 sets out the DCC Requirements as follows:

1.1.1 Paragraph 3: Functional requirements;

1.1.2 Paragraph 4: Non-functional requirements which shall be applicable at all times during the performance of this Agreement;

1.1.3 Paragraph 5: Non-functional requirements which shall be applicable during the Mobilisation Phase;

1.1.4 Paragraph 6: Non-functional requirements which shall be applicable during the Development Phase;

1.1.5 Paragraph 7: Non-functional requirements which shall be applicable during the Transition to Live Phase; and

1.1.6 Paragraph 8: Reports which shall be delivered as set out in that paragraph.

1.2 The Contractor shall, and shall ensure that the Services shall, deliver and comply with the requirements set out in this Schedule 3.

2. CHANGES TO THE REQUIREMENTS

2.1 Subject to Paragraph 2.2, the Parties acknowledge and accept that all changes to the requirements set out in this Schedule 3 shall be subject to the Variation Procedure.

2.2 The Parties acknowledge and accept that all changes to the requirements set out in Paragraph 3 shall be agreed pursuant to the procedure set out in, or agreed pursuant to, Schedule 4 *(Agile Development Methodology)* (and not subject to the Variation Procedure).

3. FUNCTIONAL REQUIREMENTS

3.1 The Contractor shall provide the Services in accordance with Schedule 4 *(Agile Development Methodology)* so as to meet the functional requirements set out in this Paragraph 3.

3.2 The Parties shall comply with the procedure set out in Schedule 4 (*Agile Development Methodology*) to agree the Detailed Requirements.

3.3 If there any conflict between the requirements set out in this Paragraph 3 and the Detailed Requirements, the Detailed Requirements shall prevail.

3.4 For the purposes of construing this Schedule 3 the following acronyms shall have the meaning set opposite them:

- PPMID - Prepayment Interface Device;

- SMETS1 - Smart Metering Equipment Technical Specification 1;
- SMSO - Smart Meter Systems Operator;
- UTRN - Unique Transaction Reference Number;
- CSP - Communications Service Provider;
- DSP - Data Service Provider;
- DCC - Data Communications Company;
- SEC - Smart Energy Code;
- SMKI - Smart Metering Key Infrastructure;
- SLA - Service Level Agreement;
- HA - High Availability;
- HVAC - Heating, Ventilation and Air-conditioning;
- RTO - Recovery Time Objective;
- RPO - Recovery Point Objective;
- SMWAN - Smart Metering Wide Area Network;
- S1SP - SMETS1 Service Provider;
- DUIS - DCC User Interface Specification;
- IEPFR - Initial Enrolment Project Feasibility Report;
- EUI-64 - 64-bit Extended Unique Identifier (IEEE unique identifier);
- IHD - In-Home Display;
- IP5B - Integration Path (option) 5B.

If any capitalised expression used in this Schedule 3 is not defined in the Agreement, then it shall be given the meaning ordinarily given to it in connection with (as the case may be) the Smart Metering Programme and / or the provision of information technology services that are the same as or similar to the Services.

3.5 **Technical Functional Requirements**

The Contractor shall provide the Services in accordance with Schedule 4 *(Agile Development Methodology)* to meet the following technical functional requirements and to deliver an Enduring Service that will operate in accordance with such technical functional requirements:

