

# TARGET2-SECURITIES

MANUAL OF

OPERATIONAL

PROCEDURES

(OPERATIONAL PROCEDURES AND RULES REGARDING  
DCP RELEVANT ASPECTS)

---

Date: 26/01/2017

---

## **Information from the T2S MOP to be shared with the Directly Connected Parties of OeKB CSD.**

The T2S Manual of Operational Procedures (T2S MOP) is the reference guide for the operational procedures that should be followed in order to ensure the smooth functioning of the T2S Services. The MOP describes the operational processes and procedures, organisational structure of T2S operations with roles and responsibilities of T2S Actors along with communication tools/ mechanism as well as their availability.

A T2S Information Guide was originally considered by the OMG as a deliverable to share MOP relevant aspects. The OMG supported the need for harmonised operational procedures and rules regarding DCP relevant aspects.

In the following chapters, we directly share the relevant operational processes and procedures with all Directly Connected Parties (DCPs) of OeKB CSD, covering relevant matters in their daily use of T2S.

TABLE OF CONTENTS

**INTRODUCTION**

<b>OVERVIEW OF ROLES AND RESPONSIBILITIES .....</b>	<b>3</b>
1.1.1 T2S Service Desk and T2S Service Manager .....	3
1.1.2 CSD/Central Bank Settlement Managers .....	4
1.1.3 Crisis Managers of CSDs, Central Banks, 4CB and ECB Crisis Manager .....	5
1.1.4 Directly Connected Parties .....	5
1.2 External communication tools.....	7
1.2.1 T2S-info.....	7
1.2.2 Broadcasts through the T2S GUI.....	7
1.2.3 Communication of CSDs and Central Bank with their participants .....	7
1.2.4 Overview of communication tools.....	7
1.3 T2S operational tools .....	9
1.3.1 T2S Operational Directory.....	9
1.3.2 T2S Trouble Management System.....	9
1.4 T2S Calendar .....	10
1.5 Availability of support .....	11
1.6 T2S settlement day .....	13
1.6.1 Introduction to the T2S settlement day.....	13
1.6.2 T2S change of the settlement day.....	16
1.6.3 T2S queuing during weekends and T2S closing days.....	16
1.6.4 Schedule of T2S Settlement Day.....	16
1.6.5 Delay start of D + 1 settlement day in case of RTGS delay.....	25
1.6.6 Processing of the CMS data feed .....	26
1.6.7 Night-time algorithms processing during RTS.....	27
1.6.8 T2S delay.....	28
1.6.9 T2S processing with limited liquidity .....	32
1.6.10 Opening T2S on weekends for settlement.....	33
1.6.11 Updating rule-based models .....	35
1.6.12 Handling unwanted consequences of rules-based model updates .....	36
1.6.13 Technical disconnection of a participant using abnormally the system.....	37
1.6.14 NCB-CSD Communication on DCA accounts.....	38
<b>2 INCIDENT MANAGEMENT .....</b>	<b>40</b>
2.1 General incident management process flow.....	40
2.2 Scenario 1: Incident at the level of the T2S Platform (at 4CB as T2S Operator)	
47	
2.3 Scenario 2: Incident at the level of TARGET2/ RTGS.....	52
2.4 Scenario 4: Incident at the level of DCPs or ICPs .....	56
<b>3 ACCESS MANAGEMENT .....</b>	<b>62</b>
3.1 Prerequisites and common Principles applied to all requests .....	62

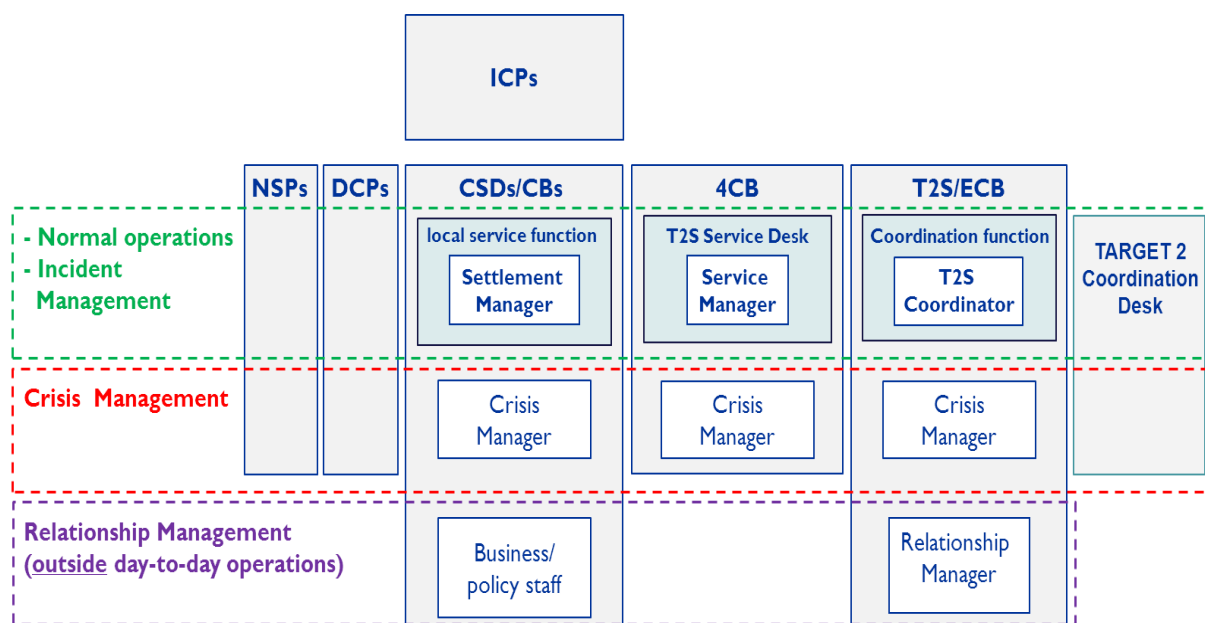
3.2	Requesting access rights.....	63
3.2.1	<i>General pattern of DiCoA requests (common to DCP/ CSD/ NCB).....</i>	63
3.2.2	<i>DCP Requests.....</i>	63
3.3	Requesting Changes to Existing Access Rights .....	66
3.4	Requesting Removal of Existing Access Rights .....	66
3.5	Supporting the Process .....	66
<b>4</b>	<b>SERVICE CONTINUITY MANAGEMENT .....</b>	<b>68</b>
4.1	Purpose and Scope of Service Continuity Management .....	68
4.2	BCM and SCM Principles as Referred to in the FA/ CPA and Related Documents.....	69
4.3	T2S Service Continuity .....	69
4.3.1	<i>Major Failure.....</i>	70
4.3.2	<i>Regional Disaster.....</i>	71
4.3.3	<i>Rebuilding Process.....</i>	73
4.4	Service Continuity Testing.....	75
4.4.1	<i>Objective of Testing.....</i>	75
4.4.2	<i>Roles and Responsibilities.....</i>	75
4.4.3	<i>Frequency and Planning .....</i>	76
4.4.4	<i>Test Results and Reporting.....</i>	76
4.4.5	<i>CSDs’/ Central Banks’/ DCPs’ Service Continuity Test.....</i>	76
4.4.6	<i>T2S Service Continuity Test .....</i>	77

1 **INTRODUCTION**

2 **OVERVIEW OF ROLES AND RESPONSIBILITIES**

3 The MOP is intended as reference guide for CSDs, the Eurosystem Central Banks, non-euro National  
4 Central Banks (NCBs) that will bring their currency to T2S and the non-euro Central Banks connected  
5 to TARGET2. Furthermore, it describes the roles and responsibilities of the 4CB in their capacity as  
6 T2S Operator and the ECB as being in charge of the T2S Coordination function.

7 This Chapter describes the roles of the aforementioned T2S Actors (excluding ICPs). For the sake of  
8 transparency, the diagram shows other players involved in the interaction (mainly when it comes to  
9 Incident and Crisis Management), i.e. Network Service Providers (NSPs); Indirectly Connected  
10 Parties (ICPs); the ECB’s T2S Relationship management function; and the TARGET2 Coordination  
11 Desk of the ECB.



13 *Figure 1 - T2S Actors and other relevant players*

14 **1.1.1 T2S Service Desk and T2S Service Manager**

15 The T2S Service Desk<sup>1</sup> provides a single point of contact for the CSDs, the non-euro National Central  
16 Banks making their currency available to T2S, the Eurosystem Central Banks, the DCPs<sup>2</sup> and the  
17 NSPs for handling all incidents, queries and requests concerning T2S operational, functional or

<sup>1</sup> This is part of T2S Operator entity as defined in Schedule 1 of Framework Agreement.

<sup>2</sup> DCPs may only contact the T2S Service Desk for incidents related to technical connectivity or concerning their connection to T2S.

18 technical issues. Moreover, the T2S Service Desk is equipped with early warning, communication and  
19 monitoring tools in order to identify a potential incident at an early stage.

20 With the exception of connectivity issues, the TARGET2 Organisational Framework applies for all  
21 cash-related issues.

22 The T2S Service Managers head the T2S Service Desk. The T2S Service Manager liaises with the  
23 T2S Coordination function and the CSD/Central Bank Settlement Managers, in order to provide  
24 advice on the T2S operations.

25 The roles of the T2S Service Desk in normal operations are summarised below:

- 26 ▶ Providing information on T2S functionality as described in the UDFS;
- 27 ▶ Providing information concerning the running of the system;
- 28 ▶ Dealing with Service Requests in line with the SLA (see FA/CPA Schedule 6); capturing and  
29 maintaining system parameters. ;
- 30 ▶ Keeping the BIC Directory up-to-date;
- 31 ▶ Dealing with the authorisation of the subscription to the T2S Closed Group of Users (CGUs) of  
32 the licenced NSPs;

33 The roles of the T2S Service Desk in abnormal situations are summarised below:

- 34 ▶ Supporting the ECB T2S Coordination function (the Settlement Manager/Crisis Managers'  
35 conference calls) by providing operational and technical information on the platform;
- 36 ▶ Supporting the aforementioned T2S Actors (excluding ICPs) in the case of T2S incident and/or  
37 crisis, but also in the event of a local/ national incident/ problem;
- 38 ▶ Providing support in the event of a network failure.

### 39 **1.1.2 CSD/Central Bank Settlement Managers**

40 Each CSD and Central Bank requires a Settlement Manager. The Settlement Manager usually leads  
41 the business support functions of the each CSD and Central Bank.

