Data Communications Company

# Consultation on changes to the SMETS1 Transition and Migration Approach Document (TMAD) for:

1) MOC Secure; and

2) Minor changes to apply to all cohorts (IOC, MOC and FOC).

**Date:** 13 March 2020

**Classification:** DCC Public

**Filename:**

# 1. Introduction and Context

A number of energy Suppliers have installed first generation smart devices (known as SMETS1 devices) in consumers' premises across Great Britain. The Data Communications Company (DCC) has designed a solution for the enrolment of SMETS1 devices into its network. Part of DCC's plan to deliver SMETS1 services involves a detailed approach for migrating SMETS1 Installations into DCC's systems. The detailed technical and procedural requirements of this approach are set out in the SMETS1 Transition and Migration Approach Document (TMAD). The current TMAD (which covers requirements for the initial operating capability (known as 'IOC') for SMETS1 Services) was first designated by the Secretary of State on 21 June 2019 and included in the Smart Energy Code (SEC) from version 6.14 onwards as Appendix AL of the SEC.

Subsequently, there are a limited number of changes to the TMAD that are required for the Middle Operating Capability (MOC) and Final Operating Capability (FOC). The MOC release includes two cohorts of devices, a Honeywell Elster device set operated via Morrison Data Services (MDS) as the Smart Meter System Operator (SMSO) (henceforth referred to as MOC (MDS)), and a Secure device set operated by Secure as the SMSO (henceforth referred to as MOC (Secure)). The FOC release covers the Trilliant and Landis+Gyr (L+G) device sets, currently operated by three SMSOs. DCC has updated a draft version of the TMAD to include changes for MOC (MDS), which was consulted on up to 6 September 2019 and concluded on 22 November 2019[1] and which BEIS is currently consulting on designating[2]. Concurrently, DCC is also developing subsequent versions of TMAD that covers the MOC (Secure) cohort and FOC cohort, this consultation covers the MOC (Secure) cohort, with the FOC consultation having concluded on 22 January. DCC considers it prudent to provide a separate TMAD consultation for each MOC cohort and FOC so that the changes can be clearly understood by those impacted.

This Secure version of the TMAD has taken as its starting point for mark-up, the TMAD (MDS) version that will be designated by BEIS on 13 March 2020.

The changes made to the TMAD (Secure) version within the scope of this consultation are specific to the technical requirements necessary to migrate the MOC (Secure) cohort. Changes which are specific to Secure are described in Section 2 of this document, whereas generic changes that apply to all cohorts are described in Section 3. All Secure-specific and generic cohort changes are listed in Section 4.

In addition, some minor administrative changes have also been made to parts of the TMAD that generally apply to all cohorts (including IOC, MOC and FOC), which are intended to provide additional clarity. These are detailed in Section 3 of this document.

Should the content of this document require further changes, DCC will consult on these at a later date.

[1] https://www.smartdcc.co.uk/customer-hub/consultations/dcc-responses/consultation-response-to-dcc-consultation-on-tmad-for-mds/

[2] https://smartenergycodecompany.co.uk/latest-news/beis-consultation-on-re-designation-date-of-the-transition-and-migration-approach-document-to-support-the-dccs-smets1-service/

This consultation document is seeking views on the changes to the TMAD set out in in this document, as well as the date for its re-designation by the Secretary of State.

**Other changes that will apply to the version of the TMAD for the MOC (Secure) cohort which are the subject of separate consultations**

It should be noted that there are other TMAD consultations[3] that have previously been issued which include content that it is proposed that would also apply to the MOC (Secure) cohort. A summary of these consultations, the status of them and the relevant changes are set out below.

| Consultation Document | Current Status | Nature of change | TMAD clause |
|---|---|---|---|
| SMETS1 Uplift 1.1 | Consultation closed, DCC in process of concluding. | Changes to allow the Secretary of State to amend the EPCL where manifest errors have occurred. | TMAD Clause 3.7 |
| SMETS1 Uplift 1.1 | Consultation closed, DCC in process of concluding. | Amendment to definition of Migration Authorisation to allow a single Migration Authorisation by the Electricity Supplier to apply across an Affiliate Gas Supplier. There are also a few consequential changes within Clause 4 consistent with this requirement covering consequently changes for providing certificates for the ESME and GSME by the Electricity Supplier. | TMAD Clause 2 Clause 4 Clause 6.4 |
| SMETS1 Uplift 1.1 | Consultation closed, DCC in process of concluding. | Migration Common File definition amended consistent with split supply processing requirement in Clause 5.8 and processing at Step 5.9.10 removed. | TMAD Clause 2 Clause 5.8 Step 5.9.10 in Table 5.9 |

[3] https://www.smartdcc.co.uk/customer-hub/consultations/consultation-on-regulatory-changes-for-smets1-uplift-11/ and https://www.smartdcc.co.uk/customer-hub/consultations/tmad-for-foc/

| | | | |
|---|---|---|---|
| SMETS1 Uplift 1.1 | Consultation closed, DCC in process of concluding. | Steps 5.9.5 to 5.9.9 amended for the improved file sequencing algorithm. | TMAD Table 5.9 |
| SMETS1 Uplift 1.1 | Consultation closed, DCC in process of concluding. | Phase 'and associated steps' added to clarify processing for roaming SIMS. | TMAD Clause 5.1 (b) (i) |
| FOC | Consultation closed, DCC in process of concluding. | To provide a more favourable consumer experience, DCC is proposing to accelerate the migration of recently dormant meters where it is expected that the new absence of a smart meter service has the greatest impact on a consumer's experience and view. | New Definition<br><br>TMAD Clause 4.30 and 4.29<br><br>TMAD Table 5.10<br><br>5.10.10 and 5.10.15 |
| | Consultation closed, DCC in process of concluding. | Minor change to reflect consistent usage of Clause throughout the document | TMAD Clause 12.1 and 14.1 |

## 2. Overview of TMAD Changes Specific to MOC (Secure)

This section provides an overview of the TMAD changes which are specific to MOC (Secure).

A comparison of the Migration arrangements with the other cohorts, is shown in Table 1 for each phase of Migration. Key differences are outlined, together with the main TMAD sections that are affected. Where there is no change to the existing TMAD sections which apply to the Secure Migration process, this is stated. To further aid understanding of the context of the changes, the last column provides a cross reference to the TMAD Process Flow given in Appendix A.

The specific changes showing the TMAD clauses affected, which specify the precise wording, are given in Section 4.

**Table 1 – Overview of TMAD Changes**

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| **Planning, Scheduling and Authorisation** | For Active Meters, Responsible Suppliers instruct firmware upgrades to make devices eligible for Migration (at EPCL versions), and instruct all pre-enrolment configuration changes necessary to meet the requirements for the Secure cohort that will be set out in Appendix AM to the SEC, the SMETS1 Supporting Requirements (S1SR). | These steps are not detailed in the TMAD as they are matters that need to be arranged between Responsible Suppliers and their SMSO. | 1 |

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| | For Dormant Meters, DCC on behalf of the Responsible Supplier, performs firmware updates to make devices eligible for Migration (at EPCL versions).<br><br>There is a 2-part configuration approach for Dormant Meters that is explained in more detail in Section 2.4.2. DCC applies Part 1 pre-enrolment configuration. This 2-part approach doesn't manifest in any change to the Secure TMAD, because this is still considered a pre-requisite for Migration in line with the current TMAD requirements.<br><br>This 2 part approach for pre-enrolment configuration satisfies the requirements for the Secure cohort will be set out in Appendix AM to the SEC, the SMETS1 Supporting Requirements (S1SR). | No Change for MOC (Secure) Cohort | 2 |
| **Data Validation** | For Dormant Meters, DCC on behalf of the Responsible Supplier, applies the Part 2 pre-enrolment configuration. | No Change for MOC (Secure) Cohort | 3 |
| | As with other cohorts, the validation of the MCF file is done by the DCC's IOC Service Provider's reusable MCF validation functionality. | No Change for MOC (Secure) Cohort | 4 |
| | Suppliers need to be aware that the pre-enrolment configuration will be verified at certain points during Migration: | No Change for MOC (Secure) Cohort | 3 & 5 |

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| | i) at the earliest opportunity after the Requesting Party receives and validates the MA; and<br><br>ii) after the Requesting Party receives the MVF early on the Migration day.<br><br>The configuration must satisfy the verification checks for the Installation to proceed any further in the Migration process. Any devices that fail the check will be rejected from Migration.<br><br>The concept that pre-enrolment configuration must comply with requirements set out in the S1SR hasn't changed for Secure. | | |
| | In addition to configuration checks, additional device checks are applied by the Requesting Party such as checking that ZigBee devices are on the CHF Whitelist and pre-payment key verification. Any devices that fail the checks will be rejected from Migration. As there are no WAN configuration changes for this cohort, some of the device checks can be carried out up to 7 days in advance of devices being handed over to the DCC. This makes Migration of Secure meters different from other cohorts in that only the SUA key change is performed during Migration. | 16.9, C1, C2 | 6 |
| | Prior to generation of the MEF file, the account that the meter operates under, is switched from the Supplier account in the SMSO to a DCC account. At this point the Supplier loses the ability to communicate with the device and it passes to the control of the DCC, therefore communication to | No Change for MOC (Secure) Cohort | 6 |