No	Description
1	develop functionality to support the processing of the service requests received via the SMETS1 service request interface (including responses and alerts).
1.1	process service request responses and alerts (critical)
1.101	receive countersigned SRV from DSP/Alternative-DSP
1.127	check that the countersigned SRV is valid and well-formed
1.102	check validity of DSP/Alternative-DSP countersignature (cryptographic protection)
1.109	check validity of the certificate used for cryptographic protection
1.128	check user signature (cryptographic protection)
1.129	check target device ID is addressable and is capable of receiving SRV
1.104	send acknowledgement to DSP/Alternative-DSP
1.130	confirm that request meets SRV specific DUIS requirements
1.107	confirm that the SMI status of the device is one of the following: i) commissioned ii) installed not commissioned iii) pending iv) whitelisted
1.110	confirm User is an Eligible User by checking if same as in SMI: i) registration data ii) Device ID iii) MPxN
1.111	validate time
1.114	check aberrant values in the countersigned SRV
1.115	validate countersigned SRV counter to check greater than last for this SRV received for the device
1.131	on counter error, create and send SMSO alert including error code to DSP/Alternative-DSP
1.117	construct SMETS1 device command
1.118	send SMETS1 device command
1.119	receive SMETS1 device response
1.120	construct service response incorporating request ID, SR and SRV from original SRV and success code
1.132	on error, send service response including error code to DSP/Alternative-DSP
1.121	sign service response
1.122	send signed service response to DSP/Alternative-DSP
1.126	receive synchronous and asynchronous acknowledgement responses from DSP/Alternative-DSP via the DSP-SMSO interface
1.2	process service request responses and alerts (non-critical)
1.206	receive countersigned SRV from DSP/Alternative-DSP
1.207	check that the countersigned SRV is valid and well-formed
1.208	check DSP/Alternative-DSP countersignature (cryptographic protection)
1.209	check validity of the certificate used for cryptographic protection
1.210	check user signature (cryptographic protection)
1.211	check target device ID is addressable and is capable of receiving SRV
1.212	on counter error, create and send SMSO alert including error code to DSP/Alternative-DSP

No	Description
1.213	send acknowledgement to DSP/Alternative-DSP
1.214	construct SMETS1 device command
1.215	send SMETS1 device command
1.216	receive SMETS1 device response
1.217	construct service response incorporating request ID, SR and SRV from original SRV and success code
1.218	on error, send service response including error code to DSP/Alternative-DSP
1.219	sign service response
1.220	send signed service response to DSP/Alternative-DSP
1.126	receive synchronous and asynchronous acknowledgement responses from DSP/Alternative-DSP via the DSP-SMSO interface
1.3	CoT & CoS
1.317	follow requirements in Section 1.2 above to process non-critical SRVs when a CoT is received
1.301	continue to execute the SMETS "Restrict Data" command for CoT in response to countersigned SRV 3.2, or develop functionality if not
1.318	receive countersigned SRV from DSP/Alternative-DSP
1.319	check supplier signature in SRV (is valid, is a supplier)
1.320	validate SRV and apply access controls as per SMETS1 critical SRV Processing requirements in Section 1.1 above
1.302	extract and store Entity ID from DS, KA and KA top up certs received
1.321	extract and store new supplier originator counter floor value (all SRVs, except 2.2 top up device)
1.322	extract and store supplier prepayment floor sequence number (All SRVs, except 2.2 top up device)
1.323	if key refresh is required on CoS, construct SMETS1 device command
1.324	construct service response incorporating request ID, SR and SRV from original SRV and success code
1.325	on error, send service response including error code to DSP/Alternative-DSP
1.326	sign service response
1.327	send signed service response to DSP/Alternative-DSP
1.328	receive synchronous and asynchronous acknowledgement responses from DCC-SMSO/S1SP interface
2	the service shall notify the SMETS1 user interface service of any service request that fails access control
2.1	notify service request access control failure
2.101	notify SMETS1 user interface service rejected requests
3	the service shall reject countersigned SRVs that fail access control.
3.1	reject countersigned SRV on access control failure
3.101	reject countersigned SRV on access control failure
3.102	log rejected countersigned SRV that have failed access control
3.103	send SMSO alert to notify countersigned SRV that have failed access control
4	the service should perform attribute-based anomaly detection on commands at the closest possible point to transmission over the

