Data Communications Company

Change of supplier credentials - DCC solution review

Options assessment

Date: 1 April 2019

Classification: DCC Controlled – BEIS and SEC Parties only

Table of Contents

1 Executive Summary

Purpose

The Change of Supplier credentials (CoS) process allows the supplier certificates associated with a losing energy supplier to be replaced with those of a gaining energy supplier whenever a consumer changes supplier. DCC Systems were originally developed to operate using a Transitional CoS (TCoS) process during the roll-out of Smart meters to minimise the impact on suppliers during this critical period, although it was recognised at the time that this was only a temporary solution.

Once rollout is complete the TCoS process must be replaced with a more resilient and secure Enduring CoS (ECoS) solution. There are two options available for implementing an ECoS solution:

- **ECoS 1:** CoS events are validated, processed and executed by the losing supplier.
- **ECoS 2:** CoS events are validated, processed and executed by a centralised CoS Party service provider.

This paper provides a quantitative and qualitative evaluation of the impacts of each of these options on DCC and market participants based on an assessment of the technical solution, along with the associated costs and risks.

Recommendation

DCC recommends that ECoS 2 should be selected for implementation.

Justification

DCC's evaluation of the two ECoS options based on the available evidence indicates that ECoS 2 provides a better solution across almost all the evaluation criteria used. The estimated operating costs shown below do not include supplier costs, which means that these are likely to be significantly understated for ECoS 1:

Solution option	Estimated implementation costs	Estimated operating costs (per annum)	Implementation timescales	Overall risk rating
ECoS 1	£174.0M - £225.2M	£0.9M - £1.2M[1]	48 months	High
ECoS 2	£37.8M - £50.1M	£2.3M - £3.1M[2]	41 months	Medium

Overall, DCC's evaluation indicates that ECoS 2 represents a superior technical solution which provides better outcomes for both market participants and consumers, along with being more cost-effective and lower-risk.

[1] Insufficient operating cost data was provided by energy suppliers. All suppliers will need to operate a CoS service and it is likely that there will be operational costs associated with this. DCC considers it highly likely that the ECoS1 operating costs will be greater ECoS 2.
[2] Under ECoS 2 DCC will operate the CoS service. The operating costs used for ECoS 2 are likely to be more comprehensive than for ECoS 1, where suppliers will operate the CoS service but have not provided sufficient cost information to support an assessment.

2 Background

When the technical and security architecture that underpins DCC Systems was originally being developed, BEIS took the decision that DCC would implement a temporary solution to replace supplier certificates on a Device when a consumer changes their supplier, rather than an enduring solution implementing a process driven by the losing supplier.

This decision was taken on the basis that the underlying Trust Model agreed between BEIS, the National Cyber Security Centre (NCSC) and energy market participants relies on the losing supplier to fulfil the role of CoS Party, which makes them responsible for generating the command to replace the supplier certificates on affected Devices with those of the gaining supplier.

It was concluded that the changes required to implement the agreed Trust Model in full would result in a significant level of disruption to suppliers' systems and processes during the rollout of Smart meters, which could impair energy suppliers' ability to complete rollout within the required timescales.

It was recognised at the time that an enduring solution would need to be developed and implemented as soon as practicable, with the decision to implement a temporary solution being conditional on ensuring that an enduring solution is made available once rollout is complete.

The rollout of Smart meters is targeted to complete during 2020, at which point the original barrier to the development of an enduring CoS solution will no longer apply. This presents an opportunity to implement an enduring CoS solution to coincide with the re-procurement of the Data Service Provider (DSP) services, expected during October 2021.

Conceptually there are only two options for an enduring CoS solution. This paper provides a quantitative and qualitative assessment of each of those options, and seeks to provide BEIS with:

- A description of the changes to DCC Systems and processes that would be needed to implement an enduring solution (Appendices 1, 2, 5 and 6);
- An estimate of the rough order of magnitude of the costs that would be incurred, including both DCC and end-to-end costs (Appendices 1 and 5); and
- A description of anticipated impacts on energy market participants (Appendices 1, 2, 5 and 6); and
- Any other relevant observations, including DCC's views of the technical feasibility and risks of each option, how such risks could be mitigated.

To support this assessment, DCC conducted a Request for Information (RfI) to obtain indicative impact and cost information from energy suppliers, current and potential future service providers, and from within DCC. The information received has been used to undertake the analysis outlined in Section 4 of this paper.

3 Requirements

3.1 Solution requirements

The drivers of the Trust Model suggest the following set of key mandatory requirements which must be fulfilled by any option which is to be considered for implementation:

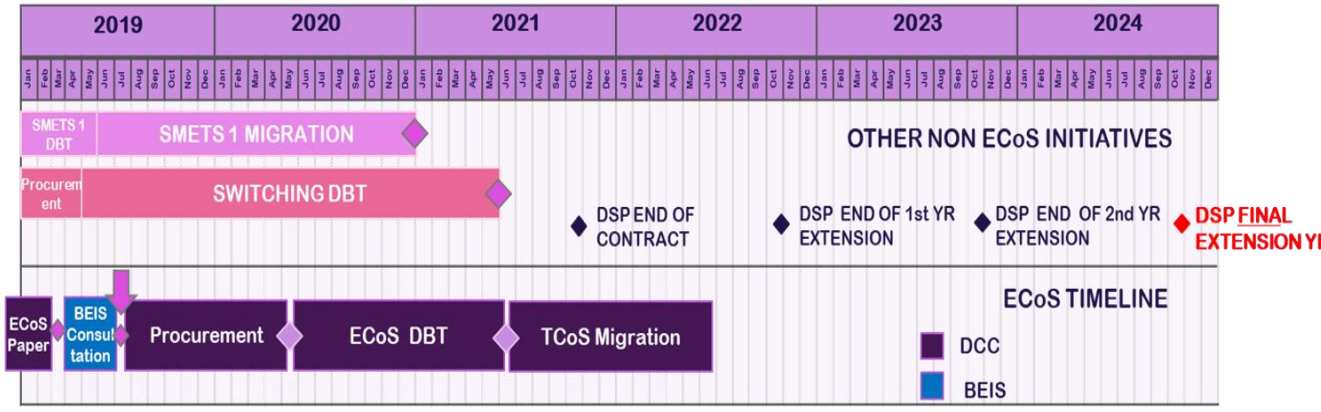
Requirement	Description	Rationale
1	The enduring solution must facilitate the change of supplier credentials relating to both SMETS1 and SMETS2 Devices.	To support the key industry events of a consumer choosing to switch Supplier, merger and acquisition activity between suppliers and the Supplier of Last Resort (SoLR) process.
2	The enduring solution must not affect the way that Devices operate, either during implementation or operation.	The impact of any need to change the hardware or firmware of installed Devices would be disproportionately large. Sufficient credential slots are available under existing Device specifications.
3	The CoS Party system must be Separate from other Systems, i.e. it must be subject to controls which ensure that no communication may take place between it and any other System, unless such communication is necessary for the intended operation of the System.	To ensure that any compromise of any of the other Systems which comprise the DCC Total System does not allow access to, or control of, the CoS Party system.
4	The CoS Party and Access Control Broker (ACB) must perform cryptographic protection checks on all data received.	To check that any data received originates from a valid and expected source.
5	The CoS Party and ACB must maintain individual reference data which is separate from other DCC Systems.	To verify legitimacy of CoS requests and ensure that any compromise of the reference data held within DCC Systems does not result in a compromise of the reference data held by the CoS Party.

Requirement	Description	Rationale
6	The CoS Party and ACB must operate using separate time-sources.	To prevent any compromise of the time-source resulting in a compromise of multiple systems, and to prevent any compromise of a time-source from going undetected.
7	The CoS Party and ACB must perform volume-based anomaly detection checks on CoS requests. Under a model which requires each losing supplier to fulfil the role of CoS Party, each supplier will need to perform such checks. Similar checks will also need to be carried out on the aggregated volume across all suppliers.	To identify anomalous system behaviour which could indicate a threat to, or compromise of, DCC Systems.
8	The enduring solution must support the change of CoS Party credentials on Devices.	This requirement ensures that the change of CoS Party functionality is incorporated into the solution so that CoS Party credentials can be completed using standard processes and functionality. This will also support the migration from TCoS to ECoS as a business-as-usual activity.
9	The CoS Party will need to be able to distinguish Devices of different technical specifications (SMETS1, SMETS2).	Each CoS request which relates to a SMETS2 Device will need to be translated into the form required by the Great Britain Companion Specification (GBCS). The transformation of a request to GBCS only applies to SMETS2 Devices, so the CoS Party will need to be able to distinguish Devices of different technical specifications.
10	The enduring solution must not impose undue or disproportionate costs or operational impacts on market participants.	Any enduring CoS solution must be cost effective in terms of both initial implementation costs and ongoing end-to-end costs.

3.2 Delivery requirements

Discussions between BEIS and DCC which took place at the outset of this assessment established that the procurement of an enduring CoS solution should commence ahead of the re-procurement of the DSP services in 2021. This would allow the migration of Devices to complete by mid-2022.

DCC originally estimated that the procurement and Design Build and Test (DBT) phases should each take around 12 months to complete[3]. The migration phase is expected to take around nine months to complete, with three months contingency time resulting in a total of 12 being allocated to this phase. The timeline below shows the target timescales for each phase of ECoS implementation in the context of other major DCC programmes:



It is expected that the existing TCoS functionality will be needed to perform the migration of Devices from TCoS to ECoS. Because of this there is a commercial imperative to complete TCoS migration prior to the current DSP contract expiring. DCC may need to extend the current DSP contract to support TCoS migration, or to ensure the continuity of other DCC Services during the transition to a new DSP contract. However, planning for the DSP re-procurement exercise is currently incomplete and it is not yet known by how long the DSP contract may need to be extended by.

In addition to this, DCC will need to consider ECoS alongside other activities managed using its change delivery capability during the target implementation window. This will include a full assessment of:

- Any risks which may arise if there are delays to the migration of SMETS1 Devices into the DCC ecosystem;
- Developments within the Faster Switching programme; and
- Any other change activities planned to take place during the target ECoS implementation window.

[3] This assumption has been made to support this analysis and does not constitute a forecast of delivery timescales, which may change during detailed planning.

4 Options analysis

4.1 Options

BEIS and the NCSC originally agreed an ECoS solution based on a model under which CoS events are validated, processed and executed by the losing supplier acting as the CoS Party. This decision was based in part on the assumption that a 'losing supplier' CoS model will be inherently more resilient due to increased diversity of the design of CoS Party systems as each supplier would take a different approach.

However, developments in the energy industry since the original policy decision was taken have prompted a review of the available options. Two of the most relevant developments are the growth in the smaller supplier market and the emergence of common DCC adapters across many suppliers, along with the progress made by Ofgem's Faster Switching programme to reduce the amount of time it takes for consumers to change energy supplier.

To access DCC Services, each User must develop or procure a DCC adaptor. It was originally expected that each supplier would use its own adaptor, resulting in many different adaptor designs being used across the market. Evidence from active Users indicates that the market is currently favouring the use of shared DCC adaptors, resulting in many suppliers using the same adaptor. If this behaviour were to be replicated when suppliers procure the required CoS Party solution, the assumption that a 'losing supplier' CoS model will be inherently more resilient due to increased diversity of design may prove to be incorrect.

Ofgem has expressed concerns that relying on the losing supplier to execute the CoS process may have a detrimental impact on the success of the Faster Switching programme by reducing the amount of control a gaining Supplier has over the CoS process. This increases the risk that the losing supplier may accidentally or deliberately frustrate the CoS process, resulting in a poor experience for consumers.

Energy suppliers have raised similar concerns, along with concerns relating to the impact on their systems and operational processes in terms of the changes required to support the 'losing supplier' solution and the need to share confidential information when configuring Anomaly Detection Thresholds (ADTs). Consequently, two enduring CoS (ECoS) options have been identified for assessment. The key difference between the two ECoS solutions is how the role of the CoS Party is undertaken:

- **ECoS 1:** This is the original solution agreed by BEIS and NSCS. CoS events are validated, processed and executed by the losing supplier acting as the CoS Party.
- **ECoS 2:** This is an alternative option intended to better support faster and more reliable switching in the energy market, along with reducing the impacts and costs on energy suppliers. CoS events are validated, processed and executed by a centralised CoS Party service provider. This is similar to the current TCoS solution, but with changes made to meet the mandatory requirements set out in Section 3.1.

Under the current TCoS solution the DSP fulfils the role of a centralised CoS Party but does not meet all the requirements of an enduring solution. The CoS Party and ACB do not maintain individual reference data, and some aspects of the CoS Party systems are integrated into other elements of the DSP systems, including the shared use of a time-source.

Because TCoS does not meet all the mandatory requirements, it cannot be considered as a candidate for an enduring solution without extensive modification. If TCoS were to be modified to meet the requirements set out in Section 3, it would effectively be the same as ECoS 2.

If BEIS does not direct DCC to procure either of the options set out in this paper, the only course of action available to DCC would be to procure a version of TCoS which has been modified to meet the mandatory requirements. This means that there is no 'zero-cost' option available. It is assumed that if DCC was to procure a replacement TCoS service, the costs would be of a similar magnitude to those associated with ECoS 2, resulting in the marginal cost of ECoS 2 being minimal.

4.2 Sources of impact and cost information

The impacts of moving to an enduring CoS model have been assessed in terms of the technical changes required to DCC and energy supplier systems. This assessment has been used to identify indicative cost impacts for affected Parties and systems, along with driving an evaluation of the complexity of implementing and operating each ECoS option. The information used in this analysis is only intended to provide an estimate of the rough order of magnitude of the costs of each ECoS option and should not be regarded as a cost forecast[4].

The cost impacts expected to arise as a result of the technical changes identified were obtained from the following sources:

- **DCC:** DCC implementation and operational costings were provided by DCC's Finance team. Implementation costs include an estimate of the DCC programme costs associated with each option based on anticipated resource requirements.

- **Suppliers:** Supplier cost information was obtained using a market-wide RfI. DCC received responses from seven suppliers comprising five Large Supplier Parties and two Small Supplier Parties. This represents a response rate of around 10% and lacks any data relating to medium-sized suppliers. In addition to this, the range of responses received varies significantly and does not provide any visibility of potential cost-efficiencies which may arise from the use of shared CoS Party solutions.

- **Third-party vendors:** Nine third-party vendors were engaged and asked to provide costs for the provision of a new centralised CoS Party service in response to the RfI. DCC received two submissions, one of which failed to fulfil all the requirements and has not been included in this this analysis. Three of the third-party vendors that did not provide submissions indicated that they would be willing to participate in a formal tender process, but not in a RfI which they regard as being speculative.