42 On the Central Bank side, the TARGET2 Settlement Managers and the TARGET2 Coordination  
43 function represent the TARGET2/RTGS system owner side, the Collateral Management function and  
44 the “bank of banks” role. TARGET2 cash related incidents are covered under the TARGET2  
45 organisational structure.

46 As each CSD and Central Bank remains fully responsible for the business relations with its respective  
47 participants, T2S has been designed in a way that allows the CSDs/ Central Banks to meet the

48 administrative and regulatory requirements in terms of service monitoring and service control. The  
49 CSD and Central Bank Settlement Managers are responsible for:

50 ▶ all contacts with, and provision of business support to, their participants, including the  
51 management of the relevant Static Data (including NCB role to provide Static Data for auto-  
52 collateralisation);

53 ▶ daily operational management;

54 ▶ monitoring of the settlement activities of their participants (e.g. settlement flows) and the  
55 technical and operational monitoring of any local technical components;

56 ▶ handling of local contingency arrangements and abnormal situations which are covered by this  
57 document and do not explicitly require the involvement of the Crisis Managers;

58 ▶ close interaction with the T2S Coordination function and the T2S Service Desk.

### 59 **1.1.3 Crisis Managers of CSDs, Central Banks, 4CB and ECB Crisis Manager**

60 Each CSD and Central Bank appoints a Crisis Manager. The ECB and 4CB also appoints a Crisis  
61 Manager. Decisions are taken in Crisis Managers' conference call, chaired by the ECB Crisis  
62 Manager. The Crisis Managers are called to deal with events which explicitly require their  
63 involvement, or are escalated to them by the Settlement Managers or that are not covered within the  
64 MOP.

### 65 **1.1.4 Directly Connected Parties**

66 A DCP is a T2S User<sup>3</sup>, which is authorised by its CSD or Central Bank to access T2S directly for  
67 using T2S Services, i.e. without the need for the CSD or the Central Bank to act as a technical  
68 interface. For the purpose of the MOP, a DCP:

69 ▶ subscribes the T2S Closed User Group (CGU) of one of the NSPs;

70 ▶ communicates with T2S Platform via the Application-to-Application (A2A) and/or User-to-  
71 Application (A2A).

72 A DCP can participate in the T2S day-to-day operations as follows (in compliance with the provisions  
73 stipulated in the FA):

---

<sup>3</sup> T2S User defines a legal entity that has contractual/legal relationship with a CSD, which has entered in to a contractual relationship for the use of T2S. It also defines a payment bank (DCA Holder), providing liquidity through an RTGS account in RTGS system to a financial institution, settling in T2S, see FA/ CPA Schedule 1.

- 74 ▶ All DCPs can contact the T2S Service Desk related to technical enquiries concerning their  
75 connection to T2S.
- 76 ▶ A DCP can inform the T2S Service Desk directly if it faces incidents related to technical  
77 connectivity, which prevents the proper usage of T2S; the T2S Service Desk must then inform the  
78 relevant CSD/ Central Bank without undue delay (for more details see *Chapter 2 - Incident*  
79 *Management*).
- 80 ▶ A DCP should contact its CSD and/or NCB directly for handling all the other T2S topics, with the  
81 exception of incidents related to technical connectivity, connectivity to T2S and technical queries  
82 as mentioned in the points above.
- 83 ▶ In order to ensure smooth communication with DCPs, the CSDs and Central Banks shall provide  
84 the T2S Coordination function with contact details of their DCPs.
- 85 ▶ Since the DCPs are not directly involved in Incident and Crisis Management activities<sup>4</sup>; it is for  
86 the respective CSD and Central Bank to ensure that the DCP is appropriately informed about on-  
87 going incidents and Crisis. They will be invited in Crisis Manager's conference call if related to  
88 the cause of the crisis.
- 89

---

<sup>4</sup> FA Article 12: Eurosystem can interact with DCPs for Crisis Management.



90 **1.2 EXTERNAL COMMUNICATION TOOLS**

91 **1.2.1 T2S-info**

92 The T2S Information System (T2S-info) provides up-to-date information on the operational status of  
93 the T2S Services to news agencies (such as Reuters, Bloomberg) and the T2S website. T2S-info  
94 informs about normal operations (start of day/end of day) and abnormal situations. In abnormal  
95 situations, T2S-info is used to provide information about the type of failure, the impact and the  
96 measures envisaged to solve the problem. T2S-info is updated by the T2S Coordination function. The  
97 dissemination of information requires the prior agreement of the Settlement Managers or Crisis  
98 Managers and synchronisation, if applicable, with the information broadcasted through the T2S  
99 Graphical User Interface (GUI). To ensure the timely communication to users, a set of templates is  
100 available for the initial communication. These templates do not require detailed information on the  
101 crisis.

102 The T2S-info with the pre-agreed templates are available as part of operational documentation.

103 **1.2.2 Broadcasts through the T2S GUI**

104 The T2S GUI allows the T2S Service Desk to send broadcast messages to the CSDs and Central  
105 Banks which in turn can also send broadcast messages to their DCPs (see *UHB V2.0, paragraph*  
106 *2.4.2*).

107 In the event that a CSD or Central Bank faces problems with the submission of messages to its  
108 community, the T2S Service Desk can send such broadcasts on behalf of the CSD or Central Bank. In  
109 case of need and upon agreement of the CSD/ Central Bank Settlement Managers, the T2S Service  
110 Desk can send broadcast messages to all participants, or to a predefined group of them, i.e. to:

- 111 ▶ all CSDs;
- 112 ▶ all CSDs and their DCPs;
- 113 ▶ all Central Banks;
- 114 ▶ all Central Banks and their DCPs.

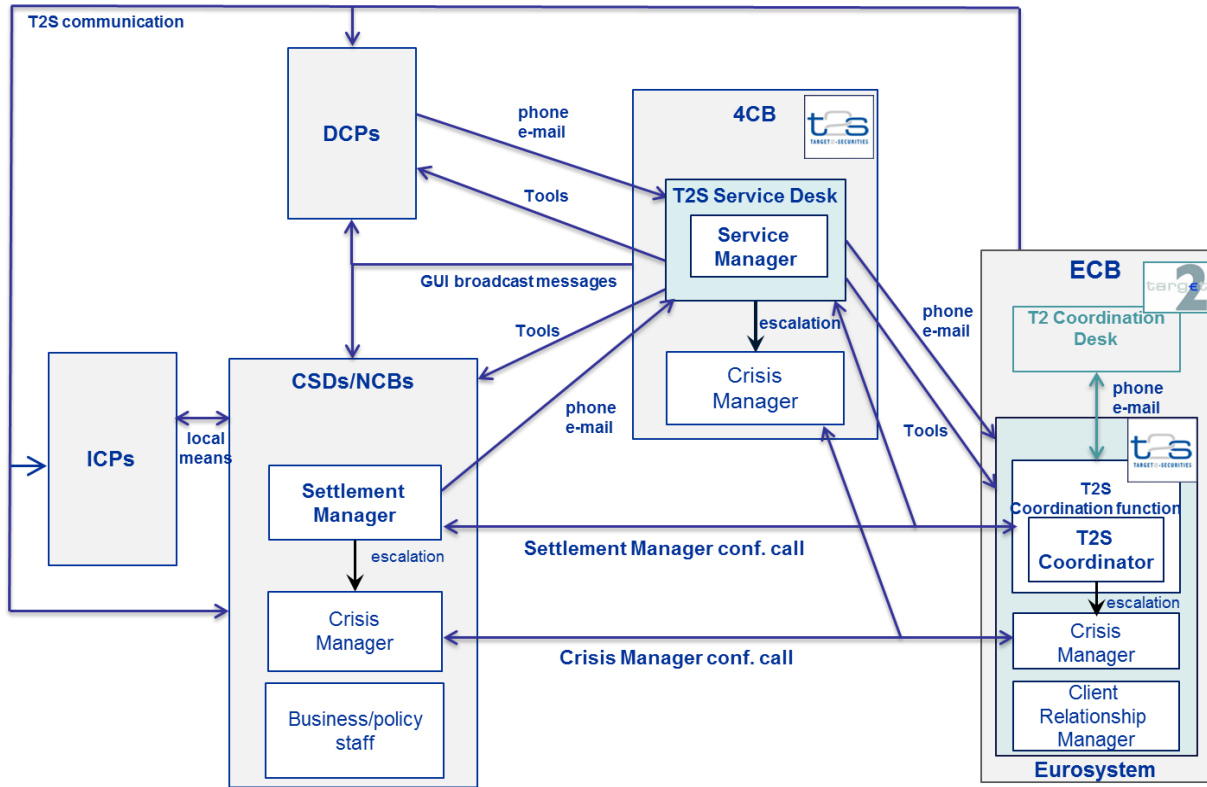
115 **1.2.3 Communication of CSDs and Central Bank with their participants**

116 Local means of communication with the participants of CSD's and CB's are the responsibility of the  
117 CSD and Central Bank Settlement or Crisis Managers.

118 **1.2.4 Overview of communication tools**

119 The interaction of the T2S Actors through the different communication tools can be depicted as  
120 follows:

121 direct



122

123

Figure 2 - Communication Tools Overview

124

125 **1.3 T2S OPERATIONAL TOOLS**

126 **1.3.1 T2S Operational Directory**

127 The T2S Operational Directory is maintained on a secure part of the T2S website. It provides the  
128 current contact information for T2S Actors (excluding ICPs) as well as the T2S Service Desk and the  
129 T2S Coordination function. Changes are communicated by respective T2S Actors (excluding ICPs) to  
130 T2S Coordination function, who keeps it updated. Additionally, the T2S Coordination function  
131 revalidates the contact information every three months. Furthermore, it contains the pre-agreed  
132 templates for the T2S Information System (T2S-info). It serves as a supporting tool for the smooth  
133 communication with the T2S Actors (excluding ICPs). The T2S Coordination function is in charge of  
134 maintaining the T2S Operational Directory and provides all T2S Actors (excluding ICPs) with  
135 passwords for accessing the secure Web pages.

136 **1.3.2 T2S Trouble Management System**

137 The T2S Trouble Management System (TMS) supports most of the activities of the T2S Service Desk  
138 related to the Service Management processes (see *UDFS V2.0, Section 1.1.5.6 Trouble Management*).

139 The T2S Service Desk uses the TMS to track all interactions (such as incidents, service requests) with  
140 CSD and Central Bank Settlement Managers as well as with the NSPs and DCPs.