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| | it by the Supplier via the SMSO and the DCC will not be possible until the Migration of the Installation containing the device has completed, noting that UTRN top up will still be available as described in Section 2.1.<br><br>Where Migrations are authorised by the Supplier for a specific day (e.g. Monday), completion of commissioning is estimated to take, on average, until the evening of the same day (i.e. Monday evening). In worst case scenarios it could take up to the evening of the second day after Migration day (i.e. Wednesday evening). Where Migrations are authorised by the Supplier for no specific day in a specific week, DCC will have the flexibility to schedule the day on which the Migration commences, in which case from the point of commencement the same timescales apply. | | |
| | There is no MGF file used during Migration as there is no change in WAN configuration. The MEF file instead contains all the required information that is passed from the Requesting Party to the S1SP and DCO. | 16.15 | 7 |
| **Device Testing** | As with other cohorts, the handover of the device to the DCC Systems entails a process whereby cryptographic keys on the meter are changed from Supplier-specific keys to those used by the DCC system. Secure Meters use a Single Use Authentication (SUA) Key which needs to be applied to both the GSME and the ESME using a “key rotation” process. | 5.4A, C5, C6 | 8 |

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| | Should there be an error detected during the rotation of the GSME SUA key, the device rollback will be invoked. See Section 2.3 below for further details about SUA Key Rotation and Rollback of a Secure Meter.<br><br>After such a rollback, Secure have stated that the device will have full functionality that can be operated using the standard tools and methods available to the Supplier, including the ability to revert the pre-enrolment configuration should this be required.<br><br>Migration can be reattempted, however for active meters, this will require the Supplier to resubmit a Migration Authorisation for the Installation in a subsequent Migration Week. | 16.11 | 9 |
| | | | |
| | Suppliers don't need to be conversant with the technical details of SUA keys, but they appear in the TMAD and are shown in the Migration schema which defines the XML format of the Migration files. | 10.1, 11.3 | N/a |
| **Commissioning & Prepayment Top-Up (UTRN Generation)** | The Commissioning of Secure Installations by DCC will follow the same process that has been undertaken for the other cohorts. Where the Supplier has elected to commission the devices itself, it will receive a S1SP Commissioning File (SCF) which can then trigger the sending of the relevant commissioning Service Requests. In all other cases, DCC will commission the devices and the Supplier will be notified via an alert. | No Change for MOC (Secure) Cohort | 10 |

| Migration Phase | Comparison with Other Cohorts | TMAD Sections Affected | Refer to TMAD Process Flow in App A |
|---|---|---|---|
| | For a temporary period post Migration of a SMETS1 Installation, UTRN generation requests from Payment Service Providers (PSPs) can be processed via the Secure SMSO, as described in Section 2.1. | 3.14B, 3.14C, 3.14D | 10 |

| | |
|---|---|
| **TMAD Q1** | *Do you have any general comments on the changes to the TMAD for MOC (Secure)?* |

Further to the above key differences that relate directly to the Migration process, the sections below provide further information about these differences, as well as more general differences due to the characteristics of the systems used for Migration of Secure Meters.

### 2.1 UTRN Cutover Arrangements

For UTRN top ups which take place via PSPs using Secure's RNSP interface, DCC is proposing a temporary cutover UTRN period (the UTRN Period), that applies from the point that the devices are commissioned with the DCC.

This is intended to give sufficient time for Suppliers to operate their devices through the DCC so that they can manage top up requests from PSPs.

The proposed UTRN cutover arrangements are as follows:

i) Currently Payment Service Providers (PSPs) can request UTRNs via Secure's RNSP interface from the Secure SMSO and can continue to do so during the Migration up to the UTRN Period (see below).

ii) Any other UTRN requests made other than using Secure's RNSP interface can continue up to the point of the account switch. Once a meter has been commissioned into the DCC, UTRN requests can be sent to the DCC using SRVs by the Responsible Supplier.

The UTRN Period applies from the point at which the S1SP generates the successful response to the Commissioning Service Request (SRV 8.1.1) for a meter, for a period of 48 hours after this S1SP processing step. During this time, a UTRN request will continue to be processed by Secure SMSO.

It should be noted that should a Supplier wish to continue to request UTRNs from the Secure SMSO during this UTRN period, they will need to ensure that their arrangements with the SMSO enable them to continue to submit such UTRN requests.

After this UTRN Period, any attempt to send a UTRN request to the Secure SMSO via Secure's RNSP interface will result in an error message which will provide the Payment Service Provider with a reason why the request failed, subject to them having arrangements in place with the Secure SMSO to pass this error message back.

From this point, the UTRN request must be processed via the sending of a Service Request by the Supplier over the DCC User Interface (using DUIS 3).

DCC is proposing that the UTRN Period is limited to 48 hours. DCC is inviting views on this via this consultation. When deciding on the UTRN Period the DCC considered several factors:

- None of the commissioning SRVs result in device communication and are used to build the details of the migrated Installation within the Inventory, therefore there is minimal risk in the commissioning process failing.

- DCC has also encountered a small number of issues where the N55 alert has been sent to the wrong party. This would introduce delays in the ability of a Supplier to operate a meter through the DCC service. This occurs due to a change of Supplier processes coinciding with the generation of the N55 alert where the registration data has not been updated in a timely manner. DCC has implemented a fix for this issue.

- The N55 alert is generated by the S1SP and passed to the DSP before transmission to users. There is a theoretical risk that the N55 is lost during transit, but this is very low due to the interface design between S1SP to DSP and DSP to Suppliers. DCC has no evidence that this has ever occurred.

- As the N55 alert and the COF, which could also be used as a trigger to switch Supplier systems from SMSO to DCC, are generated by two separate components, there is minimal risk that both of these will fail to be delivered.

Therefore, DCC feels that the proposed UTRN period of 48 hours, is sufficient time for Suppliers to switch to operating the meter and requesting UTRNs through the DCC service.

Suppliers should note the absence of any liability for DCC should it fail to discharge UTRN cutover obligations imposed on it in the TMAD, in the event that parties should suffer financial loss as a result. Refer to Section M2 of the SEC, Limitation of Liabilities.

| | |
|---|---|
| **TMAD Q2** | *Do you have any comments on the UTRN cutover arrangements including the appropriateness of the proposed UTRN period (48 hours) for processing the UTRN requests via the SMSO after the device has been commissioned?* |

### 2.2 Eventual Separation of the Secure SMETS1 SMSO System from the S1SP System

Secure operate as both SMSO and S1SP, using the same underlying SMSO system. Section G of the SEC requires that all DCC live systems are required to be separate, which includes all S1SP systems. Once all Migrations have been completed, it will be necessary to enforce separation between the S1SP system and any Secure SMSO system. The proposed changes will create an obligation to decommission interfaces to the S1SP Systems that are no longer needed (including, but not necessarily limited to between the S1SP and SMSO). In practice this will be done by severing all interfaces to the S1SP from other systems, including any Secure SMETS1 SMSO system, which it no longer needs to interface with, once all the Migrations have completed. The practical effect of this will be that, should Secure SMSO wish to continue to provide services, it will not be able to use what is currently the SMSO system, as this will form part of the S1SP system that is required to be separate. DCC proposes that this separation will happen 15 months after the “last” entry for the Secure cohort has been added to the Eligible Products Combination List. For these purposes DCC will measure a 12 month period in which there have been no further additions to the EPCL

for the Secure cohort, plus an additional 3 months of time contingency. This is currently due to occur on 16 November 2020, which will result in the separation occurring in February 2022.

| | |
|---|---|
| **TMAD Q3** | *Do you have any comments on the timescales for Separation of the Secure SMETS1 SMSO System from the S1SP System?* |

### 2.3 SUA Key Rotation and Rollback of a Secure Meter

During the Migration of an MOC (Secure) meter, there is a point of no return beyond which, should any Migration processing steps fail prior to the commissioning of the devices in the DCC, the SMETS1 Installation will not be rolled back to the SMSO. This point is when the SUA key change has taken place on the GSME. Before this point, should the Installation be rolled back, it is possible for full operation of the devices to recommence via the SMSO system. However after this point, Secure SMSO have stated that, as full operation on the SMSO cannot be supported (due to the reasons set out below in Table 2), it would no longer wish to support operation of such devices via the SMSO system. Consequently there is no benefit in rolling back the Installation after this point and introducing additional processing steps.

For a dual fuel installation, the GSME keys are rotated first and successful confirmation is required prior to rotating the ESME keys. The possible scenarios that can occur during the key rotation of the ESME and GSME are given in Table 2 below, showing where rollback will be initiated. For a single fuel installation, rows 1 – 3 don't apply.

**Table 2 – SUA Key Rotation Scenarios**

| No | GSME SUA | ESME SUA | Scenario Description | Rollback |
|---|---|---|---|---|
| **1** | Success | Success | This is the "Happy Path" outcome leading to Commissioning of the Installation. | N/A |
| 2 | Failed | Not Attempted | GSME communicating but SUA failed, and therefore GSME key hasn't rotated. | Rollback initiated as key change not taken place. |

| No | GSME SUA | ESME SUA | Scenario Description | Rollback |
|---|---|---|---|---|
| 3 | Attempt, but unable to send response | Not Attempted | Attempt to rotate GSME SUA key, but response not received by S1SP. The probability of this scenario is extremely low and is mitigated as described in Table 3 below. | Rollback will only be initiated if GSME SUA key is confirmed as not rotated. |
| 4 | Success | Success, but unable to send response | GSME key rotation successful, ESME key also rotated but response not provided to S1SP. Similar to above, the probability of this scenario is extremely low and is mitigated as described in Table 3 below. | Rollback not initiated. |
| 5 | Success | Failed | GSME key rotation successful, ESME SUA rotation failed. | Rollback not initiated. |

Refer to Section 2.3.2 below for the steps in the event of a failure including where rollback is not initiated.