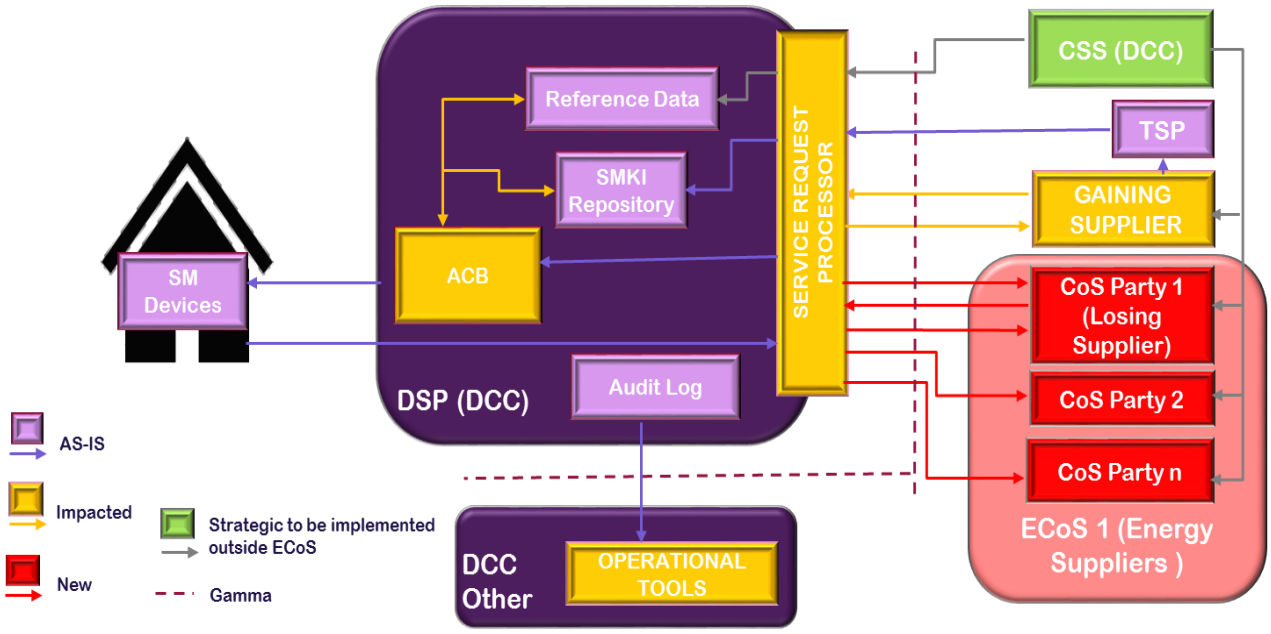
[4] Actual costs will be assessed as part of the procurement exercise.

4.3 Enduring Change of Supplier - Model 1

An overview of the ECoS 1 key characteristics and basic architecture is provided below. Further technical details of ECoS 1, along with the detailed architecture is provided in Appendix 9.

4.3.1 Overview

- CoS requests are validated, processed and executed by energy suppliers acting as the CoS Party for any CoS event where they are the losing supplier.
- Requires a new CoS interface with energy suppliers to allow them to act as CoS Party.
- Energy Suppliers will need to be involved in TCoS to ECoS migration when the CoS Party credentials on Devices within their estate need to be replaced. This is expected to done using existing TCoS functionality.
- In the event of a supplier failure an additional key that can be used to change supplier credentials will be required, otherwise any affected Devices may need to be replaced[5].



4.3.2 Impacts

The table on the following page summarises the impacts of ECoS 1 in terms of costs, operational impacts and complexity. Costs have been derived from the responses to the RfI conducted by DCC. Full details of the technical impacts and costs of ECoS 1 are provided in Appendix 1, with details of the operational impacts provided in Appendix 2.

The operational complexity of ECoS 1 has been assessed by comparing it with the baseline TCoS model. Technical complexity has been assessed in terms of implementation complexity based on system integration, timescales, migration and

[5] The cost of functionality to support the use of an additional key has not been assessed or included in this analysis.

number of parties impacted. The full results of this analysis, along with the scoring criteria used, are provided in Appendices 3 and 4.

Impacted Party	Implementation costs	Operating costs (per annum)	Operational complexity	Technical complexity
Suppliers	£143.2M - £184.1M	Insufficient data provided[6]	High	High
DCC[7]	£30.8M - £41.1M[8]	£0.9M - £1.2M[9]	Medium	High
Overall anticipated impact	£174.0M - £225.2M	£0.9M - £1.2M	High	High

The main implementation cost driver under ECoS 1 is the need for every energy supplier in the market to source, develop, or procure an instance of the CoS Party solution, along with the costs of integrating it with their back-end systems. This is also the main driver of technical complexity.

The main operating cost drivers arise from an increase in the cost of operating and maintaining DSP systems[10]. Operational complexity is mainly driven by:

- An increased need to coordinate business activities between suppliers;
- The need for each Supplier to amend its business operational processes to support acting as CoS Party;
- The need for each Supplier to establish and manage new commercial arrangements with CoS Party solution providers; and
- The need for each Supplier to operate and maintain new CoS Party interfaces.

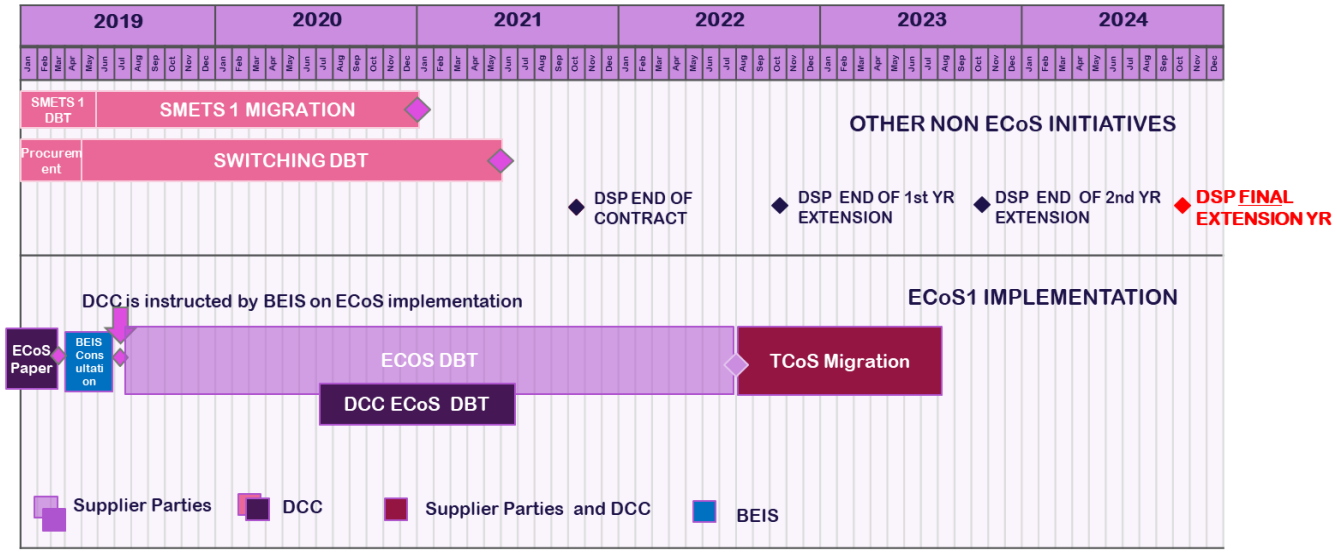
In the event of a supplier failure, access to the private key of the failed supplier may not be available. It is assumed that such a scenario would require an additional key that can be used to change supplier credentials, otherwise any affected Devices may need to be replaced. The existence of a single key which can be used to replace the supplier credentials on any Device undermines the assumption that a distributed CoS Party model should provide a more secure and resilient CoS service than a centralised CoS Party model.

[6] All suppliers will need to operate a CoS service and it is likely that there will be operational costs associated with this.
[7] A breakdown of DCC costs, including the split between DCC operational costs and the cost of making changes to the DSP systems is included in Appendix 1.
[8] Implementation costs include an estimate of the DCC programme costs associated with each option based on anticipated resource requirements.
[9] It is likely that there will be some operational cost reductions because TCoS will no longer require operational support. These cost reductions have not been quantified and included in this analysis.
[10] Insufficient data was provided in response to the RfI to support an estimate of suppliers' operating costs.

4.3.3 Delivery

BEIS' target implementation timescales indicate that the ECoS procurement phase should begin during mid-2019, with migration completing during mid-2022. These timescales are based on the assumed total implementation time (including TCoS migration) of 36 months.

In response to the RfI issued by DCC, some suppliers indicated that they would require up to 36 months to complete the DBT phase for any changes required to their systems, with migration assumed to take a further 12 months. This would result in a end-to-end implementation time of 48 months. Assuming that all suppliers would need to ensure that their CoS Party solutions are operational before the migration of Devices from TCoS to ECoS can be completed, this could delay the completion of ECoS implementation until mid-2023:



This would leave over a year before the final DSP contract extension window expires, which would result in the level of implementation risk increasing slightly compared to the original target timescales. DCC is currently considering which elements of the existing DSP contract may need to be extended to support a smooth transition to the new DSP contract. It is possible that the existing TCoS service could be retained for a period using the final DSP extension window to allow any outstanding activities to be completed.

Under ECoS 1, suppliers acting as the CoS Party will require access to registration data in order to execute CoS events. Because the functionality to provide suppliers with registration data is within the scope of the Faster Switching programme, it has been assumed that no additional integration between the CSS and CoS Party systems will be required. Consequently, no dependency between the two programmes has been identified under ECoS 1.

Each supplier acting as CoS Party will need to be able to identify whether a Device conforms to SMETS1 or SMETS2 so that it can trigger the appropriate processes. It has been assumed that suppliers will already maintain their own inventory of all the Devices within their estate. Consequently, no dependency between ECoS1 and the SMETS1 programme has been identified.

4.3.4 Key risks and issues

The table below displays the key risks associated with ECoS 1. These have been assessed qualitatively and allocated scores based on the magnitude of the impact and the probability that the risk will materialise. These have been used to derive an overall risk rating that has been used in the evaluation in Section 5 of this paper.

Overall risk rating:

1 – 8 Low
9 – 17 Medium
18 – 25 High

Risks and issues with an overall risk rating of 15 or above are displayed in the table below. The full list of risks, issues, assumptions and dependencies associated with ECoS 1 is provided in Appendix 10.

RAID reference (links to Appendix 10)	RAID description	Probability score	Impact score	Overall risk rating
024	For ECoS 1 to work in the event of a supplier failure (e.g. SoLR), where the losing Supplier may not be able to carry out the actions required of it as a CoS Party, functionality similar to that provided by ECoS 2 will need to be incorporated into the ECoS 1 design.	5	5	25 (High)
026	Providing Anomaly Detection figures for CoS service requests between suppliers could constitute an unacceptable disclosure of sensitive information.	5	5	25 (High)
006	There are many Parties involved in the ECoS 1 implementation. This results in high levels of complexity when co-ordinating end-to-end implementation across all impacted Parties. All onboarded Supplier Parties would need to demonstrate that they are able to satisfy all CoS Party obligations in a similar way that they are required to undergo User Entry Process Testing prior to being able to access other DCC Services.	5	5	25 (High)

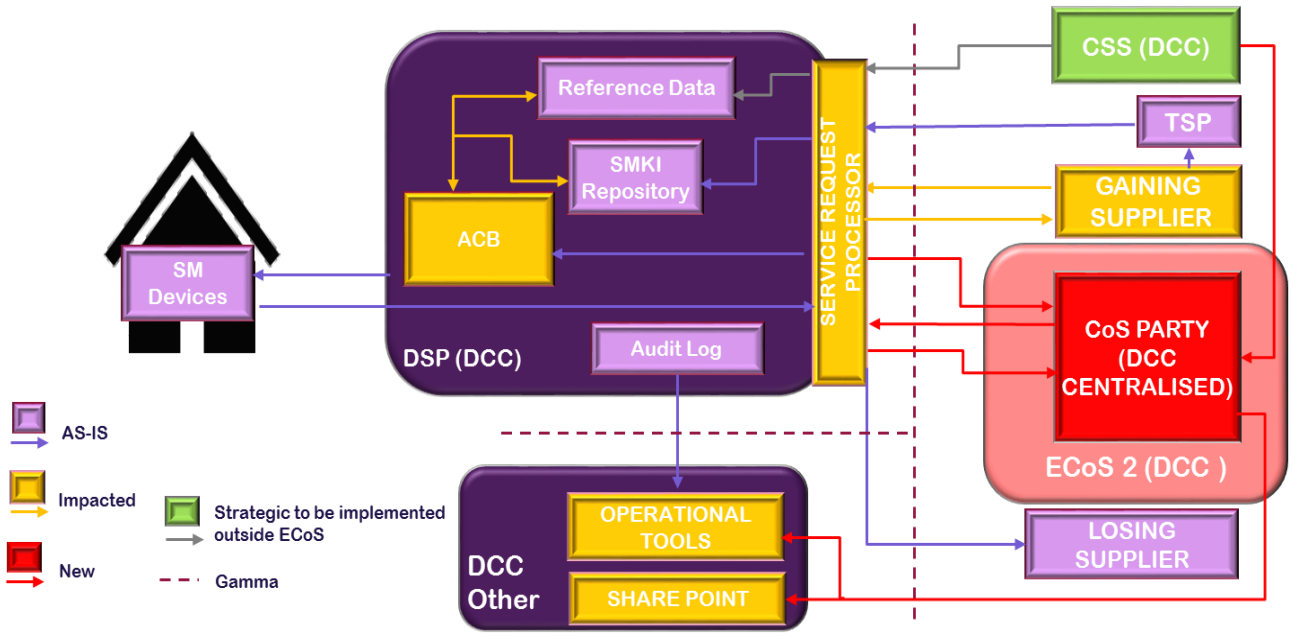
RAID reference (links to Appendix 10)	RAID description	Probability score	Impact score	Overall risk rating
008	The implementation of ECoS 1 will require resources to be allocated by energy suppliers. There is a risk that the required resources may not be available to all suppliers when needed. This risk is aggravated by the target implementation timescales, as any available resources are likely to have been allocated to other major programmes e.g. the Faster Switching programme.	3	5	15 (Medium)
027	Providing data relating to every CoS event to all suppliers gives rise to the risk that this data could be misused by market participants if monitoring and enforcement measures are not in place.	5	3	15 (Medium)

4.4 Enduring Change of Supplier - Model 2

An overview of the ECoS 2 key characteristics and basic architecture is provided below. Full details of the ECoS 2 architecture is provided in Appendix 9.