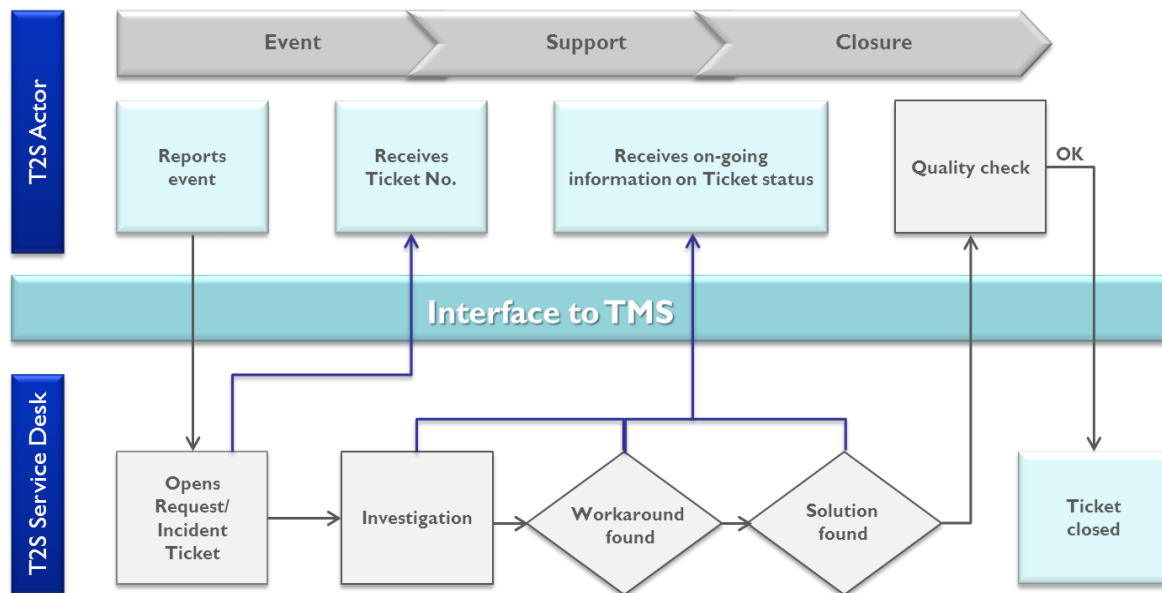


Figure 3 - TMS Overview

143 Every time a CSD or Central Bank Settlement Manager, NSP or DCP contacts the T2S Service Desk  
144 via telephone or e-mail, the T2S Service Desk opens a ticket (also for incidents). It assigns a unique

145 identifier and communicates it to the reporting T2S Actor. The CSD and Central Bank Settlement  
146 Managers as well as DCPs have read access to the TMS through its Graphical User Interface (GUI).

147 Each ticket within the TMS has a life cycle from the opening until the closure through updates and  
148 status changes. Following each status change, the entitled T2S Actor receives a notification. The  
149 closure of a TMS case always needs the agreement by either phone or e-mail of the reporting T2S  
150 Actor.

#### 151 **1.4 T2S CALENDAR**

152 T2S facilitates securities settlement in

153 ▶ euro Central Bank money (CeBM) (i.e. settlements against payment or free of delivery), for which  
154 the calendar is the same as the calendar of TARGET2;

155 ▶ Non-euro CeBM, according to the calendar for the opening days of the respective Central Bank.

156 Under normal circumstances, T2S is open from Monday to Friday every week. T2S is closed on:

157 ▶ 1 January

158 ▶ 25 and 26 December

159 T2S is open for settlement against payment aligning to the opening days of the respective Central  
160 Bank. With regards to the EUR, the TARGET2 Calendar

161 (<http://www.ecb.europa.eu/paym/t2/professional/indicators/html/index.en.html>) applies.

162 Consequently, T2S will be closed for settlement in EUR currency on:

163 ▶ Good Friday and Easter Monday;

164 ▶ 1 May

165 When the cash settlement in T2S for one currency is closed (i.e. closing day for this currency only),  
166 securities transactions can nevertheless be settled in T2S either through FOP transactions or through  
167 transactions against payment denominated in other T2S Settlement Currencies. Therefore, T2S  
168 proceeds for settlement in cases of:

169 ▶ availability of all T2S Settlement Currencies, or

170 ▶ availability of EUR and unavailability of any other T2S Settlement Currency, or

171 ▶ unavailability of EUR and availability of at least one other T2S Settlement Currency.

172 The T2S Operator maintains a T2S Calendar by currency, which includes the opening days and  
173 closing days for all T2S Settlement Currencies.

174 **1.5 AVAILABILITY OF SUPPORT**

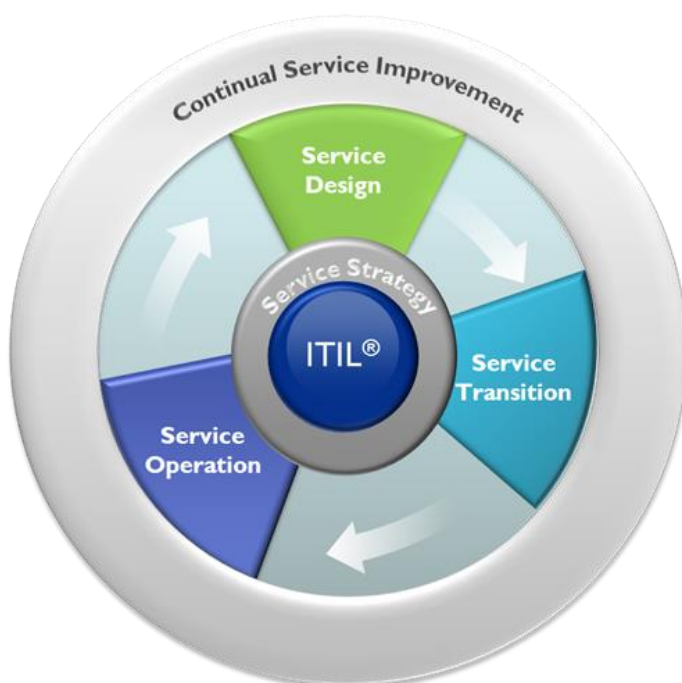
175 The means of interaction and communication used by the T2S Actors (excluding ICPs) vary  
176 depending on the time of the T2S settlement day:

177 ▶ During the standard support hours (6:30 CET – 19:30 CET on all T2S settlement days except  
178 Good Friday and Easter Monday, 1 May), T2S Service Desk offers on-site support.

179 ▶ Outside of the standard support hours, the T2S Service Desk offers on-call support only via the  
180 4CB Crisis Manager in order to communicate information that is urgently needed to avoid or limit  
181 any negative impact on T2S operations. During this time e-mails are not monitored as no e-mail  
182 request is processed outside the standard support hours unless it is pre announced by a phone call  
183 and is related to an on-going incident started outside standard support hours.

184 *Communication means available to T2S Actors (excluding ICPs) to directly contact the T2S Service Desk and*  
185 *information dissemination means used by the T2S Service Desk are described in the previous Table 1 - Support*  
186 *and availability*

187 Moreover, to address any unforeseen situation impacting T2S Operations, the 4CB Crisis Managers  
188 are reachable 24x7.



## Service Operation

- Operational Procedures During Normal Operations and in Abnormal Situations
- Incident Management
- Crisis Management
- Problem Management
- Request Fulfilment
- Access Management

190 **1.6 T2S SETTLEMENT DAY**

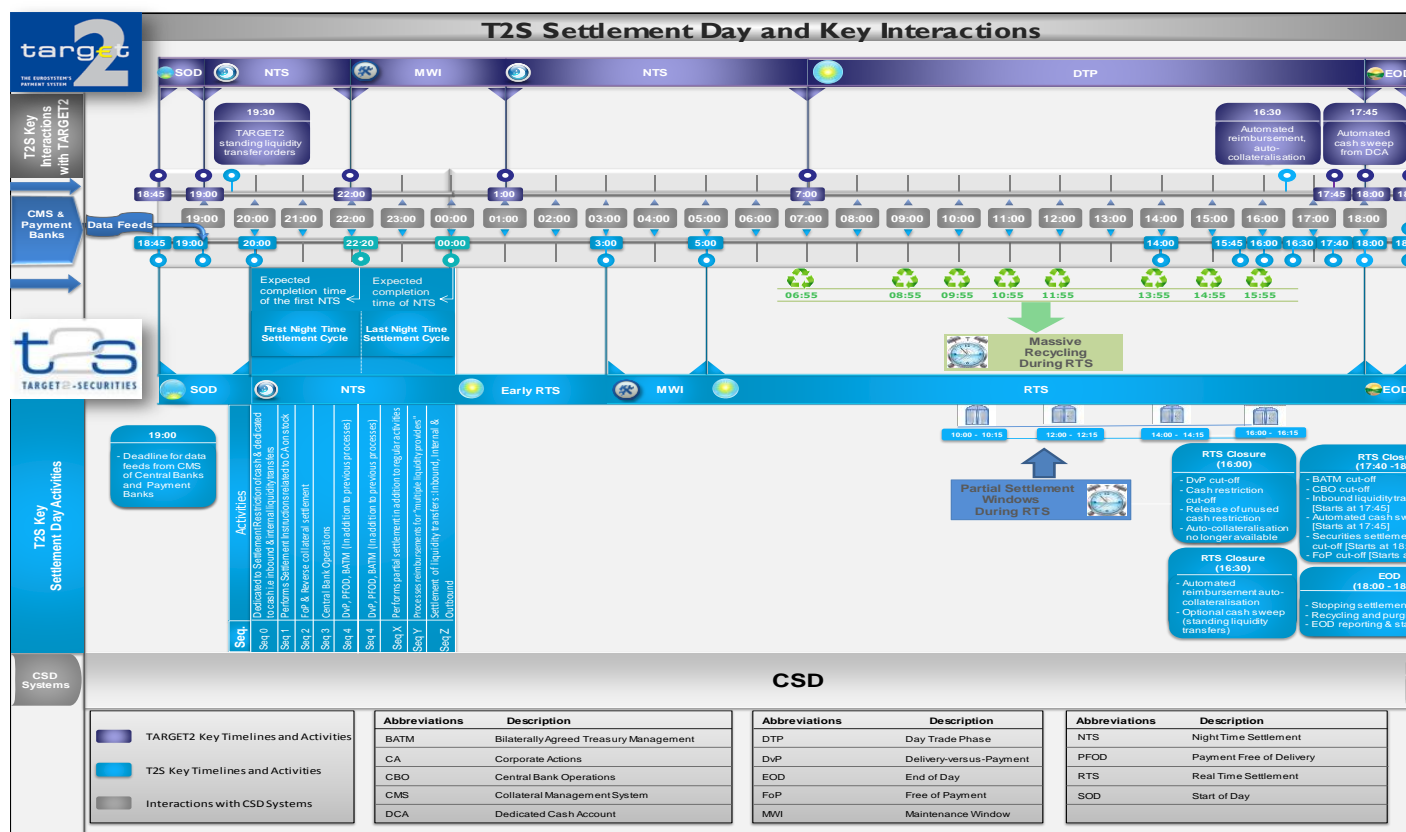
191 **1.6.1 Introduction to the T2S settlement day**

192 T2S facilitates securities settlement in CeBM, according to the calendar of the relevant RTGS system.  
193 The T2S Operator maintains a T2S operating day calendar by currency, which includes the opening  
194 days and closing days for all T2S settlement currencies (see *UDFS V2.0 Section 1.4.1 - T2S*  
195 *Calendar*).