Once the keys are rotated, they cannot be undone using any facility provided by the Secure Migration design. Although the current EPCL firmware version does support the reset of the SUA key, DCC recommends that this feature won't be made available on the basis that it would entail additional security arrangements to be put in place. The limited additional risk as shown in Section 2.3.1 below (of delaying the point of no return from the key rotation of the GSME to the key rotation of the ESME), would not justify the cost to implement the additional security arrangements. Such security arrangements would need to cover the DCC business process that would provide any capability for Suppliers to securely request a SUA key from the DCO.

### 2.3.1 Error Scenarios and Mitigations

DCC recommends the point of no return should be set in this way because of the following:

- After this point, although the device would be stranded in the Migration process, there wouldn't be any point passing the device back under SMSO control because Secure have stated that its operation on the SMSO would no longer be supported as well as the possibility for re-Migration of the SMETS1 Installation which would also not be supported.
- UTRN top ups will still be available for both meters as provided by existing SMSO and PSP arrangements. This facility will be available as the UTRN Period would not have started as device commissioning won't have been initiated.
- The error scenarios and associated risks are considered next which explains why DCC considers this conclusion is acceptable.

The error scenarios that could give rise to SUA key rotation failure, or failure to receive confirmation of successful key rotation, are considered in the table below in the following areas:

- Communications within the WAN and HAN
- Firmware
- Hardware

Very low failure is expected during Device Testing, because of the risk mitigations applied in these areas as detailed in Table 3.

**Table 3 – Error Scenarios and Mitigations**

| No | Error Scenario & Risk | Mitigation |
|---|---|---|
| 1 | Possibility of SIM / APN changeover failing within the Communications Head during Migration. | There is no WAN configuration change in the Secure Migration solution. Secure's Migration solution does not entail a SIM / APN change which potentially could be a problematic step. |
| 2 | Failure of the WAN/HAN affecting communications prior to key rotation on the GSME | For a communicating Secure GSME, communications checks are undertaken:<br>• After receiving the MA file, the Requesting Party performs a CHF communications check to ensure that both meters have communicated to the SMSO. This check is performed within 2 hours of receiving the MA file. |

| | | |
|---|---|---|
| | | • Before generating the MCF file, the Requesting Party checks the device configuration and applies configuration as required for dormant devices.<br><br>• On receiving the MA, the Requesting Party checks that the GSME must have communicated with the CHF within the last 24 hours.<br><br>• Post receiving the MVF file and before generating the MEF file, the Requesting Party validates the configuration for active and dormant devices is applied.<br><br>Thus, when a device reaches the SUA key rotation step, it's already proven to be communicating in a healthy manner which means that there is less likelihood of intermittent WAN/HAN issues at the SUA key rotation step.<br><br>This gives assurance that the Communications network is behaving reliably as a prerequisite for key rotation. |
| 3 | Failure of the WAN/HAN affecting communications during key rotation on GSME.<br><br>In this scenario it's assumed that the GSME key has not rotated successfully but there may be an issue sending a successful acknowledgement back to the CHF. | There is a retry mechanism within the Secure Installation that will push the status from the GSME to the CHF for certain retry attempts.<br><br>This is an edge case scenario where, given the reliability previously assured in Scenario #2, that communications would fail permanently at the exact moment of sending the response.<br><br>In this scenario, rollback will only be possible where there is confirmation that the GSME key has not rotated. Otherwise, Secure do not advise rollback as the Secure SMSO would not support this scenario and it could entail the Supplier to make arrangements with the SMSO to rectify. |
| 4 | Failure of the WAN/HAN affecting communications prior to or during key rotation on ESME. | For a communicating Secure ESME, communication is not dependent on the HAN as the CHF is directly connected to the ESME. |

| | | |
|---|---|---|
| | | This scenario would entail that the Supplier makes arrangements with the Secure SMSO to rectify, as there is likely to be a device-specific problem. |
| 5 | Failure of the device firmware | This is not really a Migration scenario as a firmware issue would prevent the device being added to the EPCL.<br><br>It would not be rectified by the availability of rollback as a re-Migration attempt would only give rise to the same error.<br><br>Furthermore, this scenario would not affect a specific device but all devices for that EPCL and is mitigated prior to Migration by way of:<br><br>• Testing of SUA key change at the EPCL version done in PIT and SIT. |
| 6 | Failure of device hardware | Failure of the device hardware would be a scenario specific to the particular device. This scenario would not be rectified by the availability of rollback and, similarly to Scenario #4, the outcome would be a Migration failure, as a result of a likely device-specific problem. |

### 2.3.2 Steps in the Event of Failure

As explained in the above section, due to the device checks that are performed prior to SUA key rotation there is very low risk of failure.

In the event that rollback is required, it entails handing back all the devices, that comprise the Installation, to the Supplier to operate via the SMSO. This is done by switching the account that the devices operate under, from the DCC account to the Supplier account so that control is returned to the Supplier to operate it. For active meters, the re-Migration of the Installation must be resubmitted by the Supplier using a new Migration Authorisation.

In the event that the device cannot be rolled back, the device would remain “stranded” in the Migration process and reported as a Migration failure. In this scenario, UTRN top ups by the PSP will still be available for both meters. Suppliers will need to make arrangements with Secure SMSO to handle this scenario, given that the device might need to be replaced.

Suppliers are informed of any Migration failures in the S1MIG-002 - Detail Report: Migrations Completed Unsuccessfully.

| | |
|---|---|
| **TMAD Q4** | *Do you have any comments on SUA and the implications for Rollback?* |

## 2.4 Changes to the Configuration of Meters

### 2.4.1 Active Meters

The configuration update approach for Responsible Suppliers of active meters which is being proposed for Secure in this version of TMAD is that the Responsible Suppliers will apply the configuration that is required for pre-enrolment themselves under an arrangement with the Secure SMSO.

For active devices, all parameters will have to be applied as required. Secure recommend that all parameters are applied before the Supplier provides the MA file to the DCC.

All configuration parameters for active meters will be validated by Secure Requesting Party, which happens at two points during Migration for all parameters i) after the Requesting Party receives and validates the MA and prior to it generating the MCF ii) after the Requesting Party receives the MVF and prior to it generating the MEF on the day of the Migration. In the event that any parameters are not at their required values, the Installation will be rejected from the Migration process.

The requirements for pre-enrolment configuration will be documented in the SMETS1 Supporting Requirements (S1SR).

An earlier proposal that DCC presented in previous multilaterals was the use of a two-part configuration process for active meters. It was suggested that Part 1 of the configuration process would be carried out by Suppliers using tools that are provided by Secure SMSO, while Part 2 would be carried out by DCC using the Secure Requesting Party and using software developed as part of the Migration system originally

intended for DCC. The rationale for having a two-part process was that the SMSO considered the Part 1 configuration to be mainly consumer-impacting, needing to remain under the control of the Responsible Supplier, whereas the Part 2 configuration is system operability-impacting and therefore could be applied by DCC (the Requesting Party) on the active Suppliers' behalf.

While DCC do not envisage insurmountable programme difficulties in orchestrating and applying Part 2, there has been further consideration of the implications. Primarily, the responsibility for the outcome of applying the configuration on every active device would transfer from the Responsible Supplier to the DCC. The commercial arrangements to accommodate this would be the key blocker. Risk mitigation gives rise to fundamental changes including: renegotiation of TMAD liabilities; DCC/Secure commercial agreements and supplier agreements as well as seeking further testing assurances from Secure.

The timescales for solution delivery might be impacted because of: more complex and lengthy testing arrangements, potentially involving suppliers; lengthy negotiation of change requests and contracts changes before development work can start.

DCC acknowledge that there would be efficiency benefits of a DCC-provided centralised service, including the potential for fewer rejected Migrations, but given that some Suppliers' feedback indicates that they would prefer to do this themselves, and in order for DCC to meet its obligations of delivering timely capability and enabling all meters to be enrolled, DCC is of the opinion that Suppliers will apply all configuration parameters themselves for Active Meters.

DCC has been engaging with Suppliers on a bilateral and multilateral basis to confirm that they understand the proposed configuration approach which is being proposed by this Secure TMAD, particularly as the approach is different to that presented in earlier multilaterals. Key feedback is required from Suppliers on their capability to implement it in timescales which support their Migration of Active Meters from June 2020. DCC would like to use this consultation as a means to obtain feedback on this capability.

The Supplier may contact the Secure SMSO or solution provider for guidance on executing the configuration changes on active devices.

| | |
|---|---|
| **TMAD Q5** | *Do you have any comments on the process for the configuration of active devices for MOC (Secure)?*<br><br>*Do you have any comments on your ability to apply configurations to the active devices in time to support Migration from June 2020?* |

### 2.4.2 Dormant Meters

The configuration update approach for Dormant Meters which is being proposed for Secure in this version of TMAD is that Secure will check and apply the configuration parameters on behalf of the DCC.