4.4.1 Overview

- No significant changes to energy suppliers' systems are expected as ECoS 2 is functionally similar to the existing TCoS model.
- CoS events are validated, processed and executed by a central CoS Party service provider.
- The implementation and management of the new central CoS Party will be undertaken by DCC.
- DCC will be responsible for developing the interfaces with the CoS Party system required to obtain reference data.



4.4.2 Impacts

The table on the following page summarises the impacts of ECoS 2 in terms of costs and complexity. Costs have been derived from the responses to the RfI conducted by DCC.

As with ECoS 1, the operational complexity of ECoS 2 has been assessed by comparing it with the baseline TCoS model. Technical complexity of ECoS 2 has been assessed in terms of implementation complexity based on system integration, timescales, migration and number of parties impacted. The full results of this analysis, along with the scoring criteria used, are provided in Appendices 7 and 8.

Impacted Party	Implementation costs	Operating costs (per annum)	Operational complexity	Technical complexity
Suppliers	£8.2M - £10.5M	Insufficient data provided [11]	Low	Low
DCC[12]	£29.7M - £39.5M[13]	£2.3M - £3.1M[14]	Low	Medium
Overall anticipated impact	£37.8M - £50.1M	£2.3M - £3.1M	Low	Medium

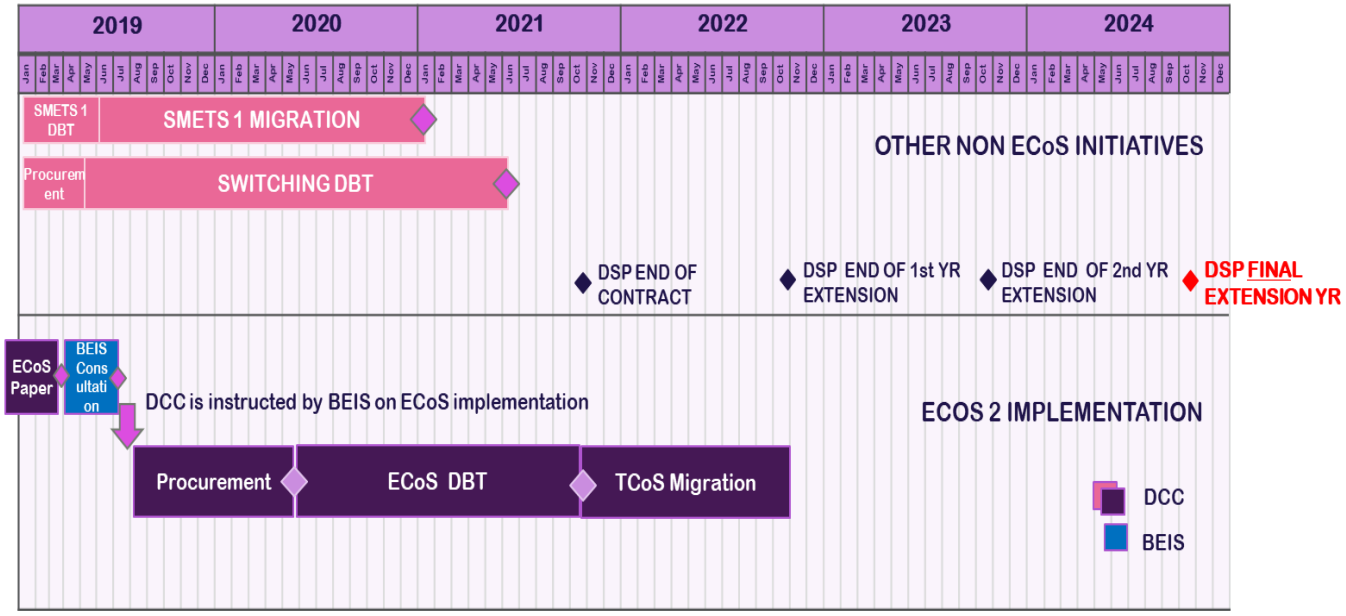
Supplier implementation costs are significantly reduced compared to ECoS 1, whilst DCC's costs increase by a relatively small amount. This reflects the lower number of CoS Party systems which would need to be developed and integrated under ECoS 2.

4.4.3 Delivery

The target implementation timescales indicate that the ECoS 2 procurement phase should begin during mid-2019, with migration completing during mid-2022. These timescales are based on an assumed total implementation time of 36 months.

The third-party vendor which provided a valid response to the RfI issued by DCC indicated that the DBT phase of ECoS 2 will take 17 months to complete, which is five months longer than the 12 months originally assumed by DCC. This results in an overall estimated implementation time of 41 months, with the migration of Devices to ECoS2 completing during Q4 2022.

[11] Energy suppliers will not be required to operate a CoS service, so supplier operating costs are expected to be minimal.
[12] A breakdown of DCC costs, including the split between DCC operational costs and the cost of making changes to the DSP systems is included in Appendix 1.
[13] Implementation costs include an estimate of the DCC programme costs associated with each option based on anticipated resource requirements.
[14] It is likely that there will be some operational cost reductions because TCoS will no longer require operational support. These cost reductions have not been quantified and included in this analysis.



This would leave little contingency time before the first DSP contract extension window expires, increasing implementation risk compared to the baseline target timescales. If detailed planning indicates that migration will take longer than the anticipated 12 months DCC would need to review the TCoS arrangements to ensure continuity of service, taking into consideration several factors including:

- The DSP contract duration required to support the DSP re-procurement;
- Any TCoS migration contingency requirements identified during detailed planning; and
- Whether it is possible to start the procurement phase earlier than currently planned to increase the amount of contingency time available.

Any decision taken will need to balance these factors, but the wider DSP re-procurement should be considered paramount due to the significant impacts on Parties which is likely to arise as a result of that work.

4.4.4 Key risks and issues

No risks with an overall risk rating of 15 or above have been identified in relation to ECoS 2. The list of risks, issues, assumptions and dependencies associated with ECoS 2 is provided in Appendix 11.

5 Evaluation

Solution option	Estimated implementation costs	Estimated operating costs (per annum)	Technical complexity	Operational complexity	Implementation timescales	Risk Rating
ECoS 1	£174.0M - £225.2M	£0.9M - £1.2M	High	High	48 months	High
ECoS 2	£37.8M - £50.1M	£2.3M - £3.1M	Medium	Low	41 months	Medium
Commentary	ECoS 2 has an estimated implementation cost saving of £136.2M - £175.1M compared to ECoS 1. The main driver of implementation cost reductions under ECoS 2 is that only one instance of the CoS Party solution needs to be developed. A single CoS Party solution also reduces integration costs.	ECoS 2 is estimated to incur additional £1.4M - £1.9M per annum in of DCC operating costs compared to ECoS 1. However, the dataset used does not include supplier costs, as insufficient data was provided in response to the RfI. The additional costs associated with ECoS 2 are mainly due to the operation and maintenance of the centralised CoS Party solution.	ECoS 2 has significantly lower levels of technical complexity than ECoS 1. The greater number of Parties involved in developing and maintaining the end-to-end ECoS1 solution increases complexity significantly compared to ECoS 2. The level of technical complexity will depend on the level of integration of each CoS Party solution with supplier back-end systems.	ECoS 2 has significantly lower levels of operational complexity than ECoS 1. The greater number of Parties involved in operating the end-to-end CoS service under ECoS1 increases complexity significantly compared to ECoS 2. The coordination of business processes, particularly error resolution, is inherently less complex under a centralised CoS model.	The implementation timescales for ECoS 2 are estimated to be around 7 months shorter than ECoS 1. This is because the longest implementation times provided by suppliers in response to the RfI are 7 months longer than DCC's estimated implementation timescales under ECoS 2.	ECoS 2 presents a lower level of risk compared to ECoS 1. The need to coordinate the procurement, development and testing of several new CoS Party solutions for ECoS 1, along with the need to ensure that all suppliers are ready to start migration on time results in higher implementation risk under ECoS 1.

6 Recommendation

DCC's evaluation of the two ECoS options indicates that ECoS 2 provides a better solution across all the evaluation criteria used, with the exception of operating costs. Because insufficient operating cost data was provided by energy suppliers in response to the RfI, supplier costs have not been accounted for as part of this assessment. DCC considers it highly likely that the ECoS1 operating costs will be greater ECoS 2.

ECoS 2 is also likely to result in a better experience for consumers when changing their energy supplier, as the possibility of the losing supplier frustrating the switching process is eliminated. A centralised CoS Party also provides a single initial point of contact for resolving CoS related issues, with DCC able to monitor the end-to-end CoS process and identify the cause of any issues or errors.

The principle that a distributed CoS Party model should provide a more secure and resilient CoS service originally appeared to provide a strong basis for implementing ECoS 1. However, the assumption that ECoS 1 will require an additional key to change supplier credentials in the event of a supplier failure undermines this principle.

In addition to this, evidence that energy market participants currently favour the use of shared software or managed service solutions suggests that ECoS 1 would not result in the variety of CoS Party systems assumed at the outset. If ECoS 1 is not demonstrably more secure and resilient than ECoS 2, no compelling evidence is available to indicate that it provides a better solution in any respect.

Following consideration of all of these factors, DCC has concluded that ECoS 2 represents a superior technical solution which provides better outcomes for both market participants and consumers, along with being more cost-effective and lower-risk.

On this basis, DCC's recommendation is that ECoS 2 should be selected for implementation.

Appendix 1 – Technical changes and costs (ECoS 1)

The table below displays the key technical changes required to implement and operate ECoS 1, including impacts and costs for all affected Parties.

Impacted Party	Description of impacts	Estimated implementation costs	Estimated operational cost (per annum)
Gaining supplier	▪ DUIS changes: alerts and population rules. ▪ Changes to the certification for XML signing of SR 6.23 (Change of credentials service request). ▪ Need to populate a new CoS ADT specification to cover need to forecast CoS events at MPID level.	£8.2M - £10.5M	Insufficient data provided
CoS Party (losing supplier)	▪ Development of CoS party functionality required to handle change of credentials, including the ability to create and parse ASN.1 message. ▪ CoS Parties will be required to consume the CoS Party APIs. It is expected that existing Gamma connectivity from energy suppliers to the DSP will be utilised for this purpose. ▪ Capability to access the reference data required for the processing of change of credentials events, including access to the SMKI repository, registration data, device information and user identifier information. ▪ Initial data load required as part of the instantiation of the CoS party. ▪ Support of the migration from TCoS to ECoS 1.	£135M - £173.6M	Insufficient data provided
TSP	▪ Provision of a new Remote Party Role of 'XML Signing'.	£0	£0
CSS	▪ None identified.	£0	£0
DSP	▪ Interface with CoS Party. ▪ Enhance functionality to handle CoS events: - Develop functionality to manage Change of CoS Party events, (including TCoS to ECoS migration).	£18.6M - £24.8M	£0.8M - £1.0M

Impacted Party	Description of impacts	Estimated implementation costs	Estimated operational cost (per annum)
	- Enhancements to the processing of reference data required to facilitate CoS events: ○ Changes to Anomaly Detection functionality in respect of CoS events; ○ Changes to the processing of User ID Range allocation; ○ Enforcement of the use of certificates with a Remote Party Role of 'XML Signing' for CoS Service Requests; and ○ DUIS Changes: new notification codes required to support to 6.23 CoS events. - Operational enhancements to Service Management. ▪ Operational enhancements to Service Management.		
DCC Operational tool	▪ None identified.	£0	£0
DCC SharePoint	▪ None identified.	£0	£0
DCC Cloud infrastructure	▪ None identified.	£0	£0

Appendix 2 – Operational impacts (ECoS 1)

The table below describes the anticipated impacts to the current business processes for impacted Parties with respect to ECoS 1:

Impacted Party	Description of impacts to business processes
Supplier	▪ For Anomaly Detection Threshold (ADT), provide forecast of CoS Events per MPID per calendar day. ▪ Provide execution datetime in the 6.23 Service Requests for both on-demand and future-dated CoS Events. ▪ Request and maintain certificates from TSP for XML Signing for 6.23 Service Requests. ▪ Sign 6.23 Service Requests using a valid certificate for XML Signing. ▪ Amend existing process to handle new error codes introduced by ECoS in Alerts N26 and N27 for CoS Events. ▪ Establish new processes for operating as a CoS Party including procedures for resolving incidents related to CoS Events. ▪ Potential changes required to the Comms Hubs ordering process to enable the correct Supplier's CoS Party certificate to be configured in the GPF on new Comms Hubs.
DCC	▪ Changes to the DCC User onboarding process to include verification of a new Supplier Party is able to operate as a CoS Party. ▪ Changes to the process for accepting the ADT for CoS Events defined in the new format. ▪ Changes to the process to set up an aggregated ADT on the DSP for CoS Events. ▪ Changes to the SMKI Inventory to hold certificates for XML signing. ▪ Changes to the process to include the various CoS Parties in the triage for incident and problems related to CoS Events. ▪ Changes to the release management process for new releases of DCC Systems to include all Suppliers in the capacity of CoS Parties. ▪ Potential changes required to the SoLR process to handle scenarios when the failed Supplier is no longer operating as a CoS Party for their Devices. ▪ Potential changes required to the Comms Hubs ordering process to enable the appropriate CoS Party certificate to be configured in the GPF on new Comms Hubs for each supplier order.
TSP	▪ Generate certificates for XML Signing to be used by Suppliers
SEC Panel	▪ Changes to the process for managing and issuing the User ID Ranges file, which includes: - Issuing a new file at regular interval, e.g. weekly;

Impacted Party	Description of impacts to business processes
	- Adding a validity period for each file; - Signing each file with a signature that can be verified using IKI.
SSC	▪ Approve the aggregated ADT for CoS Events.
SMKI RA	▪ To process requests from Suppliers for certificates for XML signing.