196 A detailed description of the T2S settlement day is available at *T2S UDFS V2.0, Section 1.4.4*. The  
197 tasks related to the T2S settlement day management, business and operations monitoring are  
198 described in the *T2S UDFS V2.0, Section 1.5.3 and 1.5.4*.

199 The T2S settlement day, i.e. Start of Day, Night Time Settlement, Maintenance Window, Real Time  
200 Settlement, and End of Day specific events from an operational point of view and generic procedures  
201 for T2S operations, are illustrated in this Chapter. However, first a description of the change of the  
202 settlement day and queuing during weekends are described in the next two Sections (*1.6.2 and 1.6.3*).

203 The overview of the T2S settlement day is described in

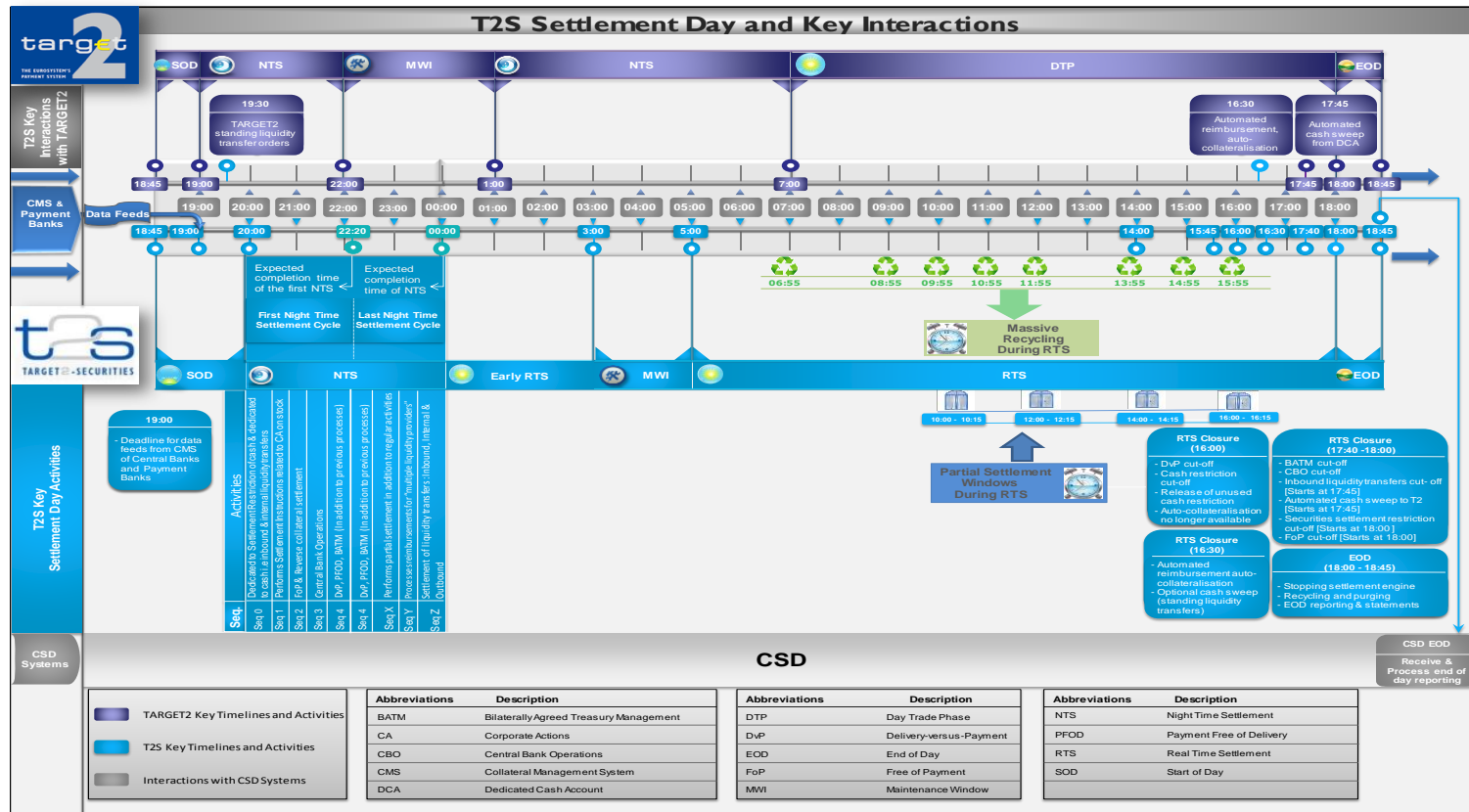


204  
205 *Figure 4, highlighting the key T2S activities and the key interactions between external systems (e.g.*  
206 *TARGET2) and T2S in different phases of the T2S settlement day. Key interactions included in the*

207 figure are those interactions that have a specific deadline. In case such a deadline is not met, it would  
208 affect the normal T2S settlement day, as described in the subsequent section.

209 In the Annex (*Section 2*), a link is provided to the below graphical representation of the T2S  
210 settlement day, to allow printing in different formats (e.g. A3).





211

212

Figure 4 - T2S Settlement Day

## 213 **1.6.2 T2S change of the settlement day**

214 The first action of the start-of-day process is the move to the next T2S settlement day according to the  
215 T2S Calendar, which occurs at **18.45 CET**.

216 On Fridays at **18:45 CET**, T2S moves the settlement date to the next T2S settlement day, i.e.  
217 Monday, and processing continues until Saturday at 03.00 CET. On Monday at 05:00 CET, T2S starts  
218 performing the schedule with the preparation of the real-time settlement as the continuation of the  
219 settlement day.

220 On the day before a T2S closing day, T2S moves the settlement date to the next settlement day (the  
221 first T2S settlement day after the T2S closing day, e.g. 2 January) and processing continues until  
222 03.00 CET on the day of the T2S closing day. On the day after the T2S closing day at 05:00 CET,  
223 T2S starts the schedule with the preparation of the real-time settlement as the continuation of the  
224 settlement day.

## 225 **1.6.3 T2S queuing during weekends and T2S closing days**

226 During weekends and T2S closing days, T2S interfaces and processes are unavailable due to the  
227 regularly executed technical maintenance activities, unless other planned activities take place (e.g.  
228 release deployments, business continuity tests). Therefore, T2S does not queue the messages.  
229 However, the Application-to-Application (A2A) communication will be queued by the NSPs until  
230 T2S is available again (*see Section 1.6.4.3 Maintenance Window (03:00 CET – 05:00 CET)*).

## 231 **1.6.4 Schedule of T2S Settlement Day**

232 The T2S settlement day is made up of a series of scheduled events. These events define the various  
233 processing steps and cut-offs, which are to be carried out during the system's operations. The default  
234 schedule for each settlement day is loaded automatically by the system upon each settlement date  
235 change on the basis of static data. The events which have to imperatively be triggered in the  
236 predefined sequence are linked to each other with a predecessor- successor relationship (*see T2S*  
237 *UDFS V2.0, Section 1.4.3*).

238 In case of an incident lasting through the settlement day occurs, it is possible to adjust the schedule  
239 and reschedule events following the Incident Management and/or Crisis Management procedures (*see*  
240 *Chapter 2 - Incident Management* . The T2S Operator will implement changes manually on the  
241 current T2S settlement day schedule at runtime in exceptional situations.

242 The schedule of a T2S settlement day constitutes the major periods as listed below:

- 243 ► start of day (SOD);

244 ▶ night-time settlement (NTS);

245 ▶ maintenance window (MWI);

246 ▶ real-time settlement (RTS);

247 ▶ end of day (EOD).

248 The following sections describe the procedural tasks during a normal operational day. The MOP  
249 describes only the procedures that are relevant for all T2S Actors (excluding ICPs).

#### 250 1.6.4.1 Start of day (18:45 CET – 20:00 CET)

251 The SOD process is launched at **18:45 CET**. This is confirmed via the “Status of the T2S settlement  
252 day Notification” message, an entry in the T2S GUI “Daily Schedule” screen and “T2S Diary  
253 Response” query response message.

254 The SOD period includes:

255 ▶ changing of settlement date in T2S;

256 ▶ preparing the NTS:

257 ■ Revalidating settlement and maintenance instructions that failed to settle or to be executed as  
258 of their Intended Settlement Date (ISD);

259 ■ Accepting data feeds from Collateral Management Systems (CMS) and Payment/ Settlement  
260 Banks received continuously throughout the day. However, 19:00 CET is the final deadline to  
261 accept data feeds (e.g. auto-collateralisation, client-collateralisation) effective for the current  
262 settlement date;

263 ▶ Valuation of securities positions;

264 ▶ Valuation of collateral eligible Settlement Instructions.

265 During this period settlement does not take place. This period is used by the T2S Actors (excluding  
266 ICPs) to prepare for NTS (e.g. corporate actions (CA) processing). Settlement instructions for  
267 processing in the NTS can be submitted during this period.

#### 268 1.6.4.2 Night-time settlement (20:00 CET– 03:00 CET)

269 The NTS starts after the successful completion of the SOD period and is followed by the MWI and  
270 the RTS periods. This is confirmed via the “Status of the T2S settlement day Notification” message,  
271 an entry in the T2S GUI “Daily Schedule” screen and the “T2S Diary Response” query response  
272 message (messages are available to the T2S Actors (excluding ICPs) upon subscription).