The configuration will be applied in two parts. Part 1 will be applied by the Secure SMSO Helpdesk as part of the Dormant Meter Readiness Process (DMRT), and Part 2 will be applied by Secure Requesting Party using software developed as part of the Migration system. Part 2 will be applied after the Requesting Party receives and validates the MA file and prior to generating the MCF file. For both parts, Secure will first check the parameter values and only where they are not the required values for pre-enrolment will they be changed to the required values.

As with active meters, configuration parameters for dormant devices will be validated by Secure Requesting Party post receipt of the MVF file. In the event that any configuration parameters are not at their required values, the Installation will be rejected from the Migration process and will be reattempted by DCC in another week.

| | |
|---|---|
| **TMAD Q6** | *Do you have any comments on the process for the configuration of dormant devices for MOC (Secure)?* |

## 2.5 Exclusions from the Migration Process

The following types of devices are excluded from the scope of Migration and are not considered in the TMAD for the Secure cohort:

1. **Third Party devices**. Secure do not maintain details for any type of third party (non-Secure manufactured) devices that are joined to the HAN aside from the device GUID. DCC recognise that the current solution does not currently allow for the Migration of these devices. The nature of the problem relates to future definition of the EPCL entries to permit the Migration of these types of devices.

2. **Multiple Devices of the Same Type**. The Secure Migration solution makes provision for one (Secure manufactured) PPMID and IHD and CAD to be migrated. Where there are Installations that have more than one device of the same type i.e. SMETS1 PPMID or SMETS1 IHD or SMETS1 CAD.

   - For active and mixed Installations, DCC proposes that Responsible Suppliers should arrange with Secure which of the devices will be migrated.

   - For fully dormant Installations, DCC will instruct Secure that the device most recently joined to the HAN shall be migrated.

   Where there is an additional PPMID, IHD or CAD in the Installation, it can be added post enrolment by the Supplier using the relevant SRV commands.

3. **HAN repeaters**. HAN repeaters are used where a HAN-connected device cannot communicate reliably with the communications hub (CHF) it has been joined with. They are not a recognised DUIS device type so cannot be added to the Smart Metering Inventory. Industry consultation via multilaterals has advised that the use of repeaters is very low in occurrence and that where a repeater becomes faulty, the default business process would be to send a replacement repeater.

| | |
|---|---|
| **TMAD Q7** | *Do you have any comments on the exclusions from the Migration process?* |

# 3. Overview of TMAD Generic Changes which Apply to all Cohorts

## 3.1 Stopping the Commencement of Migration

TMAD proposes changes to clause 4.23 which is intended for Suppliers to be able to stop the Migration of an Installation from commencing, even though the Supplier might have previously provided an MA file to the DCC. The DCC will take reasonable steps to not commence which will entail communicating that request to the Requesting Party.

This clause applies to all cohorts, and it has been amended according to the solution design of all Operating Capabilities.

At the request of the Supplier to stop the commencement of Migration of any Installation or Installations, systems here requested by a Supplier Party, the DCC shall take all reasonable steps to avoid the commencement of the Migration of any remaining SMETS1 Installations, even though the necessary Migration Authorisations may have been previously provided.

### 3.2 Migration Schema Changes

Table 2 identifies certain changes to the Schema. It should be noted that these changes do not impact Suppliers directly because they are an implementation detail of the Secure Meters solution, but these are included so that Suppliers are aware that changes are being made.

DCC is proposing changes to the MasterKeyInformation tag as this is a higher-level tag and can be used to contain either SUAKeyDetails or an EncryptedMasterKey. These changes are intended to make it clear that a clause applied to both (change to MasterKeyInformation) or that it only applied to one.

### 3.3 EPCL Entries

Clause 3.7 has been amended to show that the Secretary of State will be required to approve new entries to the EPCL which have been added by the DMCT process and not by the PPCT process.

## 4. Details of TMAD Changes

This section provides the details of the TMAD changes for MOC (Secure) that are introduced in the section above.

There are only a small number of MOC (Secure) specific changes in the main body of the TMAD. The majority of changes are the new Clause 16 and Appendix C which detail the technical complexities involved in preparing and migrating this cohort.

The entirety of the proposed changes to the TMAD, are set out in Table Table 2 below.