No	Description
	WAN
4.1	perform anomaly detection
4.102	defend against aberrant values in critical countersigned SRVs received
4.103	implement monitoring of originator counters and only execute countersigned SRVs in ascending order
4.104	must not execute more than one countersigned SRV at a time per target device
4.105	apply attribute based anomaly detection to device commands (not xml)
4.107	develop functionality to enable execution of SMETS1 "Restrict Data" command, in response to countersigned SRV 3.2
5	the service shall suspend processing of any service request that fails anomaly detection pending authorisation from the anomaly detection service to further process that service request
5.1	suspend the processing of a service request on anomaly detection failure
5.101	detect anomaly
5.102	detect access
5.103	reject countersigned SRV
8	the SMSO systems should be able to send acknowledgement for each countersigned SRV that has been received
8.1	send acknowledgement for each countersigned SRV received
8.101	send acknowledgement to DSP/Alternative-DSP on receipt of a countersigned SRV
10	develop functionality to support the mapping of device responses in to standard service response format, containing the response as an MMC formatted payload.
11	develop functionality to support the mapping of unique device alerts to common device alerts
11.1	map unique device alerts to common device alerts
11.101	use stored EIDs to route SMSO alerts triggered by a device alert (can use OriginatorID when alert is related to a countersigned SRV received) - move to alerts section
12	integrate with the SMETS1 service request interface to enable the transmission of device alerts to users
12.1	integrate with the SMETS1 service request interface
13	integrate with the UTRN service to enable the transmission of SMSO-generated UTRNs
13.1	enable UTRN service
13.103	receive countersigned SRV from DSP/Alternative-DSP
13.113	check that the countersigned SRV is valid and well-formed
13.114	check DSP/Alternative-DSP countersignature (cryptographic protection)
13.115	check validity of the certificate used for cryptographic protection
13.116	check user signature (cryptographic protection)
13.117	check target device ID is addressable and is capable of receiving SRV
13.118	on counter error, create and send SMSO alert including error code to DSP/Alternative-DSP
13.104	calculate UTRN based on top up value in the countersigned SRV 2.2 (If CV2 or CV3, extract top up value from UTRN data item

No	Description
	and calculate UTRN. If CV1 do not calculate UTRN)
13.105	generate SMSO alert containing UTRN and ResponseID derived from RequestID in SRV (CV2 or CV3 only)
13.106	send SMSO alert containing UTRN (CV2 or CV3 only)
13.119	generate device command (s) containing UTRN (extracted from SRV for CV1 or as calculated for CV2) (CV1 or CV2 only)
13.107	send device command(s) including to read device date-time to ESME or GSME (CV1 or CV2 only)
13.108	receive response(s) including device date-time from ESME or GSME (CV1 or CV2 only)
13.109	create service response using RequestID, SR & SRV from original SRV, device date-time and device response (to top up command)
13.110	where device date-time is not provided, create service response using RequestID, SR & SRV from original SRV, without device date-time device response (to top up command)
13.111	sign service response
13.112	send service response to DSP/Alternative-DSP
13.120	receive meter notification of the successful application of UTRN entered locally including receipt of the locally entered UTRN
13.121	generate device alert to notify local UTRN acceptance, look up TargetID in registration data, generate originator counter and include UTRN in body
13.122	send a device alert to DSP/Alternative-DSP (locally entered UTRN only)
15	integrate with the service management interface to enable exchange of incident, problem and change tickets
15.1	integrate with the SMETS1 service management interface
16	integrate with SMETS1 service management interface to enable exchange of data extracts from the smart metering inventory and registration database, communications hub device pre-notifications, communications hub status and communications hub diagnostic data
16.1	integrate with the SMETS1 service management interface
17	data processing: ensure adherence to the data processing and privacy policy in the role of both data processors and data controller
17.1	ensure compliance with data processing and privacy policy
18	the SMSO/S1SP systems should be able to receive a bulk firmware update countersigned SRV
18.1	receive a request for firmware update
18.101	implement fully the 2 stage process supported by the meter (SRV 11.1 to trigger SMETS1 firmware distribution and SRV 11.3 trigger activation, as for SMETS2)
18.102	mimic the behaviour of the 2 stage process if not supported by the meter
18.103	manage meters that are capable of supporting a 2 stage update process and store a hash of the firmware image (SRV 11.1) pending receipt of SRV 11.3
	receive & validate firmware update (Stage 1)
18.110	receive distribute firmware image web service request from DSP/Alternative DSP