273 In case NTS completes before **03:00 CET** RTS begins immediately after the NTS completion,  
274 before the scheduled start of the MWI at **03:00 CET**. The target completion time of NTS is **00:00**  
275 **CET**. The target completion time of the first NTS cycle is at **22:20 CET**.

276 During the NTS, T2S processes the settlement instructions, settlement restrictions and liquidity  
277 transfers in two settlement cycles, according to an automatic predefined order called “sequence”. A  
278 Settlement Cycle consists of more than one sequence (for settlement of different types of settlement  
279 instructions, settlement restrictions and liquidity transfers).

280 The NTS sequences in T2S include processing of

281 ▶ new settlement instructions, settlement restrictions and liquidity transfers received before the start  
282 of the sequence which are eligible for settlement during this sequence (e.g. for the sequence 0  
283 those received in T2S before **20:00**);

284 ▶ pending settlement instructions not settled during previous sequences.

285 T2S validates and accepts the static data maintenance instructions and other maintenance instructions  
286 (e.g. cancellation instructions, amendment instructions or hold/release instructions during the NTS  
287 period on a continuous basis. However, these updates are only processed in between the different  
288 sequences, unless these updates do not impact the settlement (see *UDFS V2.0, Section 1.6.3*). T2S  
289 sends the information on the status of the static data maintenance instructions and maintenance  
290 instructions immediately after the end of their processing (i.e. acceptance, execution).

291 For all static data updates, i.e. immediate updates and updates with future date, T2S also performs a  
292 validation of all settlement instructions and settlement restrictions to ensure that they are valid for the  
293 intended static data update.

294 In case a maintenance instruction was created for a settlement instruction or a settlement restriction,  
295 but the underlying settlement instruction or settlement restriction has been cancelled during  
296 revalidation, the maintenance instruction execution will be denied, but the maintenance instruction  
297 will not be cancelled.

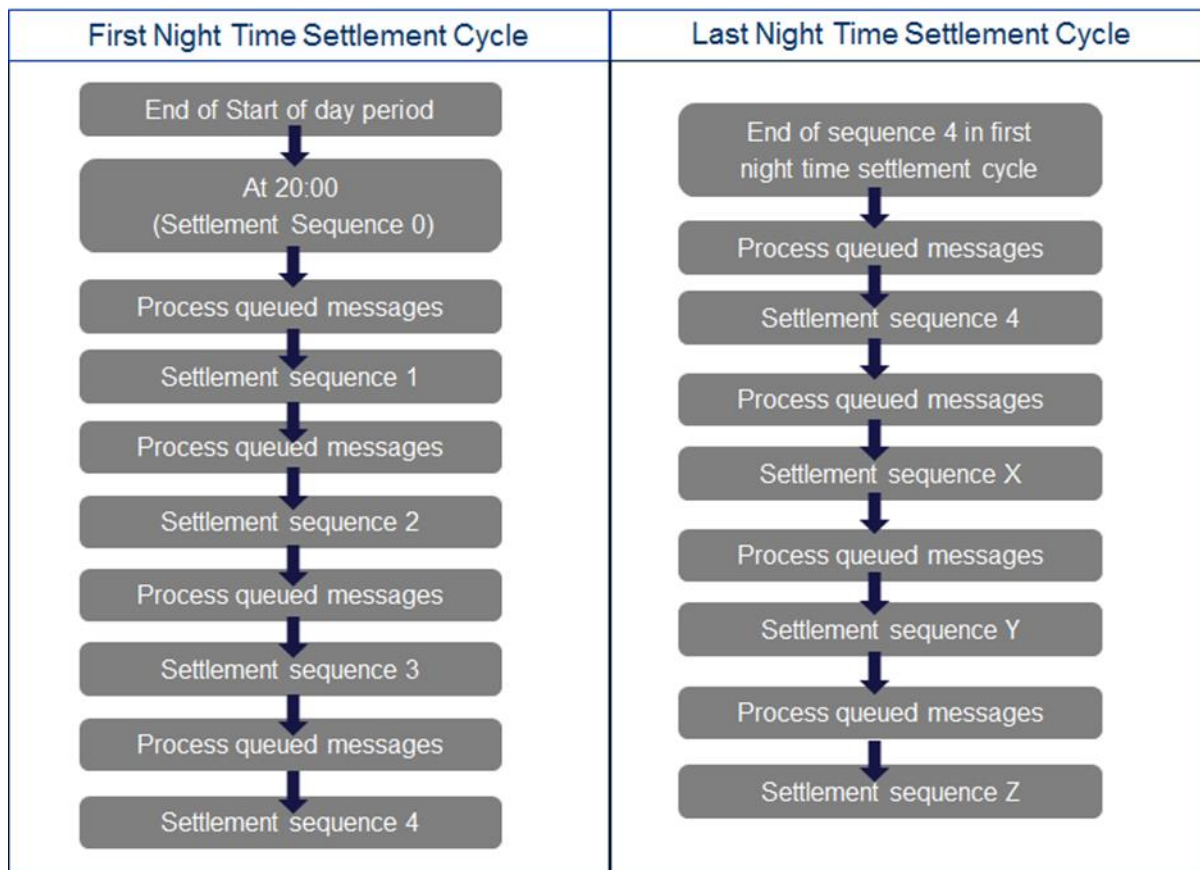
298 Queries related to securities positions and cash account balances, received and validated during a  
299 settlement sequence, are processed by the T2S with a query response back to the sending party after  
300 completion of the sequence. All other queries are processed immediately.

301 Once the processing of an NTS sequence is completed, T2S sends the messages that were queued  
302 during the execution of the settlement sequence, i.e. settlement advice, settlement confirmation,  
303 posting notification, etc.

304 At the end of each NTS sequence, T2S generates full or delta reports as per report configuration setup  
305 of the respective CSD, Central Bank or DCP.

306 During the NTS, T2S performs the processes in two different settlement cycles, as document in the  
 307 following table.

308



309

310

Figure 5 - T2S settlement cycles

311 Generally, NTS sequences perform the same activities. However, certain sequences in the NTS are  
 312 dedicated to specific activities and processing specific set of messages. These sequences are described  
 313 below:

- 314 ▶ Sequence 0 is dedicated to cash i.e. inbound liquidity transfers, internal liquidity transfers and  
 315 other cash settlement restrictions. T2S reattempts the inbound liquidity transfers and cash  
 316 settlement restrictions in subsequent sequences in case it is unable to process in sequence 0.
- 317 ▶ Sequence 1 performs settlement of instructions related to CA on stock new liquidity transfers,  
 318 new cash Settlement Restrictions and all cash Settlement Restrictions not settled in the previous  
 319 sequence.

320 ▶ Sequence X performs partial settlement in addition to regular activities. T2S applies partial  
321 settlement to all fails due to lack of securities or cash which are eligible for submission to partial  
322 settlement processing.

323 ▶ Sequence Y processes reimbursements for “multiple liquidity providers”. This reimbursement  
324 procedure involves the execution of a series of outbound liquidity transfers from a DCA (of a  
325 payment/ settlement bank in T2S) to RTGS accounts in accordance to a pre-set sequence of  
326 reimbursement.

327 The end of the NTS is confirmed via an entry in the T2S GUI “Daily Schedule” screen and the “T2S  
328 Diary Response” query response messages, which are available to CSDs, Central Banks and DCPs  
329 upon request.

#### 330 1.6.4.3 Maintenance Window (03:00 CET – 05:00 CET)

331 The MWI is scheduled from 03:00 CET until 05:00 CET after the completion of the NTS period. The  
332 start of maintenance window is reported via “Status of the T2S settlement day Notification”  
333 (messages are available to T2S Actors (excluding ICPs) upon subscription).

334 During the maintenance window and with the exception of the T2S interface application process, all  
335 T2S processes are unavailable. The interface application process starts the queuing of all requests  
336 received in A2A mode. This is followed by a technical validation (i.e. format validation) of the  
337 incoming A2A store and forward messages (or files).The U2A communication as well as A2A real  
338 time messages are not queued during the MWI.

#### 339 1.6.4.4 Real-time settlement (05:00 CET – 18:00 CET)

340 The RTS starts after the end of the NTS<sup>5</sup> and is followed by the EOD.

341 The RTS period includes:

- 342 I. Preparing the real-time settlement;
- 343 II. Performing the real time settlement with the two partial settlement windows to optimise  
344 maximum value and volumes of settlement transactions;
- 345 III. Closing the real time settlement with different cut-offs for settlement instructions, settlement  
346 restrictions and liquidity transfers categories.

347

---

<sup>5</sup> Following the indicative timing for the completion of the NTS the start of RTS could be already at 00:00 CET.

348 **I. Preparing real-time settlement**

349 The start of the RTS is confirmed via the "Status of the T2S settlement day Notification" message, an  
350 entry in the T2S GUI "Daily Schedule" screen and "T2S Diary Response" query response messages,  
351 which are available to the T2S Actors (excluding ICPs) upon request.

352 T2S identifies and processes static data maintenance instructions received in the A2A.

353 T2S identifies new settlement instructions, maintenance instructions and liquidity transfers available  
354 for the current settlement day. T2S identifies all settlement and maintenance instructions, not settled  
355 and/or executed during the NTS period, and recycle them for RTS. The recycling takes place after the  
356 revalidation of the settlement instructions and settlement restrictions, subject to a static data change.

357 **Massive recycling of failed transactions during RTS**

358 Massive recycling is a time driven function, that triggers recurrent and automatic recycling of all  
359 transactions failed due to lack of resources. The failed transactions are submitted for settlement during  
360 the massive recycling.

361 In T2S the massive recycling is performed at predefined time which are 06:55, 08:55, 09:55, 10:55,  
362 11:55, 13:55, 14:55 and 15:55 CET. Since massive recycling is time based and settlement runs in  
363 parallel, it does not affect other T2S Services.

364 .

365 **II. Performing the real-time settlement**

366 RTS attempts to process all new settlement instructions, maintenance instructions and newly received  
367 liquidity transfers intraday in T2S and all previous unsettled settlement instructions after the arrival of  
368 new securities and/or cash resources.

369 T2S also performs the execution of static data maintenance instructions. Additionally, T2S revalidates  
370 all settlement instructions and all settlement restrictions, subject to static data updates. Moreover,  
371 T2S generates reports triggered by business or time events.