Appendix 3 – Operational complexity assessment (ECoS 1)

The evaluation of operational complexity has been carried-out by assessing the impacts of ECoS 1 on the current business operations under the TCoS arrangement. The scoring represents DCC's view on the level of changes/impacts to the current business operations for DCC, along with information provided by suppliers in response to the RfI, wherever this has been provided:

0: No impact

1: Low impact

3: Medium impact

5: High impact

Scoring criterion	DCC		Each supplier	
	Score	Rationale	Score	Rationale
Changes to current business operations and processes.	5	Collaboration will be required across many CoS Parties, which adds complexity to several operational processes e.g. Incident management, Problem management, User onboarding and release management.	5	Each supplier will need to amend their business processes to support acting as the CoS Party for Devices within their estate. Changes to the ADT definitions for CoS requests will be required.
Coordination of any upgrades.	3	Collaboration will be required across many CoS Parties.	3	Suppliers will be responsible for implementing upgrades to CoS Party systems individually.
Operational management and monitoring of interfaces.	3	A new CoS Party interface will be required between the DSP and many CoS Parties systems.	3	A new CoS Party interface will be required.
Demarcation of responsibilities (e.g. SLA, performance measures).	3	No commercial agreements are currently in place between suppliers and CoS Party service providers.	5	No commercial agreement is currently in place to support the provision of a CoS Party service. Losing suppliers in their capacity as CoS Party may not process the

Scoring criterion	DCC		Each supplier	
	Score	Rationale	Score	Rationale
				6.23 request promptly, unlike under TCoS, which is managed by DCC to ensure performance.
Additional resourcing.	1	Additional DCC resourcing will be required to: ▪ Coordinate implementation activities across many suppliers; and ▪ Support additional procedures for User onboarding to verify that suppliers are able to function as CoS Party.	1	No information provided. Impact assumed to be 1–2 FTE resources.
Total	15 (Medium)	1 – 5 Low 6 – 15 Medium 16 – 25 High	17 (High)	1 – 5 Low 6 – 15 Medium 16 – 25 High

Appendix 4 – Technical complexity assessment (ECoS 1)

The evaluation of technical complexity has been carried-out by comparing ECoS 1 against ECoS 2. The criteria used is as follows:

0: Unable to rate

1: Low complexity

3: Medium complexity

5: High complexity

Scoring criterion	DCC		Each supplier	
	Score	Rationale	Score	Rationale
Technical - Logical Architecture	3	Although DCC will not be responsible for developing, deploying and maintaining a CoS Party solution under ECOS1, DCC will responsible for the CoS party specifications. In addition to this, certain CoS scenarios such as SoLR may require additional development within DCC Systems.	5	Significant changes have been reported by Supplier Parties to support the functionality required by an ECoS 1 solution. The exact level of complexity will depend on the level of integration of the adaptor solution with supplier back end systems, which may vary between suppliers
Technical Integration	1	Although energy suppliers acting as CoS Parties will need to consume a new set of CoS APIs, the existing Gamma connection be re-used.	5	New interfaces or changes to the existing interfaces are expected to be required to support the ECoS 1.

Scoring criterion	DCC		Each supplier	
	Score	Rationale	Score	Rationale
Number of parties involved in implementation	3	DCC will need to engage with each energy supplier to verify they can function as CoS Party (via on-boarding or similar)	3	Energy suppliers will need to engage with their own service providers to develop the required CoS Party functionality, along with making changes to their back-end systems to integrate with the CoS Party system.
Time to implement	5	DCC will be responsible for planning and coordinating the end-to-end implementation and migration of ECoS 1.	5	As energy suppliers will need to develop the CoS Party functionality along with the generic changes required by both ECoS options, a lengthier timescale is expected for implementation compared to ECoS 2. The RfI Reponses received from energy suppliers indicate that the DBT phase could vary from 2 to 36 months, with an additional 12 months assumed to be required to support TCoS to ECoS migration (48 months in total).
Challenges to implement	5	DCC will be responsible for the integrity of the end-to-end solution, which will entail co-ordinating energy suppliers and DCC service providers.	3	Suppliers will need to make resources available for implementation and migration to meet the project timescale.

Scoring criterion	DCC		Each supplier	
	Score	Rationale	Score	Rationale
ECoS installation, maintenance, updates, patches and fixes -	5	DCC will be responsible for coordinating and managing any changes/impacts regarding the end-to-end solution.	3	Each Supplier will be responsible for any updates to their CoS Party solution.
Change management-	5	DCC will need to coordinate a large number of Parties when implementing change.	3	Each energy supplier acting as CoS Party will need to work with their own service providers when implementing change.
Total	27 (High)	1 – 7 Low 8 – 21 Medium 22 – 35 High	27 (High)	1 – 7 Low 8 – 21 Medium 22 – 35 High

Appendix 5 – Technical changes and costs (ECoS 2)

The table below displays the key technical changes required to implement and operate ECoS 2, including impacts and costs for all affected Parties.

Impacted Party	Description of impacts	Estimated implementation costs	Estimated operating costs (per annum)
Gaining supplier	▪ DUIS changes: alerts and population rules. ▪ Changes to the certification for XML signing of SR 6.23 (change of credentials). ▪ Need to populate a new CoS ADT specification to cover need to forecast CoS events at MPID level.	£8.2M - £10.5M	Insufficient data provided
CoS Party (DCC centralised)	▪ Integration with SharePoint required to obtain - Supplier user id ranges info - Change of Credential info ▪ Integration to DSP for consumption of: - Change of Credential related APIs - SMKI Repo info - Registration Data (tactical) ▪ Development of CoS party functionality required to handle change of credentials including the availability to create and parse ASN.1 message. ▪ Initial data load required as part of the instantiation of the CoS Party. ▪ Support of the migration from TCoS to ECoS 2. ▪ Data storage and accessibility. ▪ Hosting (option for CoS party solution to be hosted within DCC cloud). ▪ Application management. ▪ Service management. ▪ Operational security. ▪ CoS Party compliance with the security standards as defined by section G of the SEC.	£5.5M - £7.3M	£1.4M - £1.9M
TSP	▪ Provision of a new Remote Party Role of 'XML Signing'	£0	£0

Impacted Party	Description of impacts	Estimated implementation costs	Estimated operating costs (per annum)
CSS	▪ Interface with the CoS Party to allow the sharing of Registration Data required to support the Change of Credentials process.	No data provided	No data provided
DSP	▪ Interface with CoS Party. ▪ Enhance functionality to handle CoS events: - Develop functionality to manage Change of CoS Party events, (including TCoS to ECoS migration). - Enhancements to the processing of reference data required to facilitate CoS events: ○ Changes to Anomaly Detection functionality in respect of CoS events; ○ Changes to the processing of User ID Range allocation; ○ Enforcement of the use of certificates with a Remote Party Role of 'XML Signing' for CoS Service Requests; ○ DUIS Changes: new notification codes required to support to 6.23 CoS events; and ○ Make RDP registration data files available to CoS Party. ▪ Operational enhancements to Service Management.	£18.6M - £24.8M	£0.8M - £1.0M
DCC Operational Tools	▪ The tools used by Technical Operation Centre will required a feed to the CoS Party information to guarantee operational support of the service.	Under £10K	Under £5K
DCC SharePoint	▪ Integration of SharePoint to the CoS Party to enable sharing of reference data i.e. ID ranges and Anomaly detection threshold files	£0	£0
DCC Cloud infrastructure	▪ To host the Cost Party ▪ Provide connectivity to:	£0.5M- £0.6M	Under £210K

Impacted Party	Description of impacts	Estimated implementation costs	Estimated operating costs (per annum)
	- DSP via Gamma network - SharePoint - Operational tools		

Appendix 6 – Operational impacts (ECoS 2)

The table below describes the anticipated impacts to the current business processes for impacted Parties with respect to ECoS 2:

Impacted Party	Description of impacts to business processes
Supplier	▪ For Anomaly Detection Threshold (ADT), provide forecast of CoS Events per MPID per calendar day. ▪ Provide execution datetime in the 6.23 Service Requests for both on-demand and future-dated CoS Events. ▪ Request and maintain certificates from TSP for XML Signing for 6.23 Service Requests. ▪ Sign 6.23 Service Requests using a valid certificate for XML Signing. ▪ Amend existing process to handle new error codes introduced by ECoS in Alerts N26 and N27 for CoS Events.
DCC	▪ Changes to the process for accepting the ADT for CoS Events defined in the new format. ▪ Changes to the process to set up an aggregated ADT on the DSP for CoS Events. ▪ Changes to the SMKI Inventory to hold certificates for XML signing. ▪ Manage an additional Service Provider to provide the central CoS Party service.
TSP	▪ Generate certificates for XML Signing to be used by Suppliers
SEC Panel	▪ Changes to the process for managing and issuing the User ID Ranges file, which includes: - Issuing a new file at regular interval, e.g. weekly; - Adding a validity period for each file; - Signing each file with a signature that can be verified using IKI.
SSC	▪ Approve the aggregated ADT for CoS Events.
SMKI RA	▪ To process requests from Suppliers for certificates for XML signing.

Appendix 7 – Operational complexity assessment (ECoS 2)

The evaluation of operational complexity has been carried-out by assessing the impacts of ECoS 2 on the current business operations under the TCoS arrangement. This scoring represents DCC's view on the level of changes/impacts to the current business operations for DCC, along with information provided by suppliers in response to the RfI, wherever this has been provided:

0: No impact

1: Low impact

3: Medium impact

5: Substantial impact

Scoring criterion	DCC		Suppliers	
	Score	Rationale	Score	Rationale
Changes to current business operations.	1	There will be a need to manage an additional DCC Service Provider contract.	1	Some changes are required to the Anomaly Detection Thresholds for CoS requests.
Coordination of any upgrades.	1	There will be one additional DCC Service Provider to be considered when coordinating any upgrades.	0	The new centralised CoS Party service will be managed by DCC, similar to the current TCoS model, resulting in minimal changes.
Operational management of interfaces.	1	There will be one additional DCC Service Provider to be considered when carrying-out operational management of interfaces.	0	The new centralised CoS Party service will be managed by DCC, similar to the current TCoS model, resulting in minimal changes.
Demarcation of responsibilities	1	There will be one additional DCC Service Provider to be considered.	0	The new centralised CoS Party service will be managed by DCC, similar to the current TCoS model, resulting in minimal changes.
Additional resourcing	0	No additional resourcing is anticipated because the ECoS 2 model is similar to the existing TCoS model in terms of	0	The new centralised CoS Party service will be managed by DCC, similar to the current

Scoring criterion	DCC		Suppliers	
	Score	Rationale	Score	Rationale
		operational resourcing requirements.		TCoS model, resulting in minimal changes.
Total	4 (Low)	1 – 5 Low 6 – 15 Medium 16 – 25 High	1 (Low)	1 – 5 Low 6 – 15 Medium 16 – 25 High

Appendix 8 – Technical complexity (ECoS 2)

The evaluation of technical complexity has been carried-out by comparing ECoS 2 against ECoS 1. The criteria used is as follows:

0: Unable to rate

1: Low complexity

3: Medium complexity

5: High complexity

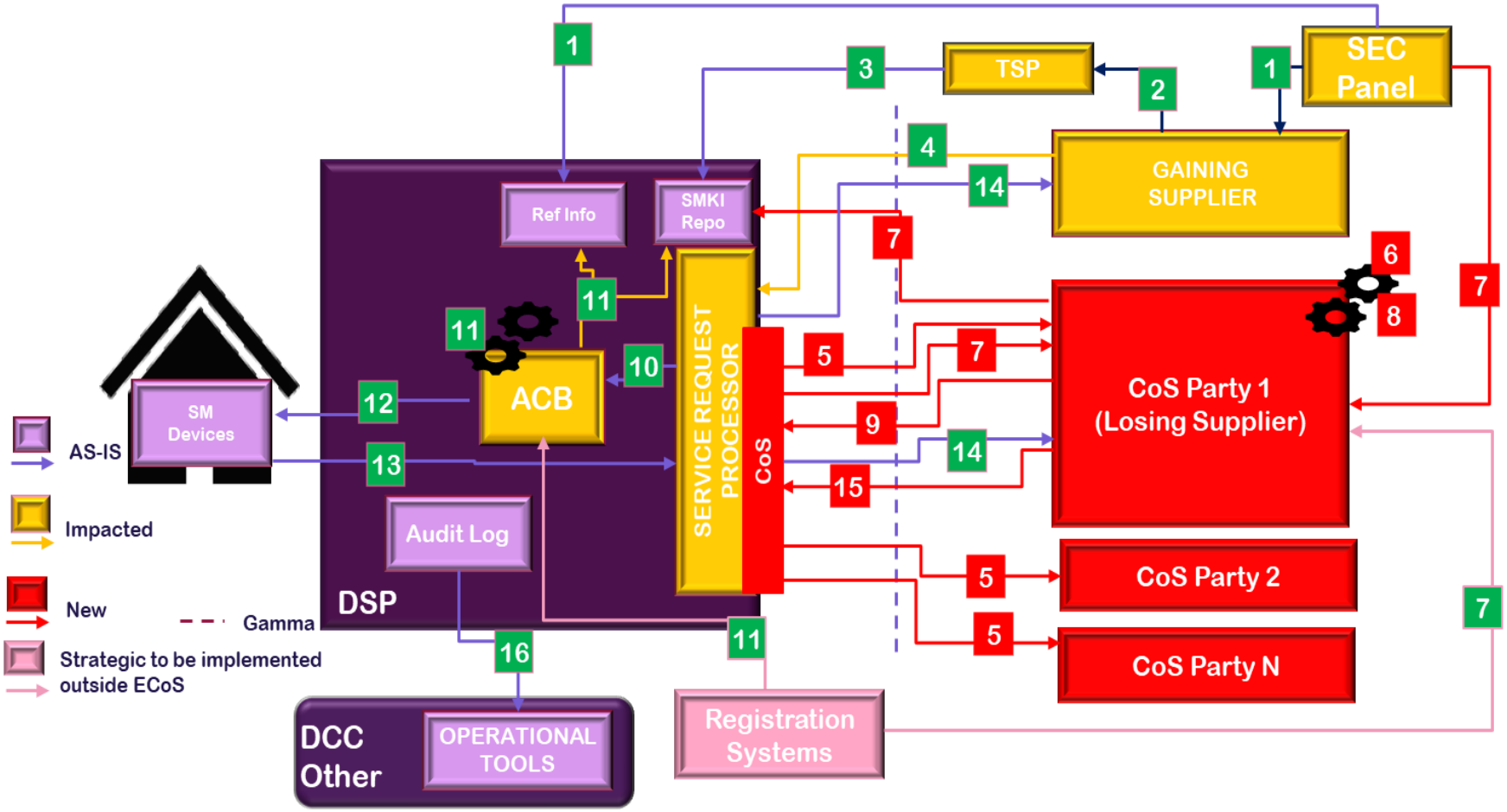
Scoring criterion	DCC		Suppliers	
	Score	Rationale	Score	Rationale
Technical - Logical Architecture	3	Although DCC will be required to develop a centralised ECoS service separate from the DSP, the control DCC will be able to exert over both services is expected to increase the integrity on the final solution. It should be possible to adapt some existing DSP applications and systems to enable and support the solution.	1	ECoS 2 is preferred by energy suppliers due to a substantially lower impact compared to ECoS 1, as they will not be required to implement their own CoS Party solution.
Technical Integration	3	As DCC will be responsible for the Cos Party, a new physical interface to the DSP will be required to enable the CoS Party to consume a new set of CoS APIs. The CoS Party will require new interfaces to various existing DCC Systems in order to obtain refence data, along with the operational tools to ensure the operability of the service.	1	Energy suppliers will not need to make any changes in order to integrate with existing DCC Systems.