**Table 4 – Details of TMAD Changes**

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 1. | Section 2 Defined Terms and Interpretations | New definition:<br><br>DCO Public Key – Shall mean a public key produced pursuant to Clause 5.4A. | A definition that is required for the Checks and Process that are defined in Tables C5 and C6. |
| 2. | Section 2 Defined Terms and Interpretations | New definition:<br><br>Last EPCL Entry – Means, in respect of entries that include Secure SMSO Limited, the entry on the list of SMETS1 Eligible Product Combinations which has been approved by the Secretary of State after which no other entries in respect of Secure SMSO Limited have been approved by the Secretary of State for a period of 12 months. | This definition is the point at which there can no longer exist connections between the S1SP system and the Secure SMSO. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 3. | Section 2 Defined Terms and Interpretations | Change to the following definition:<br><br>Migration Group File - Shall mean a file created by a Requesting Party pursuant to Clause 5.12(f) which details a list of SMETS1 Installations which the Requesting Party wishes to Migrate, as identified by the CHF Identifier of each, along with, where required for the Group identified by Group ID, any additional Group Specific Requirements for the relevant Group ID. For clarity, such files shall only be processed where they are specified as being required in Group Specific Requirements. | This change to the definition has been made for clarification reasons because, MOC (Secure) does not require a Migration Group File, which is different to other cohorts. |
| 4. | Section 2 Defined Terms and Interpretations | New definition:<br><br>Relevant Device - Relevant Device means a SMETS1 Device with which, prior to the UTRN Period, Secure SMSO communicated on behalf of the Responsible Supplier. | This definition is included for new clause 3.14B. |
| 5. | Section 2 Defined Terms and Interpretations | New definition:<br><br>Single Use Authorisation Code (SUA) - A one-time authorisation code used by Devices with GroupID = “DA” when cryptographically verifying commands. | This definition is included as it is necessary to provide for the SUA key rotation that is unique to the Secure cohort. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 6. | Section 2 Defined Terms and Interpretations | New definition:<br><br>SUA Symmetric Key - A secret, symmetric key used by the DCO to authorise Critical Instructions (with its SMETS1 Supporting Requirements meaning), in relation to Devices with a GroupID = “DA”.. | This definition is included as it is necessary to provide for the SUA key rotation that is unique to the Secure cohort. |
| 7. | Section 2 Defined Terms and Interpretations | New definition:<br><br>UTRN Period - In relation to an ESME or a GSME that forms part of a SMETS1 Installation that is within the Group with a GroupID = ”DA”, a period that:<br><br>(a) commences from the time at which the step in 3.14C(a) has been successfully passed in relation to that Device; and<br><br>(b) has a duration that is 48 hours; | This definition is included as it is necessary to define the period of time for the UTRN cutover arrangements. DCC proposes that this will be a period of 48 hours. It commences from the point at which the S1SP successfully processes the SRV 8.1.1 commissioning request. |
| 8. | Clause 3.7 | The DCC shall not add, other than to the extent that it has the approved by the Secretary of State to do so, an entry to the list of SMETS1 Eligible Product Combinations other than ~~to the extent that it has the approval of the Secretary of State to do so~~ those that arise as a consequence of Pending Product Combination Tests. | This clause has been amended to show that the Secretary of State will be required to approve new entries to the EPCL which have been added by the DMCT process and not by the PPCT process. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 9. | Clause 3.14B | New Clause:<br><br>3.14B For GroupID = "DA", the DCC shall, in relation to each Relevant Device during the UTRN Period in relation to that Device, ensure that any request to generate a SMETS1 UTRN for a non-negative prepayment top up in relation to that Device that;<br><br>(a) is received by the SMETS1 SMSO; and<br><br>(b) had it been received prior to the commencement of the UTRN Period, would have been processed by the SMETS1 SMSO,<br><br>is processed by the SMETS1 SMSO and/or the SMETS1 Service Provider (as the case may be) in materially the same manner (including to have the same effect on the Relevant Device) as it would have had, if it had been processed by the SMETS1 SMSO prior to the commencement of the UTRN Period. | This clause sets out obligations for the SMSO which provides continuity of UTRN generation to ensure that, for a period after commissioning in the DCC systems of the Electricity Meter and Gas Meter due to a migration, UTRN requests which are received by the Secure SMSO are forwarded on to the S1SP and UTRNs generated by the S1SP are returned via the current (RNSP) interface.<br><br>Subsequent to this period, a UTRN request to the Secure SMSO for devices in a migrated SMETS1 Installation will receive a response that indicates that the request was not successful. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 10. | Clause 3.14C | New Clause:<br><br>The DCC shall ensure that the SMETS1 SMSO for GroupID = "DA":<br><br>(a) is not capable of generating a SMETS1 UTRN in relation to a SMETS1 Device after the S1SP has successfully processed a Service Request with Service Reference Variant 8.1.1 for that SMETS1 Device as set out in Clause 8.1 and Table 8.7.2.<br><br>(b) does not provide any response to a request to generate a SMETS1 UTRN in relation to such a SMETS1 Device after the step in 3.14C(a), other than a response that is generated by the relevant S1SP in accordance with Clause 3.14D below.. | This clause sets out obligations for the SMSO which means it will no longer generate UTRNs , after commissioning in the DCC systems of the Electricity Meter and Gas Meter due to a migration, which are received via the current (RNSP) interface to Secure.<br><br>Neither will it generate a response to the UTRN request, given that the response will be generated by the S1SP given the circumstances set out in clause 3.14D.<br><br>This clause covers the cases where commissioning is done by the DCC or by the Responsible Supplier. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 11. | Clause 3.14D | New Clause<br><br>For GroupID = “DA”, during the UTRN Period for an ESME or GSME and where the S1SP receives a request to generate a SMETS1 UTRN for such a SMETS Device from the SMETS1 SMSO, the S1SP:<br><br>(a) shall send a UTRN for the relevant Device that is consistent with the request to that Device and/or to that SMETS1 SMSO; or<br><br>(b) otherwise, up to the point in time at which the UTRN Period ends for the relevant Device, shall only send a response to the SMETS1 SMSO that indicates that the request to generate a UTRN has been unsuccessful. | This clause sets out obligations for the S1SP which provides continuity of UTRN generation to ensure that, for a period after commissioning in the DCC systems of the Electricity Meter and Gas Meter due to a migration, UTRN requests which are received by the Secure S1SP from the SMSO will result in UTRNs to be generated and returned via the current (RNSP) interface.<br><br>Subsequent to this period, a UTRN request for devices in a migrated SMETS1 Installation will generate a response that indicates that the request was not successful. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 12. | Clause 3.14E | New Clause:<br><br>The DCC shall ensure that, by no later than 15 months after the Last EPCL Entry for the S1SP related to the GroupID = "DA", all interfaces to the Systems of that S1SP that are not required by the DCC for the provision of Services under the SEC (excluding any amendments to those Services made by virtue of this TMAD) are securely and irrevocably disconnected from the S1SP Systems. | The purpose of this Clause is to require DCC to irrevocably disconnect all interfaces to the S1SP (for example interfaces to the secure SMETS1 SMSO) that are not required for the provision of enduring services under Section G2 of the SEC. DCC proposes that this happens no later than 15 months after the Last EPCL Entry for the Secure cohort. Thereby, this provides a 3 month contingency over and above the standard 12 month migration period for an EPCL entry. By this time, if any interfaces are required only for the provision of TMAD related services (rather than also being needed for enduring purposes) those interfaces are nevertheless required to be irrevocably disconnected. |
| 13. | 3.14F | New Clause:<br><br>The DCC shall as soon as reasonably practicable following the carrying out of the steps referred to in Clause 3.14E obtain an independent audit and provide to the SMKI PMA and the Security Sub-Committee the report of that audit confirming that the steps have been properly and successfully carried out together with any remediation plan that may be required. | The purpose of this clause is to verify independently that the separation of systems steps in clause 3.14E have been successfully carried out. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 14. | Clause 4.23 | ~~The DCC shall, where requested to do so by a Responsible Supplier for one or more SMETS1 Installations comprising an Active Meter for which that Supplier is the Responsible Supplier~~, Where requested by a Supplier Party, the DCC shall take all reasonable steps ~~not~~ to avoid ~~start~~ the commencement of the Migration of ~~those SMETS1 Installations notwithstanding~~ any SMETS1 Installation for which that Supplier Party is a Responsible Supplier for one (or both) Active Meters. The effect of this shall be that ~~the~~ DCC ~~has previously received~~ shall do so by not commencing the Migration of any remaining SMETS1 Installations contained in any Migration Authorisations received from that Supplier Party. ~~a Migration Authorisation in respect of them from the Responsible Supplier.~~ | This clause has been revised to reflect the capability of all cohorts including MOC (Secure) to be able to not start the migration of an Installation commencing even though the Supplier has already provided authorisation.<br><br>The RP migration systems cannot stop a specific installation in a specific MA file, but instead will stop the commencement of all installations for the Supplier for the remainder of the migration week. |
| 15. | 4.34A | New Clause:<br><br>4.34A Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation that solely comprises Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, being the one that most recently joined the HAN. | |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 16. | Clause 5.1(a), 5.3, 5.12(g), 5.15(a), 11.1 and 11.5 | The term EncryptedMasterKey has been replaced by MasterKeyInformation | This proposed change is required to ensure the secure transfer of master key information from the SMSO to DCC. |
| 17. | Clause 5.4A | New Clause:<br><br>Before the DCC adds the first entry to the SMETS1 Eligible Product Combinations with a GroupID = "DA", the DCO shall generate at least one Private Key and corresponding Public Key(s) for that GroupID to be used solely in relation to 'Securing a SMETS1 GSME' and 'Securing a SMETS1 ESME' for that GroupID in Appendix C. Such Private Key(s) shall be generated by, and known only to, the relevant DCO. | This process is required for secure transfer of EncryptedSUAKey from SMSO to DCO pursuant to TMAD Table 11.3-b. |
| 18. | Table 5.9.1 | Confirm the xml file is well formed and valid against the SMETS1 Migration Schema and meets the requirements of Clause 10.1 and meets the requirements of the "Additional File Structure Validation" for this Group ID. | This is required to ensure that the Migration Common File for MOC (Secure) is validated for SUAKeyDetails. SUAKeyDetails are not required for other Group IDs. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 19. | Clause 5.12(f) | if required by the 'Migration Group File' section of this TMAD for the specified Group ID, populate a Migration Group File with details for the Requested Installations required for the specified Group ID, Digitally Sign and then submit it to the DCC, with the Migration Header having the same values as the Migration Common File; and | This proposed change is necessary because the MOC (Secure) solution doesn't require an MGF file. |
| 20. | Clause 5.23 | For a Migration Group Encrypted File where EncryptedS1SPGroupInformation is required for this Group ID, the S1SP shall then: | This proposed change is necessary because the MOC (Secure) solution doesn't require EncryptedS1SPGroupInformation element name |
| 21. | Table 5.25.1.1 | For each CHFIdentifier in the Migration Group File, where one is required for this Group ID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this Group ID, confirm that the Migration Common File contains a CHFIdentifier with the same value | This proposed change is necessary because the MOC (Secure) solution doesn't require an MGF file. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 22. | Table 5.25.1.2 | For each CHFIdentifier in the Migration Group File, where one is required for this Group ID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this Group ID, confirm that the Migration Common File contains a CHFIdentifier with the same value | This proposed change is necessary because the MOC (Secure) solution doesn't require an MGF file. |
| 23. | Clause 5.27 (iii) | undertake no further processing in relation to that SMETS1 Installation as part of the processing of that 'S1SP Required File Set' and discard information it has stored or derived about that SMETS1 Installation; and | Clarification that there is no MGF file, only the MEF file that is provided to the S1SP and DCO. |
| 24. | Clause 6.7 | New Clause:<br><br>The S1SP for GroupID = "DA" shall not process any request, received via its interface with the SMETS1 SMSO for that GroupID, to communicate with or generate instructions for a Device in relation to which the steps in Clause 5.12(e) have been carried out, except pursuant to Clause 3.14D. | This proposed change provides the ability for the S1SP to allow UTRN generation for prepayment top ups to be processed when received from the Secure SMETS1 SMSO for a period after the device has been commissioned. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 25. | Table 10.1 | New XML element in the schema:<br><br>EncryptedSUAKey<br><br>As required by clause 11.3B and Appendix C of this TMAD | This proposed change is required to allow for the transfer of the SUA Key from SMSO to S1SP.<br><br>Changes were made to references in this table to specify references. |
| 26. | Clause 11.1 | A Requesting Party shall only have access to any populated EncryptedS1SPGroupInformation and MasterKeyInformation, where required for the specified Group ID, provided by the relevant SMETS1 SMSO, and shall not have access to either the Plaintext or symmetric keys which were used as input to the population of such elements | This proposed change is required to ensure secure transfer of master key information from SMSO to the DCC. |
| 27. | Table 11.3B | New Clause:<br><br>For Group ID = “DA”, the DCC shall ensure that each SMETS1 SMSO shall populate any required EncryptedSUAKey element according to Table 11.3-b<br><br>New Table 11.3-b | This proposed change is required to transfer SUA Keys securely from SMSO to DCC with appropriate cryptographic protection. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 28. | Clause 11.5 | The DCC shall ensure that each SMETS1 SMSO shall, in populating any required EncryptedS1SPGroupInformation and MasterKeyInformation elements to provide them to the Requesting Party, not decrease the security of the Secret Key Material used as input to the formation of the corresponding Plaintext. | This proposed change is required to ensure the secure transfer of master key information from the SMSO to DCC. |
| 29. | Clause 12.14, 13.15, 14.15 | New Clause:<br><br>Migration Group File<br><br>A Migration Group File is required for this Group ID. | This proposed change is required because MOC (Secure) does not use an MGF but other cohorts do.<br><br>Clauses 12.14, 13.16 and 14.15 now specifically show that an MGF file is required. |
| 30. | Clause12.15, 13.16 14.16 | New Clause:<br><br>Additional File Structure Validation<br><br>A Migration Group Encrypted File is required for this Group ID, and each such file must include EncryptedS1SPGroupInformation and EncryptedMasterKey, and must not include any SUAKeyDetails. | This proposed change is required to explain the common XML schema that is used across cohorts and provides that relevant cohorts only validate appropriate data elements in the XML file. For cohorts other than Secure Meter devices, the SUAKeyDetails element in XML must not be used.<br><br>Clauses 12.15, 13.17 and 14.16 now specifically show that the SUAKeyDetails element in XML must not be used. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 31. | Clause12.16, 13.17 14.17 | New Clause<br><br>Migration Common File Device Selection Requirements | This clause details the scenario where a SMETS1 Installation has more than one Secure manufactured device of a particular type, such as a PPMID, IHD or CAD. This is not used for other cohorts. |
| 32. | Section 16 | New section titled:<br><br>Requirements specific to Group ID = “DA”, | New section detailing requirements for MOC Secure device sets. |
| 33. | Clause 16.1 | New Clause:<br><br>This Clause 16 specifies the requirements which are specific to processing in relation to SMETS1 Installations where Group ID = ”DA”. | Introduction to the new section for MOC (Secure). |
| 34. | Clause 16.2 | New Clause:<br><br>**Pre-enrolment Configuration Requirements**<br><br>NOT USED | Not required for MOC (Secure) |
| 35. | Clause 16.3 | New Clause:<br><br>**Migration Group Encrypted File**<br><br>A Migration Group Encrypted File is required for this Group ID. | This requirement is in line with other cohorts. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 36. | Clause 16.4 | New Clause:<br><br>**S1SP Required File Set**<br><br>The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, and one Migration Group Encrypted File, all with the same Migration Header, and so the same Group ID. | This is required because the S1SP Required File Set for MOC (Secure) is different to the other cohorts. |
| 37. | Clause 16.5 | New Clause:<br><br>**DCO Required File Set**<br><br>The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same Group ID. | This is required because the DCO Required File Set for MOC (Secure) is different from the other cohorts. |
| 38. | Clause 16.6 | New Clause:<br><br>**S1SP Migration Group File data validation**<br><br>NONE REQUIRED | Not required for MOC (Secure) |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 39. | Clause 16.7 | New Clause:<br><br>**DCO Migration Group Encrypted File data validation**<br><br>The checks at Table 16.7 shall be the 'DCO Migration Group Encrypted File data validation' for this Group ID. | The information within the table states that the EncryptedSUAKey element for the relevant device type will be checked for the SMETS1 Installation.<br><br>Change to reflect the MOC Secure meter sets, over the IOC / MOC MDS meter sets. |
| 40. | Clause 16.8 | New Clause:<br><br>**S1SP Migration Group Encrypted File data validation**<br><br>NONE REQUIRED | Not required for MOC Secure |
| 41. | Clause 16.9 | New Clause:<br><br>**S1SP / DCO Commissioning of SMETS1 Installation**<br><br>16.9 The steps at Table 16.9 may be carried out up to [7] days in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.<br><br>The checks detailed within the Table refer to the processes described in Appendix C. | This details the MOC (Secure) S1SP and DCO steps required for Installing an ESME, GSME or PPMID where applicable. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 42. | Clause 16.10 | New Clause:<br><br>The steps at Table 16.10 shall not be carried out in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question. | This details the MOC (Secure) S1SP and DCO steps required for Securing an ESME, GSME or PPMID where applicable. |
| 43. | Clause 16.11 | New Clause:<br><br>**Installation Rollback**<br><br>The processing at Table 16.11 shall be the 'Installation Rollback' for this Group ID.<br><br>If GSME is present, the S1SP shall revert control of the SMETS1 Installation to the relevant SMETS1 SMSO where any of the steps in "Securing a SMETS1 GSME" fails for this Group ID.<br><br>The S1SP shall not revert control of the SMETS1 Installation to the relevant SMETS1 SMSO if any of the steps in "Securing a SMETS1 ESME" fails for this Group ID. | This details the MOC (Secure) rollback. See Section 2.3 SUA Key Rotation and Rollback of a Secure Meter for further details. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 44. | Clause 16.12 and 16.13 | **CHF Whitelist**<br><br>The CHF Whitelist shall, for this Group ID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.<br><br>The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF. | This details the CHF Whitelist requirements for MOC (Secure). |
| 45. | Clause 16.14 | New Clause:<br><br>**Post Migration Configuration**<br><br>NOT USED | Not required for MOC (Secure). |
| 46. | Clause 16.16 | New Clause:<br><br>**Additional File Structure Validation**<br><br>A Migration Group Encrypted File is required for this Group ID, and each such file must not include any EncryptedS1SPGroupInformation or any EncryptedMasterKey, and must include SUAKeyDetails. | This proposed change is required to explain the common XML schema that is used across cohorts and provides that relevant cohorts only validate appropriate data elements in the XML file. For Secure Meter devices, the SUAKeyDetails element in XML must be used. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 47. | Clause 16.17 | New Clause:<br><br>**Migration Common File Device Selection**<br><br>Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation that solely comprises Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, being the one that most recently joined the HAN. | This clause details the scenario where a SMETS1 Installation has more than one Secure manufactured device of a particular type, such as a PPMID, IHD or CAD.<br><br>For fully dormant installations, the device that was last joined to the HAN will be migrated. |
| 48. | Appendix C | New Appendix:<br><br>**Device Installation – For Group ID DA,** | We have included a new Appendix C specifically for the MOC (Secure) Group ID rather than add to the existing Appendix A and B due to the different technical requirements presented by the MOC (Secure) device set. |
| 49. | C1 | New text:<br><br>**Installing a SMETS1 Electricity Meter**<br><br>The checks and processing at Table C1 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' and shall take place in the order specified in that Table. | The table identifies the checks and processes that are required for installing an ESME that are specific to MOC (Secure). |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 50. | C2 | New text:<br><br>**Installing a SMETS1 GSME**<br><br>The processing at Table C2 shall be that required of the S1SP for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table. | The table identifies the checks and processes that are required for installing a GSME that are specific to MOC (Secure). |
| 51. | C3 | New text:<br><br>**Installing a SMETS1 PPMID**<br><br>No additional checks or processing is required. | Not required for MOC (Secure). |
| 52. | C4 | New text:<br><br>**Commission Device (CHF)**<br><br>The processing at Table C4 shall be that required of the S1SP for 'Commission Device (CHF)'. | This is similar to other cohorts. |