372 The RTS also includes the following four partial settlement windows:

- 373 ▶ First partial settlement window **(10:00 CET– 10:15 CET);**
- 374 ▶ Second partial settlement window **(12:00 CET - 12:15 CET);**
- 375 ▶ Third partial settlement window **(14:00 CET - 14:15 CET);**
- 376 ▶ Fourth partial settlement window **(15:45 CET- 16:00 CET), 15 minutes before the beginning of**  
377 **the DVP cut-off time.**



- 378       ▪ During the partial settlement windows, T2S takes care of: Partial settlement of new settlement  
379       instructions arriving into T2S in this period, eligible for partial settlement.
- 380       ▪ Settlement of previously unprocessed or partially processed settlement instructions, eligible  
381       for partial settlement.
- 382 All processes available during the real time settlement are also available during both the partial  
383 settlement windows.

384 **III. Closing real-time settlement**

385 The process starts after the completion of the second partial settlement window. It does not start  
386 before 16:00 CET. The following processes are executed sequentially:

TIME (CET)	T2S settlement day events / processes
16:00	DVP cut-off
16:00	Cash restriction cut-off
	Release of unused cash restriction
16:30	Automatic reimbursement
	Optional cash sweep (standing liquidity transfers)
17:40	Bilaterally Agreed Treasury Management (BATM) cut-off
17:40	Central Bank Operations (CBO) cut-off
17:45	Inbound liquidity transfers cut-off
	Automated cash sweep
18:00	Securities restriction cut-off
18:00	FOP cut-off

387 *Table 2 - Sequential settlement day event*

388 The cut-offs are confirmed via an entry in the T2S GUI “Daily Schedule” screen and the “T2S Diary  
389 Response” query response messages, which can be available to the T2S Actors (excluding ICPs)  
390 upon request.

391 1.6.4.5 End of day (18:00 CET – 18:45 CET)

392 T2S settlement day closes at **18:00 CET**. The EOD processing starts after the successful completion  
393 of the RTS period, when settlement no longer takes place. It is followed by the SOD period of the  
394 next settlement day.

395 Following the cut off and until **18:45 CET**, the following events take place:

- 396 ▶ Stopping settlement engine;
- 397 ▶ Recycling and purging;
- 398 ▶ End of day reporting and sending statements.

399 T2S generates all the EOD reports as per the agreed prioritisation and sends them to the subscribing  
400 T2S Actors (excluding ICPs). The agreed prioritisation is:

- 401 ▶ Statement of holdings

- 402 ▶ Settled settlement instructions
- 403 ▶ Pending settlement instructions
- 404 ▶ Statement of Account
- 405 ▶ Statement of Settlement Allegement
- 406 ▶ Statement of settled intra-balance movements
- 407 ▶ Statement of pending intra-balance movements

408

409 The execution of the EOD process is confirmed via the "Status of the T2S settlement day  
410 Notification" message, an entry in the T2S GUI "Daily Schedule" screen and "T2S Diary Response"  
411 query response messages, which are available to the T2S Actors (excluding ICPs) upon request.

#### 412 **1.6.5 Delay start of D + 1 settlement day in case of RTGS delay**

##### 413 **Issue Description**

414 The RTGS system (e.g. TARGET2) either (i) has not yet closed its previous business day due to a  
415 delay or due to some unexpected incapability<sup>6</sup> or (ii) is not capable of starting the new business day.

##### 416 **Issue Resolution**

417 If the RTGS Operator (TARGET2 Coordinator) realises that it is not possible to close the RTGS  
418 system in time or the RTGS system is not able to change to the next business day, then the RTGS  
419 Operator will immediately inform the T2S Coordinator. The T2S Coordinator initiates the T2S  
420 Incident Management process (see *Chapter 2 - Incident Management, Section 2.1*).

421 T2S settles against cash on DCAs that receive funds from RTGS accounts. At the end of the day,  
422 liquidity is reimbursed to these RTGS accounts. Moreover, T2S is supporting auto-collateralisation  
423 features in a fully harmonised way, allowing settlements to take place without injecting additional  
424 cash.<sup>7</sup>

425 In case of a RTGS delay, T2S Operator can either (i) delay the start of settlement of the given  
426 currency in T2S for the next T2S settlement day, (ii) delay the start of T2S, or (iii) start the normal

---

<sup>6</sup> The relevant TARGET2 procedures are described in the Information Guide for TARGET2 users.

<sup>7</sup> It should be noted that the collateralisation techniques and the set-up for auto-collateralisation is not uniform among the central banks.

427 T2S processing, including for the currency of delayed RTGS system but only under the condition that  
428 the RTGS system successfully closed the previous business day.

429 The T2S decision depends on different aspects such as:

430 ▶ reason (technical or operational) and status (is the current business day closed or not) for the  
431 RTGS delay;

432 ▶ expected duration of the RTGS delay;

433 ▶ expected liquidity situation;

434 ▶ impact of prolonged T2S delay or T2S start on financial stability and financial markets.

435 In case the RTGS has not yet closed the current business day, the available solutions are either (i) to  
436 delay the start of settlement for the delayed currency or (ii) to delay the start of T2S for the next T2S  
437 settlement day. To prevent the currency from settling on the DCAs for the next T2S settlement day a  
438 specific restriction on the Party Central Bank will be set.<sup>8</sup>

439 Alternatively, but only in case the RTGS has closed the current business day, it will be possible to  
440 start the settlement for the next T2S settlement day in T2S without liquidity and rely on auto-  
441 collateralisation.

## 442 **1.6.6 Processing of the CMS data feed**

### 443 **Issue description**

444 The data feed for the list of eligible collateral and collateral valuation prices from the Collateral  
445 Management Systems (CMSs) is not available at 19:00 CET.

446 Central Banks that offer auto-collateralisation and Payment Banks that offer client-collateralisation in  
447 T2S are responsible for the setup and maintenance of the auto-collateralisation feature in T2S,  
448 including the configuration of static data. This information (data feed) will be provided directly via  
449 the respective CMS.

450 The CMS data feed related to the list of eligible securities for auto-collateralisation is communicated  
451 by the CMS to T2S when changes occur. With regards to the valuations of the eligible securities, the  
452 valuation is expected to be provided to T2S on a daily basis. CMS data feeds (complete set of  
453 securities valuation coefficient, delta of eligible assets, and eligible links) can be provided throughout  
454 the day; however, the data for the respective settlement day is only activated at 19:00, during the Start  
455 of Day processes.

---

<sup>8</sup> The restriction applies to all the currencies associated to the Central Bank.

456 Once the preparation of the Night-Time Settlement starts during the Start of Day process, T2S  
457 performs a check to confirm that CMS data feeds, effective for the current settlement day, have been  
458 processed in T2S. A check is also performed to confirm that for each eligible security for auto-  
459 collateralisation a valuation has been provided to T2S.

460 The unavailability of the data could be because:

- 461 ▶ CMS data feeds are not yet received by T2S;
- 462 ▶ Data feeds supplied by CMSs are not valid (i.e. cannot be processed by T2S);
- 463 ▶ CMSs supplied the data feed before 19:00 but they are blocked at the T2S Interface.

#### 464 **Issue resolution**

465 In case of unavailability in T2S of the necessary data feeds from one or several CMSs, as a general  
466 procedure, the settlement day processing is blocked and a predefined alert is raised to the T2S Service  
467 Desk. The T2S Service Desk manually resumes the T2S settlement day allowing the system to use the  
468 previous available data for the missing valuation of eligible securities<sup>9</sup> unless the NCB (its own or on  
469 behalf of their Payment Bank) triggers Incident Management process at the latest by 18:30.

470 In case the issue is on the side of T2S and there is a risk that the prices are not processed in time, the  
471 T2S Service Desk will contact the involved Central Bank(s) to ask for an authorisation to proceed  
472 with the operational day.

473 If there is a need to wait for the missing data feeds (e.g. because certain assets need to be deleted or a  
474 workaround is needed), the T2S delay procedure will be activated.

### 475 **1.6.7 Night-time algorithms processing during RTS**

#### 476 **Issue description**

477 There is abnormally low successful settlement rate during NTS.

#### 478 **Issue resolution**

479 When the number of transactions might overload the RTS Algorithms' capability to process all the  
480 transactions a technical analysis is performed and the T2S Service Manager may propose to run the  
481 OBM (Optimisation Batch Manager). The OBM is a special algorithm to manage unexpected high  
482 volumes during RTS to increase the number and value of transactions settled in T2S.

---

<sup>9</sup> Alternatively some workarounds can be applied e.g. setting zero price for unavailable data, manually revoking eligibility prior to 19:00, manually setting the auto-collateralisation limits to zero, or restricting the provision of auto-collateralisation.

- 483 ▶ The T2S Service Manager will initiate the Incident and Crisis Management process. A Settlement  
484 Managers' conference call will be initiated to inform the Settlement Managers<sup>10</sup> about the  
485 possibility to run an OBM and to agree on the timing.
- 486 ▶ A broadcast via T2S GUI will be sent to all T2S Actors (excluding ICPs) in order to inform about  
487 the changed settlement pattern and to ensure provisioning of sufficient resources. The T2S  
488 Operator starts the OBM at the agreed time, closely monitors the situation and informs the T2S  
489 Coordinator if the situation is resolved.
- 490 ▶ After the volumes are normalised, according to the standard Incident Management process, the  
491 T2S Service Manager will inform the T2S Coordinator about the situation who will initiate a  
492 Settlement Managers' conference call followed by Crisis Managers' conference call (if deemed  
493 necessary) in order to decide to de-activate the OBM and to proceed with normal processing.
- 494 ▶ A broadcast via T2S GUI to all T2S Actors (excluding ICPs) is sent accordingly.

495

## 496 **1.6.8 T2S delay**

### 497 **Issue description**

498 During the T2S settlement day different situations may occur which require the postponement of one  
499 or more phases of the T2S settlement day or even a delay of the closure of the settlement day. This  
500 may, on the one hand happen in case T2S itself is, due to different reasons (e. g. a software bug),  
501 unable to continue with the phases of the T2S settlement day as scheduled. On the other hand, also  
502 issues outside T2S may impact the T2S Schedule.

503 The following non-exhaustive list of causes might lead to a delay:

- 504 ▶ T2S failure;
- 505 ▶ settlement and liquidity management services failure;
- 506 ▶ static data services failure;
- 507 ▶ information services failure;
- 508 ▶ connectivity services failure;
- 509 ▶ CSD failure;

---

<sup>10</sup> The view of the TARGET2 Coordinator should be taken into account as the business day phase of TARGET2 and liquidity aspects may play a role in the decision-making.