Scoring criterion	DCC		Suppliers	
	Score	Rationale	Score	Rationale
Number of parties involved in implementation	1	The implementation of a centralised CoS Party service will impact a fewer number of parties.	1	Fewer critical activities will be required across many Parties as the CoS service will be centralised. CoS changes under ECoS 2 should be transparent to energy suppliers.
Time to implement	3	Shorter timescales are expected for implementation and migration to ECoS2 compared to ECoS 1, as DCC is expected to have full control over the solution.	1	Shorter timescales are expected for energy suppliers because they will only need to develop the generic changes common to both ECoS.
Challenges to implement	3	DCC will be responsible for the integrity of the end-to-end solution, but the need to coordinate energy suppliers is reduced under ECoS 2 compared to ECoS 1.	1	The number of changes energy suppliers are required to make are reduced compared to ECoS 1 because they will only need to make the generic changes common to both ECoS options.
ECoS installation, maintenance, updates, patches and fixes	3	DCC will be have full responsibility for managing and implementing all updates, patches and fixes.	1	Energy suppliers will not be required to implement updates, patches and fixes.
Change management-	3	DCC will have full control of the solution and the number of parties involved will be reduced compared to ECoS 1.	1	The changes that energy suppliers will be responsible for implementing under ECoS 2 are expected to be minimal.

Scoring criterion	DCC		Suppliers	
	Score	Rationale	Score	Rationale
Total	19 (Medium)	1 – 7 Low 8 – 21 Medium 22 – 35 High	7 (Low)	1 – 7 Low 8 – 21 Medium 22 – 35 High

Appendix 9 – End-to-end architecture

ECoS 1 architecture



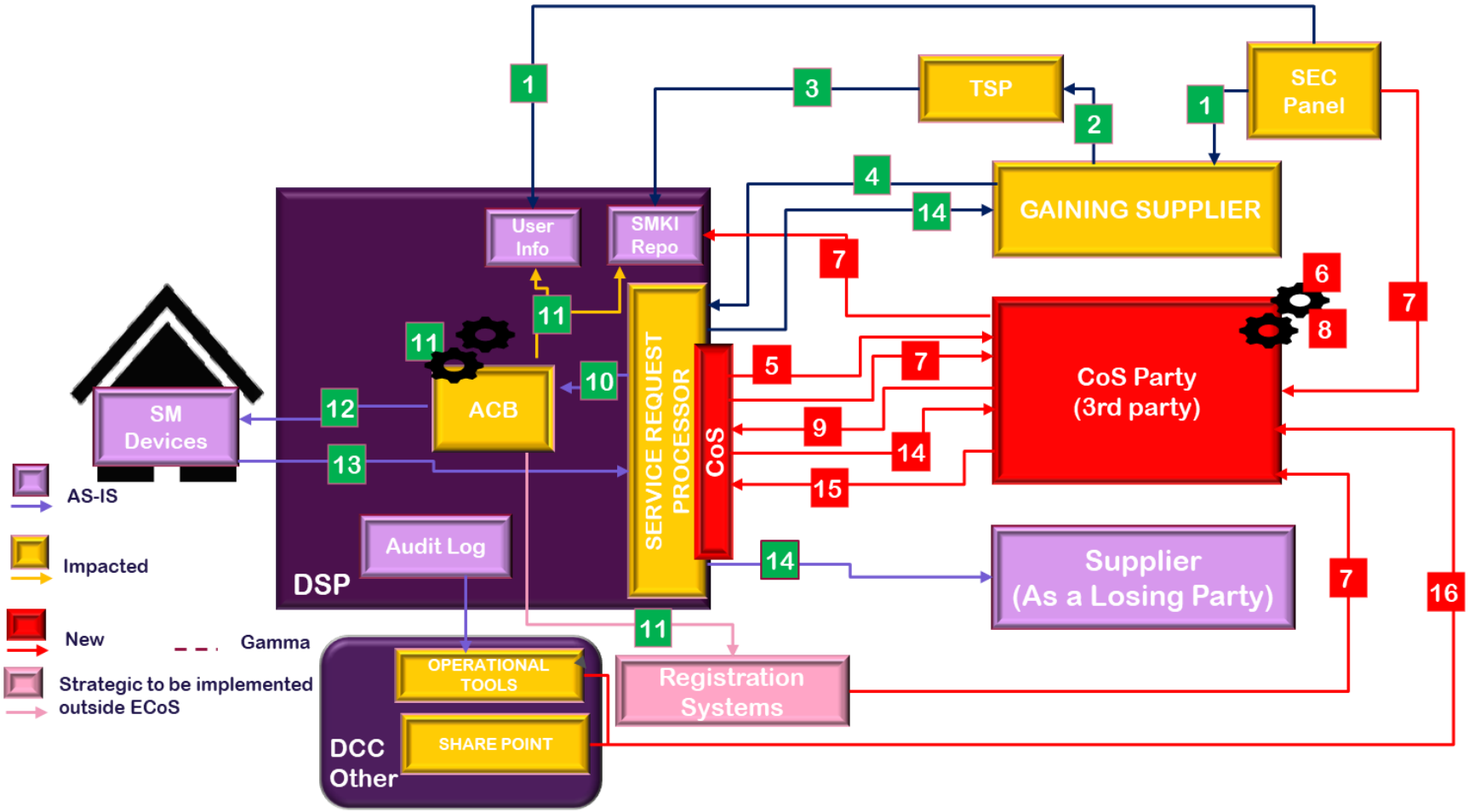
REF	CoS Flow	WHAT IS NEW	PARTIES IMPACTED
1	- As part of the onboarding into Smart DCC Supplier Parties are provided with a set of user ID ranges by Panel - Panel also shares the user ID ranges with DCC, with information being stored by Service Request Processor	- The Panel (SECAS) will: - add a valid from and valid to date to the file format - remove any MPID details from the file format - issue at least one file per week, each being valid for 8 days and each being placed on SEC Website - sign each file in such a way that the signature can be verified using IKI	Panel
2	Energy supplier obtains the relevant Cryptographic Certificates from the TSP	- Energy Supplier will need to obtain a new certificate for purpose of 6.23 XML signing - the XML Signing Certificate should contain – 1. User ID + Electricity and/or Gas MPID 2. This XML signing certificate will be used to validate 6.23 requests	Supplier Parties
3	Key and certification is shared with DCC and stored by the Service Request Processor	Provision of a new Remote Party Role of 'XML Signing by the TSP	TSP
4	-Gaining Supplier submits a 6.23 - 'Update Security Credentials' - service request to initiate a Change of Credentials - Request will be submitted AS-IS	Supplier Parties will sign the 6.23 using XML sign certificate as specified on flow reference 2	Supplier Parties (as described in Step 2 above)

REF	CoS Flow	WHAT IS NEW	PARTIES IMPACTED
5	The Service Request Processor will apply basic validations to the 6.23 and distribute the message to all recognised CoS parties	Service Request Processor will made available new schemas to enable Change of Credentials with CoS Parties. These schemas will be separate from the DUIS schemas	- Service Request Processor - Energy Suppliers (As CoS parties)
6	- Upon receiving the 6.23 service request, Supplier Parties acting as CoS Parties will inspect the request. - The CoS Party that recognises the CoS request as being related to one of the devices within its estate, will process the Change of Credentials request	Supplier will need to develop the necessary means to obtain the required information and capability required to process a CoS event. This will include: - Access to the user id ranges (Assumed to be currently available) - Access to Cryptographic material - SMKI Repo- (Assumed to be currently available) - Device information - assume to be currently available although enhancements are expected thus to allow transition from TCoS to ECoS -- Registration Data. Assumes Energy Suppliers will have access to their own registration date as well as changes of registration impacting their devices. - ADT files - CoS parties will be required to also store ADT information on other CoS parties thus to perform the validations described on the next step (#7)	Supplier Parties (As CoS Parties)

REF	CoS Flow	WHAT IS NEW	PARTIES IMPACTED
7	This flow depicts the various reference data required by the CoS Party to verify and validate a Change of Credentials request.	The energy supplier acting as a CoS Party will need to develop the necessary functionality to obtain the following reference data: - User ID Ranges - Cryptographic material - Registration data - Device info - ADTs	Supplier Parties (As CoS Parties)
8	Upon satisfactory completion of step #7 - the Energy supplier acting as a CoS Party will transform the Message into GBCS (only applicable to SMETS2+ Devices)	Parse as well Correlate capabilities will need to be available to CoS parties to enable XML message transformation	Suppliers Parties (As CoS parties)
9	The Energy supplier, acting a CoS Party will submit the processed 6.23 request, to the Service Request Processor.	As mentioned above CoS only schemas will be made available for the interaction between Cos Parties and Service Request processor. Supplier acting as a CoS Party is expected to use a specific certificate for the purpose of a CoS request XML signing	Supplier Parties (As CoS parties)
10	Service Request Processor will pass the message to the Access Control Broker	No change	Service Request Processor

REF	CoS Flow	WHAT IS NEW	PARTIES IMPACTED
11	ACB will apply independent validation checks to the CoS request (#7)	Functionality Enhancement	Service Request Processor
12	If the above is correct the CoS request will be issued to the device for SMETS2 or to the S1SP for SMETS1	No change	N/A
13	Change of Supplier will be complete and CoS response will be sent back to the Service Request Processor	No change	N/A
14	As a result, the Supplier will receive a response to the 6.23 informing of them of the completion of a CoS Losing supplier will receive a notification informing them of 6.23 completion	No change	N/A
15	If any errors are detected apart from the validation and verification of a CoS event the CoS Party will issue a notification message via the DUIS Interface to allow further investigation by the DCC	CoS notification message will be made available via the DUIS Interface	- Service Request Processor - Supplier Parties (As CoS Parties)
16	Operational flows from DSP to DCC operational flows will continue as-is	No change	n/a

ECoS 2 architecture



REF	CoS FLOW	WHAT IS NEW	PARTIES IMPACTED
1	- As part of the onboarding into Smart DCC Supplier Parties are provided with a set of user ID ranges by Panel - Panel also shares the user ID ranges with DCC, with information being stored by Service Request Processor	- The Panel (SECAS) will: - Add a valid from and valid to date to the file format - Remove any MPID details from the file format - Issues at least one file per week, each being valid for 8 days and each being placed on SEC Website - Sign each file in such a way that the signature can be verified using IKI	Panel
2	Energy supplier obtains the relevant Cryptographic Certificates from the TSP	- Energy Supplier will need to obtain a new certificate for purpose of 6.23 XML signing - the XML Signing Certificate should contain 1. User ID + Electricity and/or Gas MPID 2. This XML signing certificate will be used to validate 6.23 requests	Supplier Parties
3	Key and certification is shared with DCC and stored by the Service Request Processor	Provision of a new Remote Party Role of 'XML Signing by the TSP	TSP
4	Gaining Energy Supplier submits a 6.23- Update Security Credentials - service request to initiate a Change of supplier Request will be submitted AS-IS	Energy supplier will use the above defined certificate to submit 6.23 request	Suppliers Parties (As described on #2)

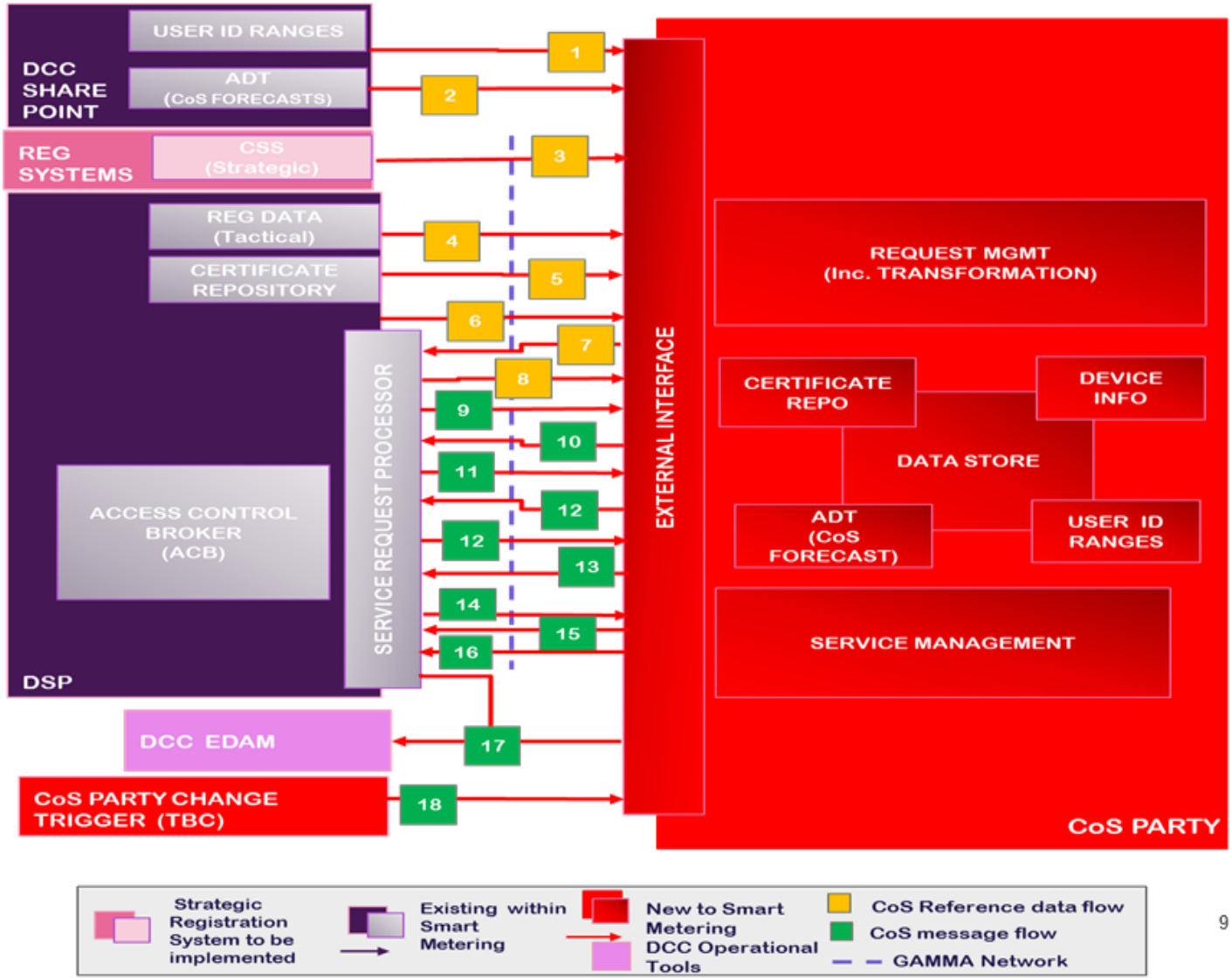
REF	CoS FLOW	WHAT IS NEW	PARTIES IMPACTED
5	The Service Request Processor will apply basic validations to the 6.23 and distribute the message to all recognised CoS parties	Service Request Processor will made available new schemas to enable Change of Credentials with CoS Parties. These schemas will be separate from the DUIS schemas	- Service Request Processor - CoS Party (as a 3rd party centralised system)
6	- Upon receiving the 6.23 service request CoS Parties will inspect the request. - The CoS Party that recognises the CoS request as being related to one of the devices within its estate, will process the Change of Credentials request	CoS party will need to develop the necessary means to obtain the required information and capability required to process a CoS event. This will include: - Access to the user id ranges (Assumed to be currently available) - Access to Cryptographic material - SMKI Repo- (Assumed to be currently available) - Device information - assume to be currently available although enhancements are expected thus to allow transition from TCoS to ECoS -- Registration Data. - ADT files - CoS parties will be required to also store ADT information	CoS Party (as a centralised system)