| No. | TMAD Reference | Description of Change (new TMAD text is coloured blue) | Rationale for Change |
|---|---|---|---|
| 53. | C5 | New text:<br><br>**Securing a SMETS1 GSME**<br><br>The checks and processing at Table C5 shall be that required of the S1SP and DCO for 'Securing a SMETS1 GSME' for the relevant Group ID and shall take place in the order specified in that Table. | The table identifies the checks and processes that are required for securing a GSME that are specific to MOC (Secure). |
| 54. | C6 | New text:<br><br>**Securing a SMETS1 ESME**<br><br>The checks and processing at Table C6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for the relevant Group ID and shall take place in the order specified in that Table.<br><br>The S1SP checks and processing detailed in Table C6 are specific to MOC Secure and differ from the equivalent Table A6. | The table identifies the checks and processes that are required for securing an ESME that are specific to MOC (Secure). |

| | |
|---|---|
| **TMAD Q8** | *Do you have any detailed comments on the changes to the legal drafting in TMAD? Please provide a rationale for your views.* |

# 5. Next Steps

Following the closure of this consultation, DCC will take into account respondents' views, and, subject to the consultation responses received, submit to the Department of Business, Energy and Industrial Strategy (BEIS) an amended version of the TMAD that it considers suitable for re-designation into the SEC by the Secretary of State.

DCC will conclude on this consultation, providing a report to BEIS no later than 05 June 2020. DCC has discussed the re-designation of the TMAD with BEIS and it is proposed that, subject to timely receipt of DCC's report, copies of relevant stakeholder responses to this consultation, BEIS will re-designate the TMAD on 26 June 2020or as soon as reasonably practicable within one month thereafter.

In order to expedite the re-designation of the TMAD, DCC is also seeking views on behalf of BEIS on the proposed date for re-designation of the TMAD being 26 June 2020 (or, if necessary, as soon as reasonably practicable within one month thereafter) as well as the draft direction which is presented in Annex A of this consultation document for stakeholder consideration.

| | |
|---|---|
| **TMAD Q9** | *Do you agree with the proposed re-designation date of 26 June 2020 (or, if necessary, as soon as reasonably practicable within one month thereafter) for the TMAD using the draft direction at Annex A*Annex A*?* |

# 6. How to respond

Please provide responses in the attached template by 16:00 on 03 April 2020 to DCC at consultations@smartdcc.co.uk.

Consultation responses may be published on our website www.smartdcc.co.uk. Please state clearly in writing whether you want all or any part, of your consultation to be treated as confidential. It would be helpful if you could explain to us why you regard the information you have provided as confidential. Please note that responses in their entirety (including any text marked confidential) may be made available to the Department of Business, Energy and Industrial Strategy (BEIS) and the Gas and Electricity Markets Authority (the Authority). Information provided to BEIS or the Authority, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004). If BEIS or the Authority receive a request for disclosure of the information we/they will take full account of your explanation (to the extent provided to them), but we/they cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

If you have any questions about the consultation documents, please contact DCC via consultations@smartdcc.co.uk.

# 7. Attachments

- Attachment 1 – Annex A Draft Redesignation (below)
- Attachment 1 – SMETS1 Transition and Migration Approach Document V3.1 (clean)
- Attachment 2 – SMETS1 Transition and Migration Approach Document V3.1 (change marked against V3.0)
- Attachment 3 - SMETS1 Migration Schema v1.2 MOC_Secure
- Attachment 4 – Response Template

# Annex A

This annex contains the draft direction and re-designation text that BEIS intend to utilise for re-designation of the TMAD.