510 ▶ RTGS failure;

511 ▶ CMS services failure;

512 ▶ Other reasons.

### 513 Issue resolution

#### 514 I. Overview

515 The decision to delay the start of the night time settlement phase or to postpone any other phase of the  
516 T2S settlement day is always made by the Crisis Managers. A delay is requested to T2S Service Desk  
517 and the T2S Coordinator is informed by the T2S Service Desk. The T2S Coordinator will initiate a  
518 Settlement Managers' conference call to inform about the request and to schedule a Crisis Managers'  
519 conference call immediately. The Crisis Managers shall decide on T2S delay at the latest 15 minutes  
520 before the requested start of the delay.

521 In case of a T2S failure that triggers the failover to another site or region, there is no other possibility  
522 than to wait until the platform recovers and to delay the closing/ postponing the phase. Meanwhile,  
523 the Crisis Managers will be informed.

524 The T2S Coordinator shall inform the T2S Actors as early as possible about the possible duration of  
525 the delay/ postponement. As long as this cannot be anticipated, regular updates of the situation will be  
526 provided.

#### 527 II. Timing of the decisions

528 Decisions on delays and/or postponement of cut-offs shall be taken as early as possible to reassure the  
529 markets that they have sufficient time to process all their business.

530 The first information is exchanged at the Settlement Manager level together with the collection of  
531 facts. Due to a possibly tight time frame it is of extreme importance that the conference calls  
532 (information collection and impact analysis) are done in a structured way.

#### 533 III. Collection of information

534 The information about the incident and when possible the impact shall be collected at the level of the  
535 Settlement Managers.

536 Collection of information during Settlement Managers' conference call should ideally (i.e. if known at  
537 this point in time, lack of known information must not delay the process here) comprise:

538 ▶ short description of the event including a clear request for a delayed closing;

539 ▶ expected time required (how long to delay);

- 540 ▶ impact on CSDs/ Central Banks with values and volumes at stake;
- 541 ▶ special days in CSDs' business (e.g. end of year, special CA processing);
- 542 ▶ impact on TARGET2 and other RTGS systems (incl. mentioning of special days like end of  
543 minimum reserve period, end of quarter).

544 Information not available at the time of the Settlement Managers' conference call, but likely to be  
545 there when the Crisis Managers have their conference call shall be clearly identified and mentioned.

546 The acceptance or rejection of a request for delay by the Crisis Managers is based on the following  
547 criteria:

- 548 ▶ time of the day;
- 549 ▶ length of the delay;
- 550 ▶ possible systemic impacts if the delay is not accepted or if the delay is accepted.

551 In the event of a T2S failure, there is no alternative but to wait for the recovery of the T2S Platform  
552 and to provide the necessary time for the CSDs and Central Banks to finish their processing.

553 At the end of the conference call, the T2S Coordinator will summarise the conclusion of the  
554 conference call preferably with an agreed recommendation to be presented for decision to the Crisis  
555 Managers, with the following structure:

- 556 ▶ reason for the delay;
- 557 ▶ impact of the delay;
- 558 ▶ proposal to accept or reject the request;
- 559 ▶ impact in case of rejection;
- 560 ▶ available options and impact in case of acceptance.

561 Immediate after the Settlement Managers' conference call, the Crisis Managers' conference call will  
562 be initiated, and the Crisis Management process applies.

#### 563 **IV. Minimum length of the T2S Settlement Day and minimum duration of the operational** 564 **day phases**

565 In order to help the evaluation of the impact of a delay and to speed up the decision making it is useful  
566 to identify the minimum duration of each phase and, consequently, the minimum duration of a whole  
567 settlement day. The following table illustrates for each main phase of the T2S settlement day the



568 standard times and the minimum times needed to complete the activities from T2S and from CSD/  
569 NCB side. The minimum duration defined in the table below is applicable once all the migration  
570 waves are complete.

T2S settlement day phase	Standard time	Minimum duration (indicative)	Actual duration <sup>11</sup> (indicative)
Start of Day (18:45 to 20:00)	75 minutes	75 minutes	75 minutes
Night Time Settlement (20:00 to 3:00)	7 hours	4 hours	1 hour 15 minutes
Maintenance Window (3:00 to 5:00)	2 hours	0	0
Real Time Settlement (first part 5.00 to 16.00)	11 hours	4 hours	4 hours
Real Time Settlement (second part 16.00 to 18.00)	2 hours	2 hours	2 hours
End of Day (18:00 – 18:45)	45 minutes	45 minutes	15 minutes
Total	24 hours	12 hours	8 hours 45 minutes

571 *Table 3 - Minimum Duration of Each Phase and Minimum Time to Complete Activities*

572 The table is a tool in the hand of the T2S Coordinator and the CSD's/ Central Bank's Settlement  
573 Manager and Crisis Managers to quickly evaluate the impact of a delay on the operational day. For  
574 example after a recovery of the T2S Platform the information present in the table will help to identify  
575 how much time would be needed to complete the settlement day without delaying of the EOD/ SOD,  
576 or in case of prolonged outage what is the impact on the following settlement day. Tools will be  
577 available to the participants of the Settlement Managers' and Crisis Managers' conference call to  
578 visualize the effect of the delay on the current and following T2S settlement days and on the  
579 interconnected systems.

## 580 **V. Prolonged T2S outage**

581 Such scenario covers the unlikely situations that, despite all the efforts (normally after several  
582 subsequent delays) T2S cannot start the new T2S settlement day without impacting the timely closure  
583 of the next T2S settlement day. As, declaring the next day as non T2S settlement day, would cause the  
584 system to reject instructions with that Intended Settlement Date, the only solution is to run one or  
585 more "special" T2S settlement days skipping the maintenance window and where possible reducing

---

<sup>11</sup> Values represent a statistical calculation on the basis of wave 1 volume. These values require update after each migration. The Real Time Settlement phase includes in total four partial settlement windows at 10:00, 12:00, 14:00 and 15:45.

586 the duration of certain settlement phases to catch up with the processing and to resume the normal  
587 settlement day as soon as possible. For such decision the Crisis Management process will be followed.

## 588 **1.6.9 T2S processing with limited liquidity**

### 589 **Issue description**

590 A situation might occur that while T2S is able to open and start the settlement day, no or only some  
591 liquidity transfers have been received. This situation can occur due to the following reasons:

- 592 ▶ RTGS is running, but there is a failure of liquidity transfer processing in the RTGS;
- 593 ▶ failure of communication between the RTGS system and T2S ;
- 594 ▶ RTGS had closed the previous business day for payment processing (and T2S has opened),  
595 however, the RTGS has a failure during its subsequent phases i.e. Start of Day, Night Time  
596 Settlement, or Real Time processing.

597 Any of the above failures affect the Inbound Liquidity Transfers (from an RTGS account to a DCA)  
598 which are initiated in the relevant RTGS System and cannot be triggered in T2S. It concerns  
599 Immediate, Predefined and Standing Liquidity Transfer Orders equally, which execution is possible  
600 during the NTS sequences and the RTS period.

## 601 Issue resolution

602 If only some Liquidity Transfers are missing, the T2S Operator monitors and checks the issue with the  
603 RTGS Operator and the relevant T2S Actors (excluding ICPs) (see *Chapter 2 - Incident Management*).

604 T2S can settle without injecting additional cash due to its auto-collateralisation features. Therefore, in  
605 case of an RTGS failure, T2S can continue processing without RTGS liquidity provision or with  
606 limited liquidity available from auto-collateralisation and settle FOP transactions. The Incident  
607 Management process (see *Chapter 2 - Incident Management, Scenario 2: Incident at the level of*  
608 *TARGET2/ RTGS*) will be launched and a Settlement Managers' conference call will be initiated on  
609 the T2S side whereas the RTGS Operator will monitor and handle the failed Liquidity Transfers, and  
610 initiate its own contingency measures.

611 If disruption in the RTGS System is so severe that it cannot be solved for a prolonged time and the  
612 liquidity situation is not expected to improve in the T2S system, the T2S Crisis Managers may decide  
613 to delay the actual settlement phase in T2S.

### 614 1.6.10 Opening T2S on weekends for settlement

#### 615 Description

616 In addition to the procedure to open T2S during weekends for trial purposes (i.e. business continuity  
617 related tests of T2S system), in specific situations T2S could be opened during a weekend for  
618 settlement in the following cases:

- 619 ▶ A large issuance in a direct holding country;
- 620 ▶ Major releases deployment on the side of the CSDs and Central Banks ;
- 621 ▶ Major T2S release deployment;
- 622 ▶ Business continuity verification at CSDs/NCBs level.

623 The purpose of requesting T2S to open during weekends for settling real instructions (i.e. without any  
624 code words required) is to allow identifying and solving potential problems (in case of a release  
625 deployment) or settle potential large volumes (e.g. large issuance in a direct holding country) on  
626 Saturday instead of Monday morning. When this is requested by CSDs/NCBs within their business  
627 continuity verification, the possibility to settle instructions in Real Time under the option 3 (see  
628 below) is a complement of the exercise itself as requested by the supervisory authorities.

629 T2S would be open for these activities and would provide all services as available on a normal  
630 settlement day, except liquidity transfers as the RTGS systems would not be available at that time. To  
631 this extent, time triggered Standing Orders Liquidity Transfers should be deactivated on Friday and

632 re-activated on Monday by T2S operator to avoid their unwished execution. Transactions executed  
633 during the weekend activities would have a settlement date of Monday since they are executed after  
634 the Start of Day event. Time-triggered reports whose scheduled time falls during the real-time phase  
635 on Saturday (options 1 and 3), will not be executed.