REF	CoS FLOW	WHAT IS NEW	PARTIES IMPACTED
7	This flow depicts the various reference data required by the CoS Party to verify and validate a Change of Credentials request.	The CoS Party will need to develop the necessary functionality to obtain the following reference data: - User ID Ranges - Cryptographic material - Registration data - Device info - ADTs	-CoS Party (as a 3rd party centralised system) - SharePoint - Registration Systems (as CSS)
8	If all the above are correct - CoS Party will transform the Message into GBCS (applicable only to SMETS2+ Devices)	Parse as well Correlate capabilities will need to be available to CoS parties to enable XML message transformation	CoS Party (as a 3rd party centralised system)
9	CoS Party will submit the processed 6.23 request to the User using the DUIS Interface	As mentioned above new URL with CoS only schemas will be enabled within the DUIS interface to enable the communication between Service Request Processor and CoS parties. A Supplier acting a CoS Party is expected to use a specific certificate for CoS request XML signing	CoS Party (as a 3rd party centralised system)

REF	CoS FLOW	WHAT IS NEW	PARTIES IMPACTED
10	Service Request Processor will pass the message to the Access Control Broker	Functionality Enhancement	Service Request Processor
11	ACB will apply independent validation checks to the CoS request (step 7)	Functionality Enhancement	Service Request Processor
12	If the above is correct the CoS request will be issued to the device for SMETS2 or to the S1SP for SMETS1	No change	N/A
13	Change of Supplier will complete, and CoS response will be sent back to the Service Request Processor	No change	N/A
14	As a result of the above, Gaining Supplier will receive a response to the 6.23 informing them of the completion of CoS Losing supplier will receive a notification informing them of 6.23 completion	CoS response will be also shared with applicable CoS Party	Gaining Supplier Losing Supplier CoS Party
15	If any errors are detected apart from the validation and verification of a CoS event the CoS Party will issue a notification message via the DUIS Interface to allow further investigation by the DCC	CoS notification message will be made available via the DUIS Interface	- Service Request Processor

REF	CoS FLOW	WHAT IS NEW	PARTIES IMPACTED
			- Supplier Parties (as CoS parties)

CoS Party functional architecture



9

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
1	USER ID RANGES	Flow used for the sharing of user id ranges	DCC -Share Point	CoS Party	File based	IKI	Microsoft Share point
2	ANOMALY DETECTION CoS (ADT) FORECASTS	Flow used for the sharing of forecast thresholds on: - Change of Supplier - Change of CoS Party Credentials	DCC - Share Point	CoS Party	File based	IKI	Microsoft Share point
3	REGISTRATION DATA (Strategic)	This flow provides the relationships between Market Participant IDs and Meter Points (MPxN) over time.	Registration systems - CSS	CoS Party	Message Based (Strategic)	SMKI XML signing	HTTP Post
4	REGISTRATION DATA (Tactical)	This flow provides the current and future relationships between Market Participant IDs and Meter Points (MPxN). This will be a tactical flow to be replaced by the Registration Data Strategic interface	DSP	CoS Party	File based	SMKI file signing	
5	CERTIFICATE REPOSITORY	This flow provides information from the SMKI Repository including: • SMKI Certificates	DSP	CoS Party	Message based (XML)	X.509 Elliptic Curve or RSA	HTTP Post

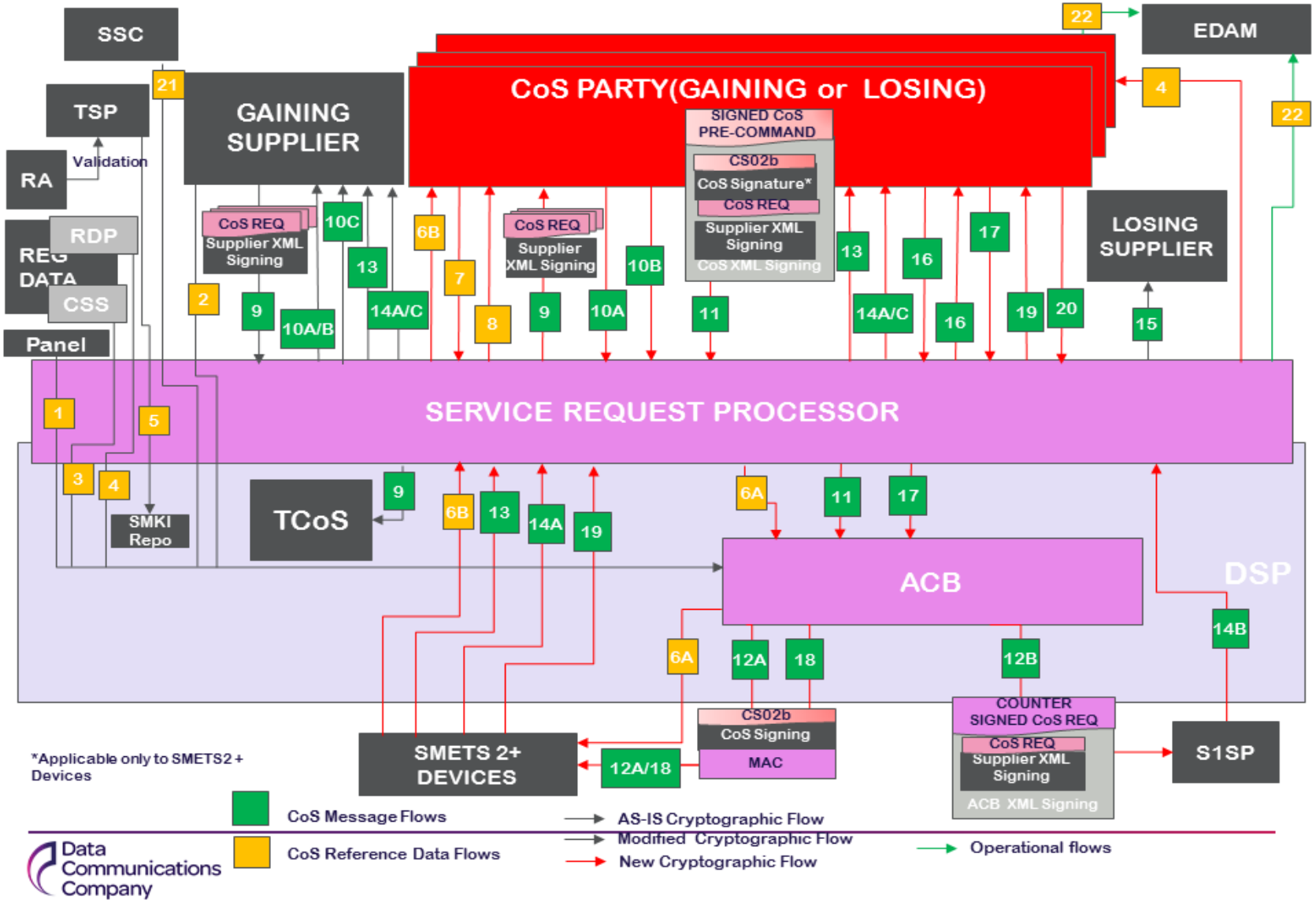
REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		• IKI Certificates					
		• SMKI Certificate Revocation Lists					
		• SMKI Authority Revocation Lists					
		• IKI Certificate Revocation Lists					
		• IKI Authority Revocation Lists					
		• Meta data extracted from those certificates (for the purposes of search)					
		• Validity information (indicating whether certificates are currently in use)					
6	DEVICE COMMISIONING	For a SMETS2+ Device, a Device Response confirming the Device ID and the CoS Party credentials that are on the Device	Device via Service Request Processor	CoS Party	Message Based	SMKI Device ASN.1 signing	HTTP Post
		For a SMETS1 Device a message confirming that this is the CoS Party for the Device ID specified.		CoS Party	Message Based	SMKI XML signing	HTTP Post
7	READ INVENTORY	This flow will be used by CoS party to retrieve	CoS Party		Message Based	SMKI XML signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		- Device Type,		Service Request Processor	(XML based on DUIS specification)		
		- whether the device is SMETS1 Device or SMETS2+ Device,					
		- the associated MPxN and the MPID associated with MPxN along with the start date.					
8	DEVICE DETAIL MAINTENANCE	Either Device removal or changes to the Device ID to MPxN mapping	Service Request Processor	CoS Party	Message Based	SMKI XML signing	HTTP Post
9	CoS REQUEST	Only the Relevant CoS Party will process the request based on its store of Device details	Service Request Processor	All CoS Parties	Message Based (XML based on DUIS specification)	SMKI XML signing	HTTP Post
10	SIGNED CoS PRE-COMMAND	Each such message includes the original supplier's CoS Request and, for a SMETS2+ Device only, a corresponding signed GBCS command	CoS Party	Service Request Processor	Message Based (XML based partly on DUIS specification)	SMKI XML signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
11	COUNTERSIGNED CoS SMETS1 RESPONSE	For a SMETS2+ Device, the Device Response to the GBCS command	Device via Service Request Processor	CoS Party	Message Based	SMKI Device ASN.1 signing	HTTP Post
		For a SMETS1 Device, a Countersigned CoS SMETS1 Response	S1SP via Service Request Processor	CoS Party	Message Based (XML based partly on DUIS specification)	SMKI XML signing	HTTP Post
12	CHANGE OF CoS PARTY CREDENTIAL REQUEST	Request from a Gaining CoS Party to a Losing CoS Party for changes of CoS Party credentials for the Device	Gaining CoS Party	Losing CoS Party via Service Request Processor	Message Based	SMKI XML signing	HTTP Post
13	CHANGE OF CoS PARTY CREDENTIAL SIGNED PRE-COMMAND	Each request includes the original CoS Party request and, for a SMETS2+ Device only, a corresponding signed GBCS command	Losing CoS Party	ACB via Service Request Processor	Message Based	SMKI XML signing	HTTP Post
14	CHANGE OF CoS PARTY	For a SMETS2+ Device, Device Response to the GBCS command	Device via Service Request Processor	CoS Party	Message Based	SMKI Device ASN.1 signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
	CREDENTIALS RESPONSE	For a SMETS1 Device, a message confirming the change		CoS Party	Message Based (XML based partly on DUIS specification)	SMKI XML signing	HTTP Post
15	INCIDENT NOTIFICATION	This flow is to raise incidents with DCC	CoS Party	DCC			
16	ALERTS	This flow covers Alert notification to other parties e.g. confirmation for receipt of requests from CoS Parties; notifications of errors	CoS Party	Other parties via Service Request Processor	Message Based	SMKI XML signing	HTTP Post
17	CHANGE OF CoS PARTY TRIGGERS	A mechanism to tell the Gaining CoS Party that they should gain a Device		Gaining CoS Party			
18	OPERATIONAL FLOWS	This flow covers the flow of Audit information required to support DCC Operational process	CoS Party and Service Request Processor	Enterprise Data Analytical Model (EDAM)			

Key change of credentials cryptographic flows



REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
1	USER ID RANGES	Flow used for the sharing of User ID ranges	Panel	ACB (via the Service Request Processor)	File based	IKI	
2	ANOMALY DETECTION CoS (ADT) FORECASTS	Flow used for the sharing of forecast thresholds for CoS Event	Gaining Supplier	ACB (via the Service Request Processor)	File based	IKI	
3	REGISTRATION DATA (Strategic)	This flow provides confirmed changes to the relationships between Market Participant IDs and Meter Points (MPxN).	Registration Systems - CSS	ACB (via the Service Processor)	Message Based (Strategic)	SMKI XML Signing	HTTP Post
4	REGISTRATION DATA (Tactical)	This flow provides the current and future relationships between Market Participant IDs and Meter Points (MPxN). This is a tactical flow to be replaced by the Registration Data strategic interface.	RDP	ACB and CoS Parties (Via the Service Request) Processor	File based	SMKI file signing	FTPS (input to Service Request Processor) on the flow from DSP

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
5	CERTIFICATE REPOSITORY	SMKI Repository includes • SMKI Certificates • IKI Certificates • SMKI Certificate Revocation Lists • SMKI Authority Revocation Lists • IKI Certificate Revocation Lists • IKI Authority Revocation Lists • Meta data extracted from those certificates (for the purposes of search) • Validity information (indicating whether certificates are currently in use) This is available to all Parties (including the SRP, ACB, CoS Parties etc.) apart from SMETS2+ Devices.	TSP	SMKI Repository			