**Draft Re-designation Text**

*This direction is made for the purposes of the smart meter communication licences granted under the Electricity Act 1989 and the Gas Act 1986 (such licences being the "DCC Licence") and the Smart Energy Code designated by the Secretary of State pursuant to the DCC Licence (such code being the "SEC").*

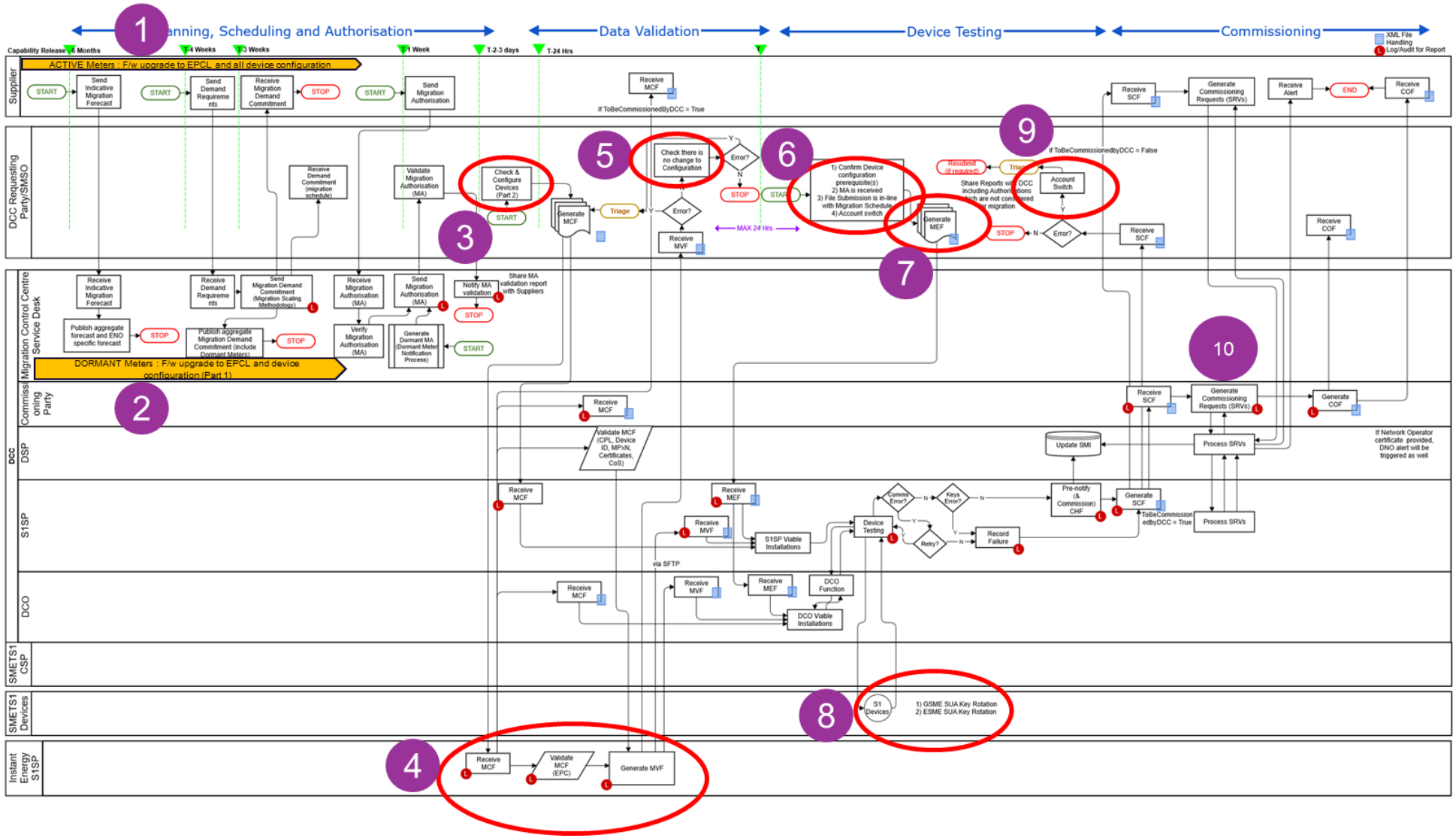
*Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.*

*Pursuant to Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code) of the SEC, the Secretary of State directs that, with effect from [26 June 2020], the SMETS1 Transition and Migration Approach Document previously designated and incorporated into the SEC as Appendix AL is hereby re-designated and incorporated in the form set out in Annex [XX] to this direction.*

*For the avoidance of doubt such re-designation of the SMETS1 Transition and Migration Approach Document shall be without prejudice to anything done under the DCC Licence or the SEC on or after this document first being designated, or to the continuing effectiveness of anything done under this document prior to its re-designation (which shall have effect as if done under the re-designated document).*

*This direction is also being notified to the SEC Administrator.*

# 8. Appendix A – TMAD Process Flow



# 9. Appendix B – Timeline for Applying Configuration

This Appendix provides guidance to Suppliers by showing the timeline for applying pre-enrolment configuration to Secure devices.

Four scenarios are considered:

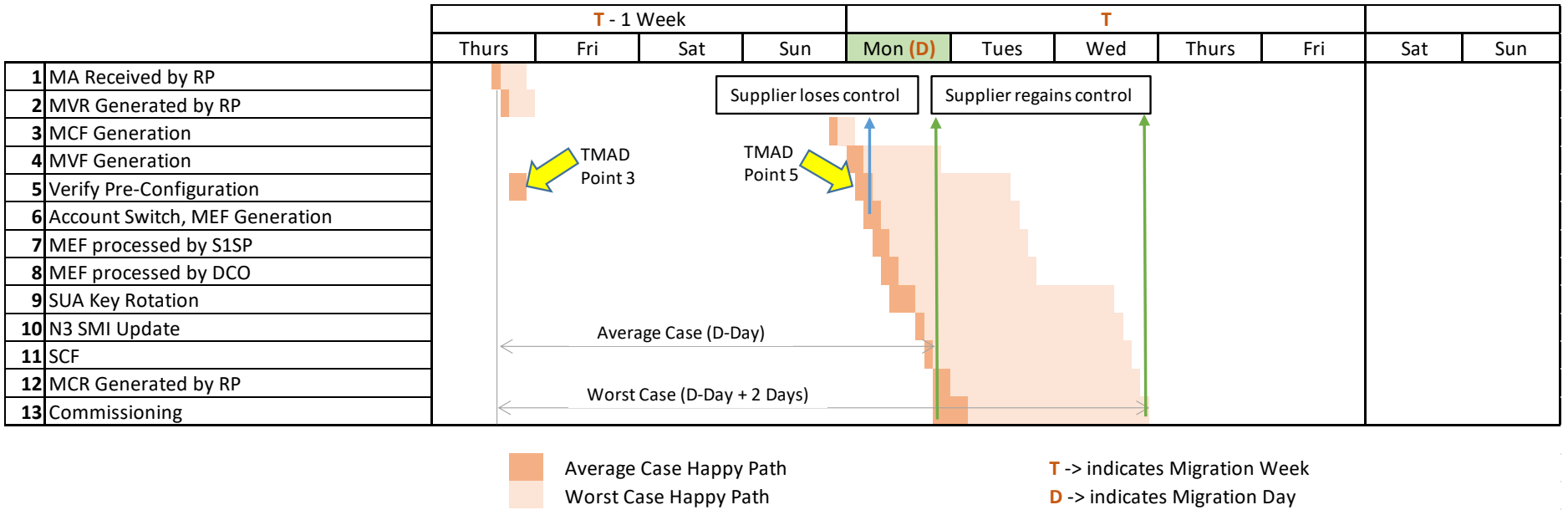
- Active meter – where migration is planned for Monday of the migration week
- Active meter – where migration is planned for Friday of the migration week
- Dormant meter – where migration is planned for Monday of the migration week
- Dormant meter – where migration is planned for Friday of the migration week

For Active meters, Secure recommend that all configuration is applied in advance of providing the MA file to the DCC. This is represented by point 1 in the TMAD Process Flow given in App A. However DCC recommend that Suppliers discuss with Secure SMSO.

For Dormant meters, the configuration is applied in two parts. Part 1 configuration is checked and applied by the Secure SMSO Helpdesk at point 2 in the TMAD Process Flow in App A. Part 2 is checked and applied at point 3 where required.

The parameters verification points are also shown in the TMAD Process Flow (3 and 5 for active meters, and 5 for dormant meters), as well as the more detailed migration timeline shown below.