No	Description
18.111	validate 'FirmwareImage' data item. i) perform validation checks as per CSP validation rules, except image size (ref: DUIS N18, N21, N22, N23); ii) perform additional validation of OTA header in FirmwareImage to check device model attributes in CPL (for the manufacturer image hash supplied in the upgrade image) are a match for the target device; iii) perform additional validation checks where required.
18.115	validate list of target devices
18.116	confirm that first device listed is recognised by SMSO/S1SP
18.117	on success, lookup stored supplier DS certificate serial number for target device (or for ESME associated with CHF if target device is communication hub) and retrieve supplier DS certificate
18.119	verify signature in GBCS upgrade image using retrieved supplier DS certificate
18.139	on successful validation of the first device, validate subsequent listed devices based on stored DS certificate serial number for that device (or ESME)
18.120	generate list of devices that failed validation (either not recognised or certificate mismatch)
18.121	send an SMSO alert response to DSP/Alternative DSP (error code and failed device IDs included in JSON payload)
18.122	stop all SMSO/S1SP processing if FirmwareImage fails validation
18.123	distribute manufacturer image and retain image hash and firmware version extracted from OTA header against all valid target devices (if standalone distribution supported by device and no contention with in-flight firmware distribution to the communication hub)
18.124	receive successful acknowledgement of the receipt of Image by the device
18.125	where a device does not support 2-stage firmware update process, store manufacturer image and firmware version extracted from OTA header against list of target devices that passed validation
18.126	generate and sign firmware distribution receipt alert (MMC output format payload) as SMSO alert
	activate firmware update (Stage 2)
18.128	follow SMETS1 critical SRV processing [during validation of device status ""Suspended"" is a permissible state]
18.129	check that a hash or image for the target device is stored
18.130	check image hash contained in countersigned SRV 11.3 is a match for most recent stored hash/hash calculated from last stored image for target device
18.131	on error, create and send 'Activate Firmware Response' (MMC output format payload) with error code (ref: GBCS 11.5.2)
18.132	construct firmware activation device command for immediate execution (including firmware image where device is not capable of storing image)

No	Description
18.133	send firmware activation device command
18.135	receive device response
18.136	construct and sign 'Activate Firmware Response' (MMC output payload format) [response payload includes success or failure response code plus firmware version for image that is now active non device (stored by SMSO/S1SP for image that was sent and successfully activated, or extracted from SMI data where firmware activation failed)]
18.138	send signed 'Activate Firmware Response' to DSP/Alternative-DSP
19	enrolment design
19.1	pre-enrolment
19.2	enrolment & installation
19.201	receive countersigned SRV from DSP/Alternative-DSP to add a device to the HAN device log
19.206	apply validation, cryptographic protection, access control and anti-replay
19.207	check if the device is not on a different HAN
19.208	send SMSO alert on error and stop processing
19.202	if the device being added is not already on the specified HAN, send "add device to CHF device log" command
19.203	receive response from device confirming device ID added to device log
19.209	create and sign service response confirming device ID added to HAN device log
19.204	send service response to DSP/Alternative-DSP confirming device ID added to device the log
19.209	if the device being added is not already on the specified HAN, wait for a confirmation from the communications hub that the device is communicating on the HAN or if timed out
19.210	Create SMSO alert to inform that the device is communicating on the HAN or timed out
19.211	where target device is ESM, GSM or GPF, reject countersigned SRV validation if the supplier remote party and network operator remote party is already known for the target device
19.212	where target device is ESM, GSM or GPF, extract and store entity IDs from supplier certificates, supplier DS certificate serial number, supplier (originator counter) floor sequence number, supplier prepayment top up floor sequence number
19.213	where target device is ESM, GSM or GPF, extract and store entity IDs from network operator certificates, network operator DS certificate serial number, network operator (originator counter) floor sequence number
19.3	commissioning
19.303	receive countersigned SRV for processing from DSP/Alternative-DSP
19.304	perform validation checks as per non critical SRV processing (See Section 1.2)
19.305	create and send device command to synchronise clock
19.306	receive response from device
19.307	send service response to DSP/Alternative-DSP

3.6 **Security Functional Requirements**

The Contractor shall provide the Services in accordance with Schedule 4 *(Agile Development Methodology)* to meet the following security functional requirements and to deliver an Enduring Service that is capable of operating in accordance with such security functional requirements:

No	Description
20	support a DCC security audit to document as-is controls to enable the required level of system hardening to be determined
20.1	system hardening
20.101	to provide the necessary information, and access to personnel and systems required, to enable DCC and its representative to gain a detailed understanding of the existing technical and security controls in place and their configuration
20.102	to validate the technical correctness of the background and system/process descriptions on which the audits are based
20.103	to use the audit to identify what vulnerabilities exist and what measures would be the most appropriate to improve the security of the system
20.2	system islanding
20.201	if sufficient security can't be achieved by other controls, need to split the system into multiple islands, each of a sufficiently small size (this is an option of the last resort, other security options would be preferred due to the cost implication)
21	implement required system hardening controls that result from the DCC security audit
21.1	additional system hardening
21.101	conduct an impact analysis to identify the cost and timescales associated with implementing the recommended hardening controls
21.102	follow the audit to implement the recommendations from the audit based on the risk-managed approach specified by DCC
22	interface to a security service to enable cryptographic controls between the SMSO and the meter
22.1	DCO (Dual Control Organisation)
22.101	to implement a bi-direction connection from the head end system to an external DCC organisation (the DCO) with which to exchange messages and cryptographic material prior to communicating with the meter
22.102	communicate meter messages along with the original supplier messages, and potentially cryptographic material, to the DCO for validation, authorisation and/or modification prior to the transmission to meter. Pending the output of the proof-of-concept study, the DCO may implement the message encryption on behalf of the SMSO
22.103	to ensure that all communications with the DCO are strongly authenticated
22.104	to validate the responses that are returned from the DCO
22.105	to comply with the DCO code of connection
22.106	to enable encrypted messages to pass from the head end system

No	Description
	to meter
22.107	to use strong cryptography to encrypt messages to and from meters
22.108	to use unique keys to each meter and to store the keys securely
23	support SMKI user authentication via DSP - the supplier signature of each SMETS1 message will be validated by the SMSO
23.1	support SMKI authentication
23.101	validate the supplier, DSP and/or DCO signatures of each SMETS1 message, including the signing certificate, full certification path up to the trust point and any revocation information available
23.102	verify the digital signature of the received message against the public key recorded in the organisation's SMKI certificate
23.103	verify the digital signature of the received message against the content of the message
23.104	ensure that the trust point is securely held and its integrity maintained and secured
23.105	to reject any messages that do not have a valid digital signature
23.106	perform authorisation controls on the supplier against the DSP registration data
23.107	for critical message, perform authorisation controls on the supplier ID against that stored from the change of supplier operation
24	support for CSP limitation controls
24.1	support for CSP Limitation controls
24.101	ensure SMSO system should 'fail gracefully' if CSP network restricts the number of connections to less than required by SMSO
25	compliance with SEC Section G security controls
25.1	compliance with SEC Section G security controls
25.101	Section G (Security) shall have effect from the date on which this code is first modified to include that Section
26	support a service request log and reporting service
26.1	support service request log & reporting service
26.101	capture logging of service requests
26.102	baseline normal operations
26.103	construct reporting to show abnormal activities
26.104	review regularly
27	support an access request log and reporting service
27.1	support an access request log & reporting service
27.101	capture logging of service requests
27.102	baseline normal operations
27.103	construct reporting to show abnormal activities
27.104	review regularly
28	support an ongoing security assurance process
28.1	support an ongoing security assurance process
28.101	provide information and access as required to an independent security assurance process
28.102	provide real-time events and alerts to an external security monitoring service, if required
28.103	perform regular review of security situation