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
6A	READ CREDENTIALS COMMAND TO DEVICE	For a SMETS2+ Device, this flow is a Command asking the Device for its CoS Party credentials. This will be a post-commissioning obligation on the DCC for SMETS2+ Devices.	Service Request Processor	SMETS 2+ Device (Via the ACB)	Message Based	SMKI Device ASN.1 Signing	
6B	READ CREDENTIALS RESPONSE FROM DEVICE	For a SMETS2+ Device, a Device Response confirming the Device ID and the CoS Party credentials that are on the Device	SMETS 2+ Device (Via the Service Request Processor)	Relevant CoS Party (via Service Request Processor)	Message Based	SMKI Device ASN.1 Signing	HTTP Post
7	READ INVENTORY	This flow will be used by CoS Party to retrieve Device Type, whether the Device is SMETS1 Device or SMETS2+ Device, the associated MPxN and the supplier MPID associated with MPxN along with the start date.	CoS Party	Service Request Processor	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
8	DEVICE DETAIL MAINTENANCE	Either Device removal or changes to the Device ID to the MPxN mapping. These are additional alerts triggered by the Service Request Processor – (please refer to the requirements for more detail)	Service Request Processor	CoS Party	Message Based	SMKI XML Signing	HTTP Post
9	CoS REQUEST	Change of Supplier Update Security Credential Request as issued by the Supplier Party acting as the Gaining Supplier.	Supplier Party (as Gaining Supplier)	Either TCoS or All CoS Parties (Via the Service Request Processor)	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post – Except for TCoS
10A	CoS ACKNOWLEDGEMENT QUEUED	Message Acknowledgment the CoS request has been queued by the CoS Party.	CoS Party	Gaining Supplier (Via the Service Request Processor)	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
10B	CoS Acknowledgement PROCESSING	Message Acknowledgment the CoS request has been processed by the CoS Party	CoS Party	Gaining Supplier Via the Service Request Processor)	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post
10C	TCoS ACKNOWLEDGEMENT	Message Acknowledgment by the Service Request Processor that the CoS request has been queued or processed by TCoS	Service Request Processor	Gaining Supplier	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post
11	SIGNED CoS PRE-COMMAND	Each such message includes the original Supplier's CoS Request and, for a SMETS2+ Device only, a corresponding signed GBCS command. If there is no CS02b element the Service Request Processor should queue the Signed CoS Pre-Command	CoS Party	ACB (via the Service Request Processor)	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
12A	CS02b	CS02b Command generated by the ACB after applying the relevant checks and Threshold Anomaly Detection.	ACB	SMETS2+ Device	Message Based	SMKI Device ASN.1 Signing	HTTP Post
12B	COUNTER SIGNED CoS REQUEST	The ACB, after applying the relevant checks and Threshold Anomaly Detection, will incorporate the original CoS request in a Counter Signed CoS Request.	ACB	S1SP	Message Based	SMKI XML Signing	HTTP Post
13	0x00CB DEVICE ALERT	Alert telling the CoS Party the outcome of processing the Change of Credentials instruction (possible outcomes: positive, negative or partial completion). If the outcome is positive the alert will contain information on CoS Party, Losing Supplier and Gaining Supplier	SMETS2+ Device	CoS Party & Gaining Supplier (Via the Service Request Processor)	Message Based	SMKI Device ASN.1 Signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
14A	CoS COMMAND RESPONSE	For a SMETS2+ Device, the Device Response to the GBCS command. This might not arrive before the 0x00CB Device Alert. The Response either confirms receipt of the command or it will detail the outcome of processing the Change of Credentials instruction (possible outcomes: positive, negative or partial completion). If the outcome is positive, the alert will contain information on CoS Party, Gaining and Losing Supplier.	SMETS2+ Device	CoS Party& Gaining Supplier (Via the Service Request Processor)	Message Based	SMKI Device ASN.1 signing	HTTP Post
14B	CoS SMETS1 RESPONSE	For a SMETS1 Device, a SMETS1 Response. This response will always confirm the outcome of the process	S1SP	Service Request Processor	Message Based (XML based partly on DUIS specification)	SMKI XML Signing	HTTP Post

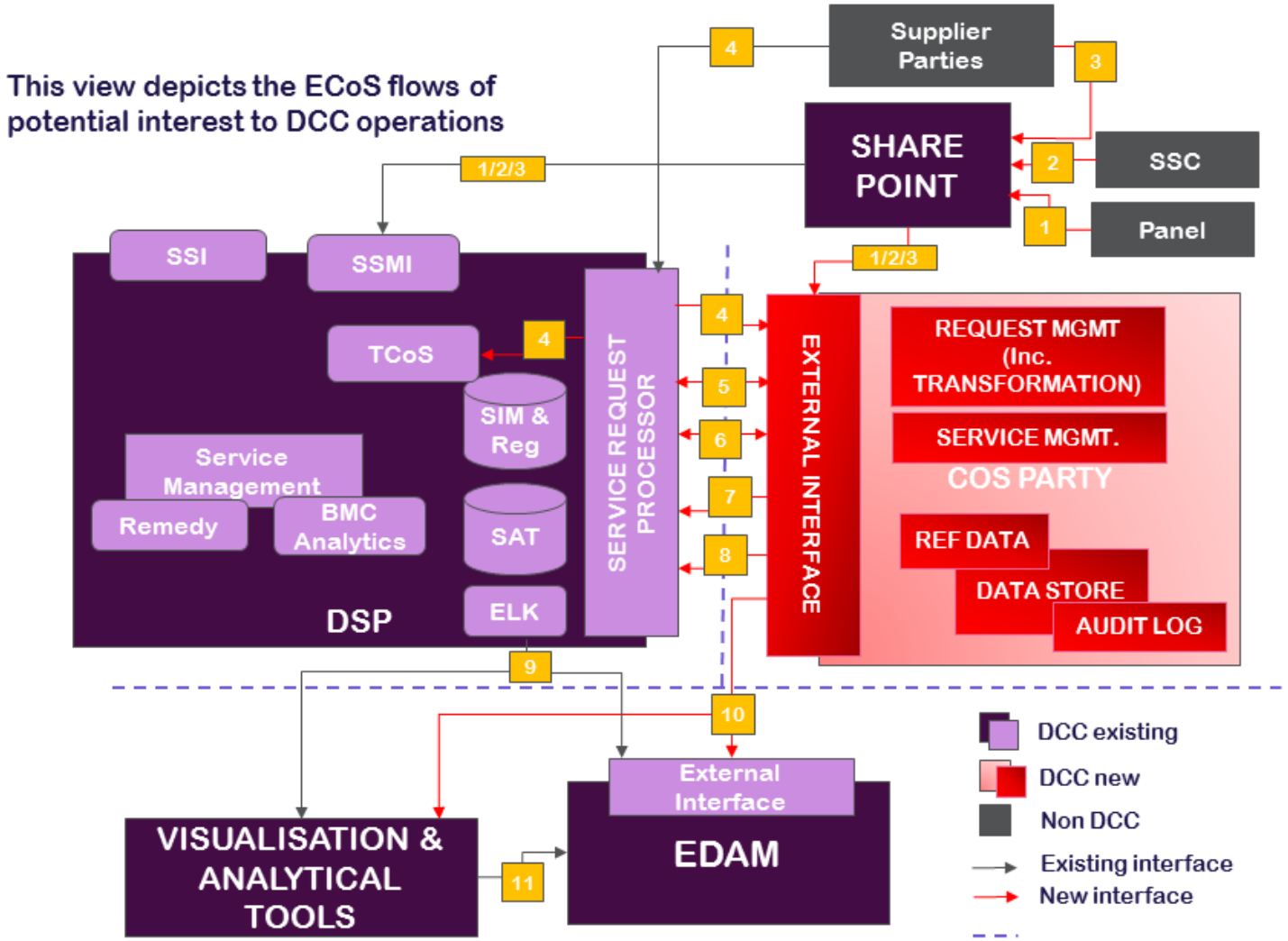
REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
14C	COUNTERSIGNED CoS SMETS1 RESPONSE	A Countersigned CoS SMETS1 response	Service Request Processor	CoS Party& Gaining Supplier	Message Based (XML based partly on DUIS specification)	SMKI XML Signing	HTTP Post
15	DCC ALERT N27	Notification to Losing Supplier of credentials change triggered by a: SMETS2+ Response; SMETS 2 + Alert; or SMETS1 Response.	Service Request Processor	Losing Supplier	Message Based	SMKI XML Signing	HTTP Post
16	CHANGE OF CoS PARTY CREDENTIAL REQUEST	Request from a Gaining CoS Party to a Losing CoS Party for changes of CoS Party credentials on SMETS2+ Note: - Change of CoS cannot be future dated - This flow does not apply to SMETS1 Devices as allocation of CoS Party to	Gaining CoS Party	Losing CoS Party (via the Service Request Processor)	Message Based	SMKI XML Signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		SMETS1 Devices will be rule based.					
17	CHANGE OF CoS PARTY CREDENTIAL SIGNED PRE-COMMAND	Each request includes the original CoS Party request and, for a SMETS2+ Device only, a corresponding signed GBCS command	Losing CoS Party	ACB (via the Service Request Processor)	Message Based	SMKI XML Signing	HTTP Post
18	CHANGE OF CoS PARTY CREDENTIAL COMMAND	Change of CoS Party Credential Command generated by the ACB after applying the relevant checks and Threshold Anomaly Detection	ACB	SMETS2+ Device	Message Based	SMKI Device ASN.1 Signing	
19	CHANGE OF CoS PARTY CREDENTIAL RESPONSE	Response telling the CoS Party the outcome of processing the CoS Party Change of Credentials instruction (possible outcomes: positive, negative or partial completion).	SMETS2+ Device	Gaining & Losing CoS Party (Via the Service Request Processor)	Message Based	SMKI Device ASN.1 signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		If the outcome is positive the alert will contain information on Gaining CoS Party and Loser CoS Party					
20	INCIDENT NOTIFICATION	Interface used by the CoS Party to raise incidents with DCC	CoS Party	Service Request Processor			
21	AGGREGATE ADT	Aggregate CoS is a function that will require agreement/approval by the Security Subcommittee (SSC) Existing process might need to be enhanced. Assume CoS aggregate files will be IKI signed by the SSC. This info will be used by the ACB only for Change of CoS	SSC	DSP and CoS Party			

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
22	OPERATIONAL FLOWS	It covers the flow of Service Audit trail information required to support DCC Operational process	CoS Party and Service Request Processor	Enterprise Data Analytical Model (EDAM)			

Operational impacts



REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
1	USER ID RANGES	Flow used for the sharing of User ID ranges	Panel	Cos Party and ACB (via External Interface and Service Request Processor respectively) - SharePoint will be used as a repository of data	File based	IKI	
2	AGGREGATE ADT	Aggregate CoS is a function that will require agreement/approval by the Security Subcommittee (SSC) Existing process might need to be enhanced. Assume CoS aggregate files will be IKI signed by the SSC.	SSC	DSP and CoS Party (via External Interface and Service Request Processor respectively) - SharePoint will be used as a repository of data			

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		This information will be used by the ACB only for Change of CoS					
3	ANOMALY DETECTION CoS (ADT) FORECASTS	Flow used for the sharing of forecast thresholds for CoS Event	Gaining Supplier	Cos Party and ACB (via External Interface and Service Request Processor respectively) - SharePoint will be used as a repository of data	File based	IKI	
4	CoS REQUEST	Change of Supplier Update Security Credential Request as issued by the Supplier Party acting as the Gaining Supplier.	Supplier Party (as Gaining Supplier)	Either TCoS or All CoS Parties (Via the Service Request Processor)	Message Based (XML based on DUIS specification)	SMKI XML Signing	HTTP Post – Except for TCoS
5	SIGNED CoS PRE-COMMAND	Each such message includes the original supplier's CoS Request and, for a SMETS2+ Device	CoS Party	Service Request Processor	Message Based (XML based partly	SMKI XML signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
		only, a corresponding signed GBCS command			on DUIS specification)		
	COUNTERSIGNED CoS SMETS1 RESPONSE	For a SMETS2+ Device, the Device Response to the GBCS command	Device via Service Request Processor	CoS Party	Message Based	SMKI Device ASN.1 signing	HTTP Post
		For a SMETS1 Device, a Countersigned CoS SMETS1 Response	S1SP via Service Request Processor	CoS Party	Message Based (XML based partly on DUIS specification)	SMKI XML signing	HTTP Post
6	CHANGE OF CoS PARTY CREDENTIAL REQUEST	Request from a Gaining CoS Party to a Losing CoS Party for changes of CoS Party credentials for the Device	Gaining CoS Party	Losing CoS Party via Service Request Processor	Message Based	SMKI XML signing	HTTP Post
	CHANGE OF CoS PARTY CREDENTIAL SIGNED PRE-COMMAND	Each request includes the original CoS Party request and, for a SMETS2+ Device only, a corresponding signed GBCS command	Losing CoS Party	ACB via Service Request Processor	Message Based	SMKI XML signing	HTTP Post

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
	CHANGE OF CoS PARTY CREDENTIALS RESPONSE	For a SMETS2+ Device, Device Response to the GBCS command	Device via Service Request Processor	CoS Party	Message Based	SMKI Device ASN.1 signing	HTTP Post
		For a SMETS1 Device, a message confirming the change		CoS Party	Message Based (XML based partly on DUIS specification)	SMKI XML signing	HTTP Post
7	INCIDENT NOTIFICATION	This flow is to raise incidents with DCC	CoS Party	DCC			
8	ALERTS	This flow covers Alert notification to other parties e.g. confirmation for receipt of requests from CoS Parties; notifications of errors	CoS Party	Other parties via Service Request Processor	Message Based	SMKI XML signing	HTTP Post
9	CHANGE OF CREDENTIAL AUDIT FLOW FROM SERVICE REQUEST PROCESSOR	It covers the flow of Service Audit trail information required to support DCC Operational process	ELK (Elasticsearch-Logstash-Kibana)	Enterprise Data Analytical Model (EDAM) and Visualisation and Analytical Tools	Direct connectivity		

REF	FLOW	DESCRIPTION	SOURCE	TARGET	INTERFACE TYPE	CERTIFICATION TYPE	TECHNOLOGY
10	CHANGE OF CREDENTIAL AUDIT FLOW FROM CoS	It covers the flow of Service Audit trail information required to support DCC Operational process	CoS Party	Enterprise Data Analytical Model (EDAM) and Visualisation and Analytical Tools	Direct Connectivity to access data		
11	Cos ANALYTICS	It covers the flow of Service Audit trail information required to support DCC Operational process	Enterprise Data Analytical Model (EDAM)	Visualisation and analytical Tools	Direct Connection?		