## 9.1 Active Meter − Migration Day Monday



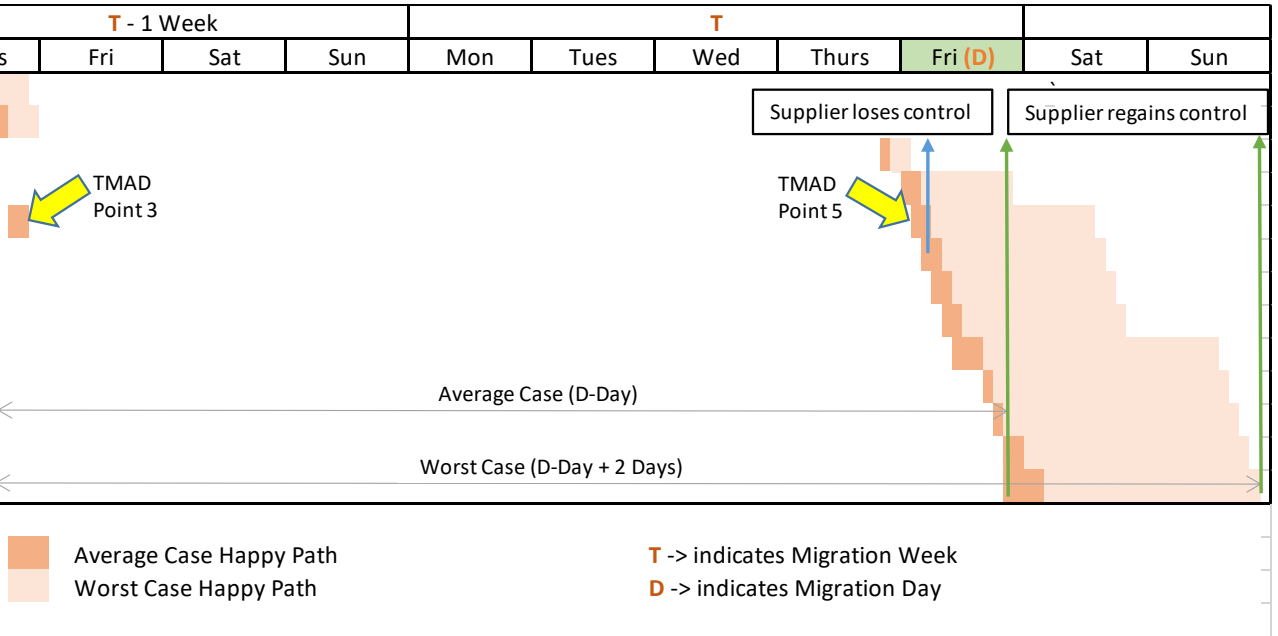

Average Case Happy Path
Worst Case Happy Path

**T** -> indicates Migration Week
**D** -> indicates Migration Day

Best Case -> Installation which is planned to be migrated on Monday, enrols on Monday (morning hours)
Average Case -> Installation which is planned to be migrated on Monday, enrols on Monday (evening hours)
Worst Case -> Installation which is planned to be migrated on Monday, enrols on Wednesday (late evening hours)

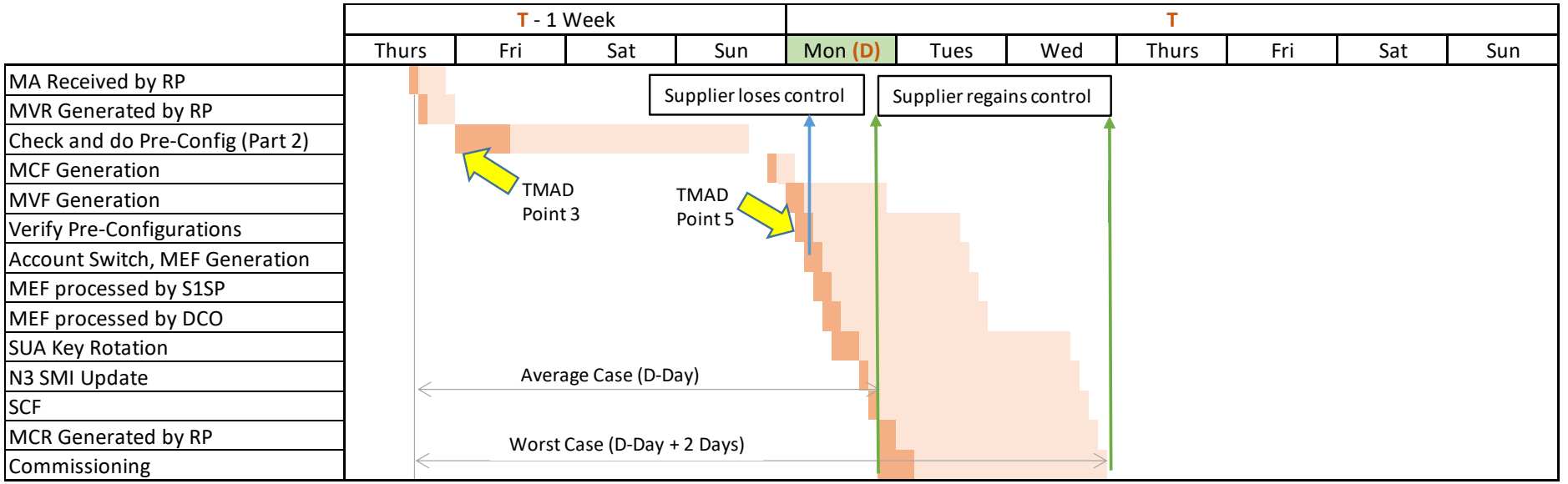
## 9.2 Active Meter – Migration Day Friday

| | |
|---|---|
| 1 | MA Received by RP |
| 2 | MVR Generated by RP |
| 3 | MCF Generation |
| 4 | MVF Generation |
| 5 | Verify Pre-Configuration |
| 6 | Account Switch, MEF Generation |
| 7 | MEF processed by S1SP |
| 8 | MEF processed by DCO |
| 9 | SUA Key Rotation |
| 10 | N3 SMI Update |
| 11 | SCF |
| 12 | MCR Generated by RP |
| 13 | Commissioning |




Best Case -> Installation which is planned to be migrated on Friday, enrols on Friday (morning hours)
Average Case -> Installation which is planned to be migrated on Friday, enrols on Friday (evening hours)
Worst Case -> Installation which is planned to be migrated on Friday, enrols on Sunday (late evening hours)

## 9.3 Dormant Meter – Migration Day Monday

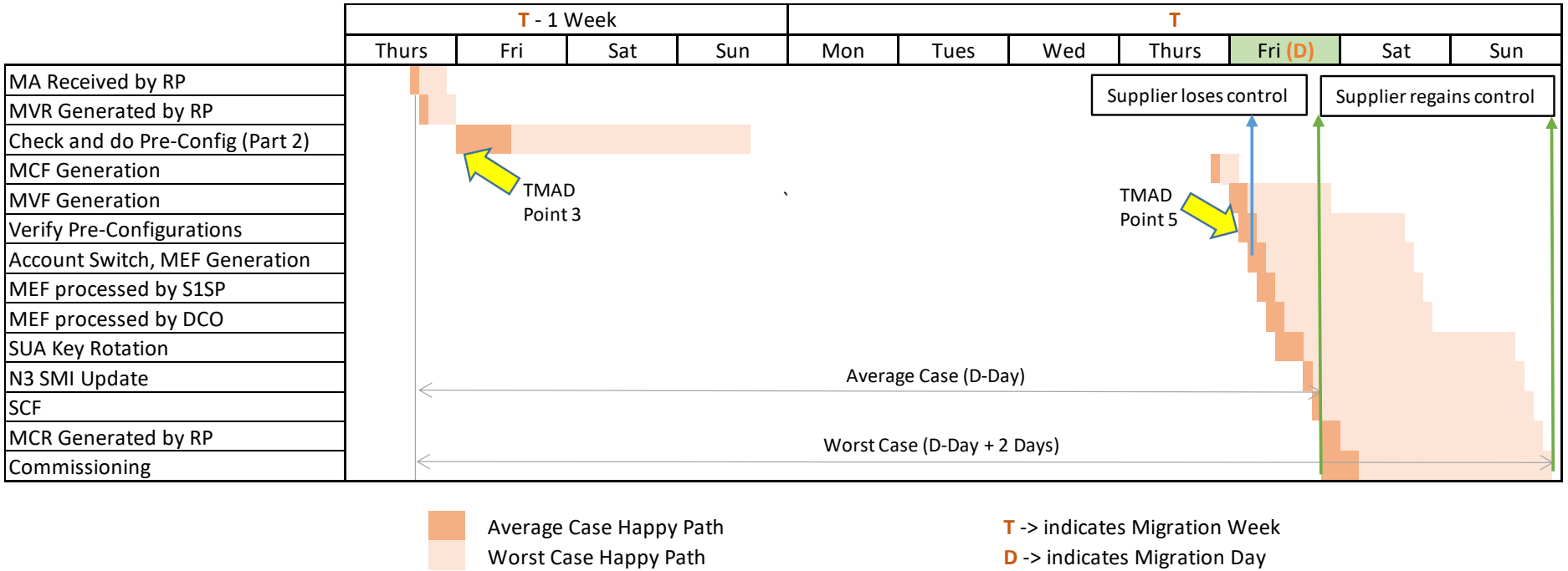



Average Case Happy Path
Worst Case Happy Path

**T** -> indicates Migration Week
**D** -> indicates Migration Day

Best Case -> Installation which is planned to be migrated on Monday, enrols on Monday (morning hours)
Average Case -> Installation which is planned to be migrated on Monday, enrols on Monday (evening hours)
Worst Case -> Installation which is planned to be migrated on Monday, enrols on Wednesday (late evening hours)

## 9.4 Dormant Meter – Migration Day Friday




Best Case -> Installation which is planned to be migrated on Friday, enrols on Friday (morning hours)
Average Case -> Installation which is planned to be migrated on Friday, enrols on Friday (evening hours)
Worst Case -> Installation which is planned to be migrated on Friday, enrols on Sunday (late evening hours)