No	Description
28.104	report any changes to systems
28.105	mitigate where appropriate
29	implement a secure connection to the DSP in accordance with the DSP connection requirements
29.1	implement a secure connection to the DSP in accordance with the DSP connection requirements
29.101	connect to DSP using transport layer security
29.102	use DCCKI issued X509 certificate to enable connections to be mutually authenticated
29.103	reject connections that fail authentication
29.104	conform to the DSP Code of Connection
30	remove external third party connections other than those third parties in the DCC SMETS1 architecture
30.1	remove external third party connections other than those third parties in the DCC SMETS1 architecture
30.101	support connections to the DSP, DCO, CSP(s), and any additional connections in the DCC SMETS1 architecture that have been approved by the DCC
30.102	SMSO SMETS1 system does not have any direct connections to supplier systems except for DCC approved temporary/transitional arrangements while enrolment of meters takes place
30.103	remove any additional network or organisational connections not identified in 30.101, without adversely affecting the functionality, performance, resilience or security of the system
30.104	use a dedicated network that is segregated from the SMSO corporate network and any SMETS2 systems to perform the administration of the SMETS1 system
30.105	if an SMSO continues to operate unenrolled meters after the enrolment transitional period in 30.102, this will require a dedicated system separated from the DCC-enrolled meter system

3.7 Service Performance Functional Requirements

The Contractor shall provide the Services in accordance with Schedule 4 *(Agile Development Methodology)* to meet the following service performance functional requirements and to deliver an Enduring Service that is capable of operating in accordance with such service performance functional requirements:

Description
The Enduring Service shall be developed such that at as a minimum level of service the Enduring Service shall perform in accordance with service levels currently in place between all relevant DCC Service Users and the Contractor.
Service Performance Model: Availability • High Availability: · target service level 99.95%; minimum service level 99%; • Enduring Service should be HA within a DC and HA across DC;

Description
• No single point of failure at HVAC; • No single point of failure in power delivery ; • The Enduring Service shall be recoverable within a specified time in the event of its non-availability - RTO 4h; • The Enduring Service shall lose no more than a specified amount of data in the event of an incident – RPO 15mins.
Service Performance Model: Scalability: • Dynamic/auto scalability; • Schedule scalability; • Ability to remove growth capacity, post scaling event.
Service Performance Model: Latency: • Minimise latency; • Provide transaction timestamps; • Transaction latency monitoring and reporting.
Service Performance Model: Capacity (Target) • Baseline Enduring Service = 700 Transactions (Service Request) per second; • Peak transaction = 800 per second.

4. NON-FUNCTIONAL REQUIREMENTS – GENERAL

4.1 The requirements set out in this Paragraph 4 will apply at all times during the Term.

Requirement	Description
Project Management	• The Contractor shall ensure that all aspects of project management are carried out in accordance with and reflect Good Industry Practice. • As part of the Services, the Contractor shall provide project management services in accordance with Good Industry Practice for the following Phases:- o Mobilisation Phase; o Development Phase; o Transition to Live Phase. • The Contractor shall provide such additional project management services as are required to implement each Variation.
Risk Management	• The Contractor shall monitor and formally report to the DCC on Services risks and issues at regular and

Requirement	Description
	agreed intervals and through mechanisms agreed with the DCC, or, in the absence of any such agreement, in accordance with Good Industry Practice. • The Contractor shall implement, operate and maintain a joint risk and issue management process, which shall include processes to identify, assess, monitor, mitigate and control risks and issues and to communicate such risks and issues to the DCC in accordance with Good Industry Practice.
Documentation Management	• By completion of the Development Phase, the Contractor shall provide and maintain a full and up-to-date version controlled documentation set for the Enduring Service which shall include the following categories of documents:- ○ system documentation; ○ service design documentation – a version of the service design shall be captured and kept at a minimum for the original solution design, the original solution implementation, major solution releases and the current solution; ○ testing documentation; ○ implementation documentation; ○ service management documentation; ○ standards compliance; ○ project management documentation; ○ training documentation; ○ business continuity and disaster recovery documentation; ○ end user guides and manuals; and ○ any other documentation reasonably required to meet the requirements set out in the Agreement or as otherwise would be required in order to comply with Good Industry Practice. • During the Development Phase the Contractor shall in accordance with, to the extent applicable, Schedule 4 *(Agile Development Methodology)*: ○ comply with the agile software development principles of "just enough documentation with enough information" to progress the delivery of the Services iteratively throughout the period of the Project Plan. ○ prepare and maintain, in accordance with Good Industry Practice, agile development artefacts including as required to demonstrate control of the