Appendix 10 - RAID Log (ECoS 1)

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
001	Managing delivery of the ECoS Programme	BEIS will need to decide who will fulfil the role of programme management and responsible for delivering the ECoS1 solution.				-	-	-
002	Magnitude of costs		For costing purpose, it is assumed that ECoS will be delivered as a standalone release.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
003	Magnitude of costs		The costing provided in this paper is a rough order of magnitude estimate based on the information available at the time from high-level impact assessment conducted by DCC and RFI responses.		Only a small percentage (8 out of 69) of Suppliers responded to the RFI to provide cost information regarding the implementation of CoS Party function, as such the ECoS1 costing provided in the options paper is a very rough magnitude of costs that is based on very limited data.	-	-	-
004	Impacted Supplier Parties				The full list of Supplier parties affected by ECoS1 cannot be identified upfront as the number of onboarded Suppliers will change over the duration of the programme. A	-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
					mechanism will be needed for managing this.			
005	Obtaining Registration Data from CSS	If the Ofgem Central Switching Service is in operation when ECoS go-live, CoS Party must be able to obtain Registration Data from CSS.	The CSS will notify the affected Gaining and Losing Suppliers of changes to Registration Data for a given Devices. It is assumed this information can be utilised for the validation of a CoS Event by the Losing Supplier acting as a CoS Party, thus ECoS will not impact the Switching Programme.	If the assumption is not valid, there will be an impact to the Switching Programme that have not been considered in the options paper.		1	5	5

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
006	ECoS 1 implementation Complexity			There are many parties involved in the ECoS 1 implementation. This creates complexities in co-ordinating the overall delivery across all impacted parties to meet the target date. To enable rollout of ECoS 1 all onboarded Suppliers need to prove that they can meet all CoS Party obligations in a similar way that they are required to undergo User Entry Process Testing for using other DCC Services. In addition, during the transition period, consideration is needed regarding on-boarding new DCC Users in the role of Supplier to ensure they are able to operate as CoS Party.	Different lead times from Suppliers to implement CoS Party	5	5	25

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
007	ECoS programme governance		A governance mechanism will be in place to manage and coordinate the all necessary activities for the delivery of the ECoS 1 solution.			-	-	-
008	Resource for implementation	All parties required to implement the solution must have the relevant resources available to work on the programme at the appropriate timescale	All parties required to implement the solution have sufficient resources are available to start working at the appropriate timescale	The implementation of ECoS 1 will require resources to be allocated by energy suppliers. There is a risk that the required resources may not available to all suppliers when needed. This risk is aggravated by the target implementation timescales, as any available resources are likely to have been allocated to other major programmes e.g. SMETS1 and the Faster Switching programme.	Supplier RFI responses indicate resources are not available for the required timescale.	3	5	15

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
009	DSP contract	DSP contract must run until the completion of the TCoS to ECoS migration.	An extension of the current DSP contract is approved to support the migration from TCoS to ECoS.	If TCoS migration is not completed before the final DSP extension period, the necessary contractual agreement will need to be in place to enable all Devices is migrated.		1	5	5
010	System integrator		CGI will be the System Integrator for the ECoS implementation			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
011	Test Environments		No additional DSP test environments are required to support an ECoS implementation			-	-	-
012	Testing		Testing with meters is required for ECoS 1 and ECoS 2			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
013	Impacted parties		SMETS1 S1SP is not expected to be impacted by ECoS			-	-	-
014	No changes to GBCS Specification		There will be no changes to GBCS specification required for ECoS.	If this assumption is not valid, this will increase the cost to deliver the programme.		1	5	5
015	Change of CoS Party		The Gaining CoS party knows the Losing CoS Party for the event of Change of CoS Party			-	-	-
016	Change of CoS Party		Change of CoS Party event cannot be future dated.			-	-	-
017	ADT		Aggregate Anomaly Detection Thresholds for CoS Events and Change of CoS Party to be defined by DCC and agreed by SSC.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
018	SMETS1 migration		There will be no new SMETS1 meter installation after March 2019. However, removal or changes to the Device ID to MPxN mappings will be possible.			-	-	-
019	DCC BAU resource		DCC Operational headcount is expected to be increased as a result of ECoS implementation and on-going BAU support			-	-	-
020	Data analytics		Business Intelligence and Management Information (BIMI) will be replaced by DCC Enterprise Data Solution by the time ECoS is implemented in 2021. Therefore, it is assumed no changes to BIMI for ECoS.	If this assumption is not valid, there will be an impact to the implementation cost.		1	3	3

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
021	ADT		Suppliers acting as a CoS Party should apply Anomaly Detection Threshold based on values given to them.			-	-	-
022	Change of CoS Party		There will be a process to trigger a Change of CoS Party event and this process will be defined as part of the detail design. It is assumed this process will be outside DSP.			-	-	-
023	SMETS1 Devices		For ECoS 1, the Suppliers will have the data on the Devices within its estate. .					

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
024	SoLR			For ECoS 1 to work in the event of a supplier failure (e.g. SoLR), where the losing Supplier may not be able to carry out the actions required of it as a CoS Party, functionality similar to that provided by ECoS 2 will need to be incorporated into the ECoS 1 design.		5	5	25

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
025	Enforcement of Supplier roles	Governance is required to ensure Suppliers are fulfilling the obligations of a CoS Party, such that CoS Requests are processed correctly and promptly.	The necessary governance is in place to ensure CoS Requests are processed correctly and promptly.	The Losing Supplier will have less vested-interested in the success of CoS, and that the Gaining Supplier will be responsible for the consumer-relationship at the point of CoS. There is a risk that avoidable inefficiency would be brought into the CoS process, where the Gaining Supplier is dependent upon, and must liaise with, the Losing Supplier for issue-resolution.	It requires tight regulations and robust enforcement to ensure that all Suppliers undertake their role as a losing supplier (acting as the CoS Party). This regulatory regime is likely to require a lot of oversight and there are likely to be many disputes that arise – all of which may be costly to manage and resolve.	3	3	9
026	Disclosure of ADT figures				Providing Anomaly Detection figures for CoS service requests between suppliers could constitute an unacceptable disclosure of	5	5	25

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
					sensitive commercial information.			
027	Broadcasting of CoS Events				Providing data relating to every CoS event to all suppliers gives rise to the risk that this data could be misused by market participants if monitoring and enforcement measures are not in place.	5	3	15

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
028	Resource for implementation			ECoS1 will have significant impacts to DCC Operations that will require changes to several business processes (e.g. Incident Management, User Onboarding, Supplier of Last Resort (SoLR)). There is a risk that the relevant Operations subject matter experts might not be available to work on ECoS1 at the required timescale due to commitments to other DCC release programmes.		3	3	9
029	Impacts to DCC and Industry not fully investigated			The extent of impacts to DCC and Industry not being fully investigated, there is a risk of underestimating the effort and costs for this option (e.g. SoLR, comms hubs ordering, provisioning of CoS Party certificates at point of manufacturing).		3	3	9

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
030	Impacts to Manufacturers not fully investigated			With each Supplier being the CoS Party for their Devices, this means supplier specific CoS Party certificates will need to be put on new Devices by manufacturers. This has not yet been considered in the solution and this could impact the cost for ECoS1.		3	3	9
031	No provision for new CSS interface		Each Supplier will have an interface with CSS via which they will have access to Registration Data, as such the ECoS1 costing does not include provision for Suppliers to implement a new interface for CSS.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
032	Single go live event		It is assumed that there will be a single Go live event which all parties involved in the service will support.			-	-	-
033	Integration testing		It is assumed that a UIT environment will be used for Suppliers to conduct integration testing with DSP to verify their CoS Party implementation.		A test strategy needs to be defined and agreed regarding how Suppliers can conduct integration testing to verify their CoS Party functions.	-	-	-
034	Test environment		CoS parties will need to integrate with DCC Pre-Prod environment if this environment is available at the time of implementation.					

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
035	DSP contract		DSP contract will be extended thus to cover the support required to complete the implementation of ECoS. A further assumption is that the TCoS to ECoS migration to be completed before the end of the DSP final contract extension.					

Appendix 11 - RAID Log (ECoS 2)

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
100	Magnitude of costs		For costing purpose, it is assumed that ECoS will be delivered as a standalone release.			-	-	-
102	Magnitude of costs		The costing provided in this paper is a rough order of magnitude estimate based on the information available at the time from high-level impact assessment conducted by DCC and RFI responses.		Nine third-party vendors were invited to respond to the RFI. Two vendors responded, of which only one provided the requested information regarding the software and service management costs. As such the cost estimate provided in this paper is a very rough order of magnitude based on very limited data.	-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
104	Obtaining Registration Data from CSS			The need to integrate the CSS with the CoS Party system results in a dependency between the two programmes. Such a dependency could increase the implementation risk associated with both programmes due to the need to coordinate development and testing activities across the two simultaneously.		3	3	9
105	Magnitude of costs		There will be one CoS Party in operation post migration. The cost estimate includes provision for DCC to appoint a Service	If this assumption is not valid, there will be an increase to the cost for implementation		1	5	5

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
			Provider to deliver the centralise CoS Party service.	and operational supports.				
106	SMETS1 Migration		The migration of SMETS1 is completed by 2020, i.e. before the planned roll-out date for ECoS.	If the SMETS1 migration is not completed within the current agreed timescale, a new mechanism will need to be defined to allow details of newly migrated SMETS1 devices to be loaded onto the CoS Party. This mechanism will need to be costed accordingly.		3	3	9

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
107	DSP contract	DSP contract must run until the completion of the TCoS to ECoS migration.	An extension of the current DSP contract is approved to support the migration from TCoS to ECoS.	If TCoS migration is not completed before the final DSP extension period, the necessary contractual agreement will need to be in place to enable all Devices to be migrated.		1	5	5
108	System Integrator		CGI is expected to be the System Integrator for the ECoS implementation			-	-	-
109	Test Environments		No additional DSP test environments are required to support an ECoS implementation			-	-	-
110	Testing		Testing with meters is required for ECoS 1 and ECoS 2			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
111	Impacted Parties		SMETS1 S1SP is not expected to be impacted by ECoS			-	-	-
112	No changes to GBCS Specification		There will be no changes to GBCS specification required for ECoS.	If this assumption is not valid, this will increase the cost to deliver the programme.		1	5	5
113	Change of CoS Party		The Gaining CoS party knows the Losing CoS Party for the event of Change of CoS Party			-	-	-
114	Impacted Parties		Energy suppliers are not expected to be impacted by the migration from TCoS to ECoS 2			-	-	-
115	Change of CoS Party		Change of CoS Party event cannot be future dated.			-	-	-
116	ADT		Aggregate Anomaly Detection Thresholds for CoS Events and Change of CoS Party to be defined by DCC and agree by SSC.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
117	BAU Resource		DCC Operations headcount is not expected to be increased for on-going BAU support	If this assumption is not valid, there will be an increase to the DCC cost for on-going operations.		1	1	1
118	Data analytics		Business Intelligence and Management Information (BIMI) will be replaced by DCC Enterprise Data Solution by the time ECoS is implemented in 2021. Therefore, it is assumed no changes to BIMI for ECoS.	If this assumption is not valid, there will be an impact to the implementation cost.		1	3	3
119	Change of CoS Party		There will be a process to trigger a Change of CoS Party event and this process will be defined as part of the detail design. It is assumed this process will be outside DSP.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
120	No costing for CSS-CoS Party interface implementation				The ECoS2 costs do not include the CSS – CoS Party integration costs.	-	-	-
121	Single go live event		It is assumed that there will be a single Go live event which all parties involved in the service will support.			-	-	-
122	Connectivity to SharePoint		It assumed that a secured connectivity to SharePoint will be established via the internet outside of the gamma network for retrieval of ADT files			-	-	-
123	Test environment		CoS parties will need to integrate with DCC Pre-Prod environment if this environment is available at the time of implementation.					

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
124	DSP contract		DSP contract will be extended thus to cover the support required to complete the implementation of ECoS. Further assumption would be for the TCoS to ECoS migration to be completed before the end of the DSP final contract extension.					
125	SMETS1 migration		There will be no new SMETS1 meter installation after March 2019. However, removal or changes to the Device ID to MPxN mappings will be possible.			-	-	-

Risk reference	Title	Dependency	Assumption	Risk	Issue	Probability 1- low 3 - medium 5 - high	Impact 1- low 3 - medium 5 - high	Overall risk rating
126	TCoS migration			If TCoS migration were to complete during Q4 2022, this would leave little contingency time before the first DSP contract extension window expires and would increase implementation risk if migration takes longer than the anticipated 12 months.		1	5	5

Appendix 12 – Defined Terms

Term	Definition
Access Control Broker (ACB)	In the context of CoS, the ACB is the DSP component responsible for applying Threshold Anomaly Detection and: ▪ For a SMETS2+ Device, Cryptographic Processing relating to the generation and use of a Message Authentication Code; or ▪ For a SMETS1 Device, Cryptographic Processing relating to the generation and use of Digital Signatures.
Centralised Switching Service (CSS)	The source of Registration Data to be implemented by 2021
Change of Supplier (CoS)	As described in this Section 3.1 of this document
CoS Event	As described in this Section 3.1 of this document
CoS Party	The entity performing the tasks ascribed to the CoS Party within this document
CoS Request	A Service Request whose Service Reference Variant is 6.23
Data Service Provider (DSP)	The DCC's provider of infrastructure to link between DCC User systems and the SMWAN
EDAM	Enterprise Data Analytical Model
Gaining Supplier	As defined in section 3 of this document
Losing Supplier	As defined in section 3 of this document
Market Participant	An identifier used in Registration Data to identify Supplier Parties

Term	Definition
Identifier (MPID)	
MPxN	Either an MPAN or MPRN
Relevant CoS Party	In relation to a specific Device, the CoS Party responsible for processing CoS Requests
Service Request Processor	The part of the DSP other than the ACB, SMKI Services and TCoS
Signed CoS Pre-Command	A message that includes the Gaining Supplier's CoS request and, for a SMETS2+ Device only, a corresponding signed GBCS command
SMETS1	The Smart Metering Equipment Technical Specifications 1
SMETS1 Device	One of the following: (a) a SMETS1 ESME; (b) a SMETS1 GSME; (c) a SMETS1 CHF; (d) a SMETS1 GPF; (e) a SMETS1 PPMID; (f) a SMETS1 IHD; and (g) any other device operating on a home area network created by a SMETS1 CHF
SMETS2+ Device	A Device which is not a SMETS1 Device
Transitional Change of Supplier (TCoS)	The part of the DSP performing the tasks ascribed to the CoS Party in the current version of the SEC Service Request Processing Document