Requirement	Description
	Services and progress against the Project Plan. ○ prepare and maintain documentation that supports the design, delivery, deployment, testing and support aspects of the Services. ○ ensure that, based on the agile development methodology approach or approaches agreed between the DCC and the Contractor, documents will be added to the deliverables log and tracked against delivery by the Contractor to the DCC of working software. ○ ensure that all Documentation will be sufficient to support third party activities outside of development and / or the Services and / or inform key stakeholders, as required. • The Contractor shall ensure that all Documentation shall be free from any IPR restrictions that may prevent the DCC from benefiting from the IPR rights granted to it under the Agreement. • The Contractor shall ensure that all Documentation is placed in a shared area that is available to, and accessible by, the DCC and its staff and the designated staff of any approved DCC Sub-contractor.
Security Audit	The Contractor shall take all reasonable steps to support a DCC security audit in order to document "as-is" controls to enable the required level of system hardening to be determined.
Service Performance Review	The Contractor shall undertake a review of current service performance capability, including a gap analysis relative to the DCC service performance model described in Paragraph 3 (*Functional Requirements*) and an assessment of the technical feasibility and cost to achieve the DCC's preferred Enduring Service performance model including as identified in Paragraph 3.7 (*Service Performance Functional Requirements*).

5. NON-FUNCTIONAL REQUIREMENTS – MOBILISATION PHASE

5.1 The requirements set out in this Paragraph 5 will apply at all times during the Mobilisation Phase.

Requirement	Description
Mobilise	The Contractor shall: • with a focus on scope and initial planning, mobilise its

Requirement	Description
	team as quickly as reasonably practicable and in any event in accordance with any Milestones or other timescales agreed under the Agreement including in the Project Plan; • configure the development and test environments and connect to third party systems as required; • establish the initial Project Plan, backlog or equivalent using preferred tools (MSP, Jira, etc.) and in accordance with the provisions of Schedule 15 (*Project Plan*); • establish governance, reporting and other agile project management mechanisms and processes as applicable to the agile development methodology approach or approaches agreed between the DCC and the Contractor; • scope and plan the initial iterations in accordance the agile development methodology approach or approaches agreed between the DCC and the Contractor; • carry out any other activities required to enable development and delivery.

6. NON-FUNCTIONAL REQUIREMENTS – DEVELOPMENT PHASE

6.1 The requirements set out in this Paragraph 6 will apply at all times during the Development Phase.

Requirement	Description
Software design, build and test process	The Contractor shall: • support DCCs iterative development of the high-level design of the Software; • carry out iterative development of the detailed design of the Software; • carry out continuous integration; • support the creation of automated testing; • make available progress tracking (ideally browser views), Jira boards, burn up/down charts and velocity charts and such other progress tracking reporting as may be required by the DCC.
Service management and performance monitoring	The Contractor shall: • support the DCC in the selection of third party tools to be used to aid service management, performance monitoring, and incident and problem resolution in

Requirement	Description
design	connection with the Enduring Service; • design the Enduring Service so that it incorporates tools for service management, performance monitoring, and incident and problem resolution; • design the Enduring Service so that DCC selected third party tools to be used to aid service management, performance monitoring, and incident and problem resolution are incorporated.

7. NON-FUNCTIONAL REQUIREMENTS – TRANSITION TO LIVE PHASE

7.1 The requirements set out in this Paragraph 7 will apply at all times during the Transition to Live Phase.

Requirement	Description
Release management	The Contractor shall ensure that it carries out the Services to: • align with and support the DCC test assurance process; • align with and support the DCC release management process; • resolve issues identified in a timely fashion.
Service Catalogue development	• The Contractor shall publish a service catalogue in the form of detailed service descriptions and capability lists, with each defined where reasonably possible as a standard change.

8. REPORTS

The Contractor shall prepare and deliver the following reports to the DCC in accordance with Good Industry Practice and by the relevant Milestone Dates:

8.1 Report 1 - A high level report, including presentation, distinguishing where appropriate, by meter type and by delivery option, to cover the following:-

Report Section	High level Proposals for:
Security	Technical and service impacts of: • authentication across interfaces; • section G compliance; • system hardening;

Report Section	High level Proposals for:
	• DCO; • islanding; and • provision of interfaces for any 3rd party organisation that DCC might require in order to apply security controls.
Message Handing	Technical and service impacts of: • consuming DUIS Service Requests (both core and elective, per the design baseline as set out in the draft SEC (including Subsidiary Documents)); • managing outputs in terms of MMC service responses; • managing alerts (both those originating from devices and those that arise as a consequence of SMSO processing); and • SMSO processing timescales.
Service Capability	Technical and service impacts of: • any CSP network limitations on the implementation; • any concerns with service availability; • business continuity and disaster recovery and reporting; and • Any scaling capacity concerns and any necessary constraints
Development of Solution	• velocity of development to provide confidence on release timescales; • providing confidence in quality of development
Project Plan	• An initial project plan for entry into and out of testing, in particular proposed initial dates for the milestones related to testing and go live to meet all the requirements, with the exception of: o system hardening; o DCO; o Islanding. • The following are each to be the subject of a separate plan:

Report Section	High level Proposals for:
	○ system hardening; ○ DCO; ○ Islanding. This initial project plan shall set out the major: ○ Risks/issues & mitigations ○ Dependencies ○ Assumptions • The report shall set out timescale ranges where required • The report shall make clear the level of confidence the Contractor has in the proposed timescales.
Cost	• The cost for the development of the Enduring Service. • The cost for the delivery of the Enduring Service expressed as a price per meter per annum. • Each cost (development and enduring) is to be presented as a base cost to meet all the requirements, with the exception of: ○ system hardening; ○ DCO; ○ Islanding. • The following are each to be costed as independent increments on the base cost: ○ system hardening; ○ DCO; ○ Islanding. • The report shall set out cost ranges where required • The report shall set out any assumptions • The report shall make clear the level of confidence the Contractor has in the proposed costs.

8.2 Report 2 - A detailed report (supported by presentations and demonstrations), distinguishing where appropriate, by meter type and by delivery option, to cover the following:-

Report Section	Detailed Proposals for:
Security	• authentication across interfaces; • a gap analysis and delivery plan for Section G compliance; • proposals and a delivery plan for system hardening; • results of the feasibility analysis for a DCO (and delivery plan if applicable); • results of the feasibility analysis for Islanding (and delivery plan if applicable); and • provision of interfaces for any 3rd party organisation that DCC might require in order to apply security controls.
Message Handing	• consuming DUIS Service Requests (both core and elective, per the design baseline as set out in the draft SEC (including Subsidiary Documents)); • managing outputs in terms of MMC service responses; • managing alerts (both those originating from devices and those that arise as a consequence of SMSO processing); and • SMSO processing timescales.
Service Capability	• confirmation that there is no impact from the implementation of CSP network limitations; • service availability; • business continuity and disaster recovery and reporting; • scaling capacity and any necessary constraints.
Development of Solution	• velocity of development to provide confidence on release timescales, supported by demonstrations; and • providing confidence in quality of development.
Project Plan	• A detailed project plan for entry into and out of testing, in particular firm dates for the milestones related to testing and go live to meet all the requirements, with the exception of: ○ system hardening;

Report Section	Detailed Proposals for:
	○ DCO; ○ Islanding. • The Contractor shall propose indicative Milestone Dates in accordance with Paragraph 7 of Schedule 15 (*Project Plan*). • The following are each to be the subject of a separate plan: ○ system hardening; ○ DCO; ○ Islanding. • The report shall sets out the: ○ Risks/issues & mitigations ○ Dependencies ○ Assumptions • The report shall make clear the level of confidence the Contractor has in the proposed timescales.
Cost	• The detailed cost for the development of the Enduring Service. • The detailed cost for the delivery of the Enduring Service, including expression as a price per meter per annum. • Each cost (development and enduring) is to be presented as a base cost to meet all the requirements, with the exception of: ○ system hardening; ○ DCO; ○ Islanding. • The following are each to be costed as independent increments on the base cost: ○ system hardening; ○ DCO;

Report Section	Detailed Proposals for:
	○ Islanding. • The report shall set out any assumptions • The report shall make clear the level of confidence the Contractor has in the proposed costs.
Commercial	• The report shall clarify any commercial/contractual impacts (other than price)