636 The above listed activities are expected to be performed outside the Maintenance Window of the  
637 NSP..

### 638 Operational procedure

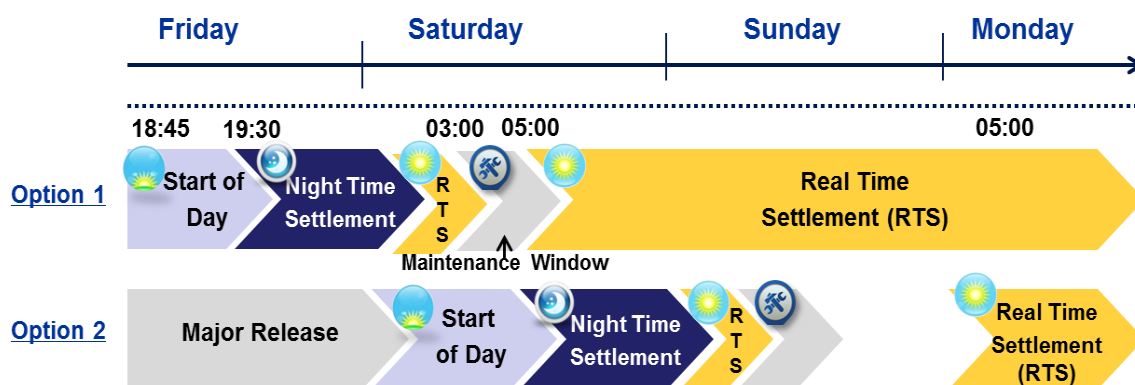
639 Three different options are available to open T2S for settlement during weekend:

640 ▶ Option 1: The NTS cycles followed by short RTS are completed and T2S would open for RTS  
641 settlement on Saturday after a shortened Maintenance Window (MWI) at a time to be agreed on a  
642 case by case basis depending on the activities to be concretely performed as well as on the  
643 duration of the release and deployment management activities. In such case the RTS would  
644 remain open until Monday at 5:00 (normal RTS beginning after the week-end) and even continues  
645 until Monday start of EOD;

646 ▶ Option 2: The T2S Start of Day event (standard time 18:45) and the following NTS, RTS and  
647 MWI phases are postponed to Saturday morning. They will start after the T2S or CSD and/ or  
648 NCB major release deployment phase is completed;

649 ▶ Option 3: The NTS cycles are completed and T2S would open for RTS settlement. This real-time  
650 phase would then remain opened until the end of the business continuity verification (time to be  
651 agreed as per CSDs' request). Afterwards, the system would enter into the maintenance window  
652 until Monday morning at 5:00 am as normally.

653



654



655

656

Figure 6 - T2S Operation during Weekend for Settlement

657 Regarding option 1 and 3 the request to open T2S during weekends for settlement is submitted to the  
658 T2S Service Desk via signed e-mail at least three months in advance, if not already included in the  
659 yearly business continuity tests calendar. The T2S Service Desk will inform the T2S Coordinator  
660 accordingly. After the feasibility check, the agreement is requested from the whole community via e-  
661 mail to Settlement Managers. The Settlement Managers can provide agreement/ disagreement within  
662 next five (5) days. Only in case of need (e.g. diverging views or different organisational needs to be  
663 accommodated) a Settlement Managers' conference call will be organized.

664 Option 2 is planned in advance according to the T2S release plan that includes time plan of major  
665 releases from CSDs and Central Banks.

### 666 1.6.11 Updating rule-based models

#### 667 Description

668 Following the specifications (see *UDFS V2.0, Section 1.7.7*), the T2S application allows T2S Actors  
669 (excluding ICPs) to configure rule sets and their parameters in a flexible way.

670 They can configure these features on the basis of rule based models, i.e. sets of rules combining a  
671 number of possible parameter types. They can update these configurations intraday directly in the  
672 production environment, but depending of the static data item the changes may only be effective as of  
673 the next day.

674 As performing these changes without any previous testing activity could lead to adverse effects in  
675 production and result in operational risk, it is strongly recommended to first test such changes.

676 The CSDs and/or Central Banks are ultimately responsible for the correct set up of their  
677 configurations.

#### 678 Operational procedure

- 679 ► CSDs and/or Central Banks are requested to announce changes to rule based models to the T2S  
680 Service Desk one T2S settlement day before the new validity date starts; the announcement  
681 should be sent via a signed e-mail. The message subject line must clearly indicate "Rule Based  
682 Model" in the header;

- 683 ▶ It is strongly recommended that the respective CSDs and/or Central Banks verifies the  
684 configuration in a test environment in order to check that the configuration fully complies with  
685 the business rules intended to be implemented. For example, if the configuration refers to the  
686 definition of a restriction type case, the respective CSD or Central Bank has to check that the  
687 newly configured restriction type accepts/ rejects or puts on hold incoming settlement instructions  
688 in the appropriate way.
- 689 ▶ The implementation in the production environment is under the respective CSD or Central Bank's  
690 responsibility, ensuring that the configuration is correctly replicated;
- 691 ▶ The CSDs or Central Banks are recommended to perform this step in 4-eyes-mode.

## 692 **1.6.12 Handling unwanted consequences of rules-based model updates**

### 693 **Description**

694 Following the implementation of new rule based model updates, the T2S Operator monitors the T2S  
695 behaviour (business as usual).

### 696 **Operational procedure**

697 In the unlikely case the T2S Operator detects that any abnormal system behaviour, even if not  
698 necessarily causing an incident is caused by a new configuration in the production environment, it  
699 contacts immediately the CSD/ Central Bank having created or updated the respective configuration  
700 in order to provide feedback on the anomaly and agree corrective actions. The T2S Coordinator is  
701 kept informed in parallel.

702 If the overall situation is already or potentially going to remarkably impact the system and other  
703 participants, the T2S Operator in coordination and agreement with the CSD/ Central Bank is able to  
704 invalidate a configuration by restoring the previous configuration. In case of a system-wide impact, a  
705 Settlement Managers conference call will be initiated.

- 706 ▶ The T2S Operator contacts the respective CSD/ Central Bank that initiated the change and the  
707 T2S Coordinator and agrees the proposed corrective action;
- 708 ▶ The T2S Operator agrees with the respective CSD/ Central Bank if the rule set should be amended  
709 or invalidated and the timing of the implementation.
- 710 ▶ To invalidate a rule set the T2S Operator may use the standard Static Data maintenance functions  
711 for updating the validity period. The T2S Operator can immediately (and temporarily) invalidate a  
712 whole rule set (i.e. a restriction type or a message subscription rule set or a CoSD rule set) by  
713 updating its validity period so that it does not include the current settlement day and it does not  
714 affect future-dated settlement instructions;

715 ▶ The activities are afterwards summarised by the T2S Operator in a signed e-mail where the  
716 reference clearly quotes “Rule based model – Correction”.

717 Once the negative effects of the wrong configuration have been neutralised, a follow-up process is  
718 initiated to analyse the reasons of the failure.

### 719 **1.6.13 Technical disconnection of a participant using abnormally the system** 720 **Description**

721 T2S Actors (excluding ICPs), accessing the T2S Platform through NSPs, are registered in the CGU.  
722 The CGU shall restrict access to the connectivity services only to the identified and authorised users.  
723 The registration process to the CGU is arranged via the NSP.

724 T2S has implemented a number of technical measures to avoid that abnormal behaviour of a T2S  
725 Actor (excluding ICP) in the technical infrastructure or application can hamper the stability of the  
726 system or have an impact on other users.

### 727 **Operational Procedure**

728 In the unlikely event that the measures referred above are not effective and there is evidence that the  
729 system’s integrity is at stake, the T2S Service Desk shall:

730 ▶ Contact the concerned T2S Actor (excluding ICPs), asking them to stop the abnormal behaviour  
731 without delay;

732 ▶ Verify, in cooperation with T2S Actor (excluding ICPs) and the NSP, if technical measures on  
733 T2S’ or NSP’s side are available to return to a normal situation;

734 ▶ Ask the NSP to withdraw the involved T2S Actor (excluding ICPs) from the CGU in case the  
735 threat to the stability of the platform with impact on other service users is still present and no  
736 other measures have been proven effective.

737 The T2S Coordinator is informed and a Settlement Managers’/ Crisis Managers’ conference call<sup>12</sup> is  
738 initiated prior to withdrawal of the CSD/ Central Bank or DCP.

739 The T2S Coordinator, in accordance with the Article 36 of the FA, will consult the Relevant  
740 Competent Authorities.

741 The NSP shall withdraw the T2S Actor(s) (excluding ICPs) from the CGU within one hour. The  
742 withdrawal can be requested for the U2A access, the A2A access, or both depending on the nature of  
743 the incident.

---

<sup>12</sup> Following the standard Incident and Crisis Management process.

744 The suspension from the CGU remains effective until the T2S Actor (excluding ICP) has declared to  
745 the T2S Service Desk that the threat no longer exists.

746 Upon the confirmation of the T2S Service Desk that the threat no longer exists, the reactivation or re-  
747 inclusion of the T2S Actor (excluding ICP) back to T2S CGU, in normal cases, can take up to two  
748 weeks.

749 This time can be shortened if the “emergency procedure” to re-join T2S CGU is opted at the level of  
750 the NSP (upon an additional fee). Such a procedure will be executed latest by the next business day  
751 after the request is submitted. The list of DNs/service(s) to be added needs to be provided to NSP by  
752 one of the Authorised Approvers at the T2S Operator.

### 753 **1.6.14 NCB-CSD Communication on DCA accounts**

#### 754 **Description**

755 In case a payment bank wants to create or close/delete a dedicated cash account it has to request this  
756 through the NCB.

#### 757 **Operational procedure**

758 The creation, closure and deletion of a DCA is performed by the responsible NCB. The NCB opens,  
759 closes and deletes DCA accounts on the request of payment banks.

760 The opening of DCA accounts is using a two-step approach:

- 761 ▶ The payment bank request the NCB to open the DCA;
- 762 ▶ Once the DCA has been opened the payment bank contacts its CSD(s) to complete the set up and  
763 perform the link of the DCA to securities account(s). The CSD(s) links the DCA to the securities  
764 account(s) in order to specify the cash account used for the settlement of the cash leg of  
765 transactions.

766 Should a payment bank wish to close/ delete a DCA, this is also done following a two-step process:

- 767 ▶ The payment bank request its CSD(s) to remove the link(s) between the DCA and the securities  
768 account(s);
- 769 ▶ Once all the link(s) have been removed the payment bank requests the NCB to close the DCA.  
770 Once the DCA has been closed it cannot be used anymore for cash settlements and liquidity  
771 transfers.
- 772 ▶ The DCA can be deleted by the NCB. Before the deletion of a DCA T2S performs an automatic  
773 check that no links to securities account(s) exist.



- 774 Payment banks will request the respective CSDs to create or remove the link(s) of the DCA to the  
775 securities account(s) when requesting the opening or closure/deletion of the DCA, consequently the  
776 CSD will be involved in the process and is made aware of created and closed/deleted DCA accounts.
- 777 In special situations such as the insolvency of a participant, where an NCB may decide to block a  
778 DCA, the NCB informs the CSD(s) using T2S broadcasts.

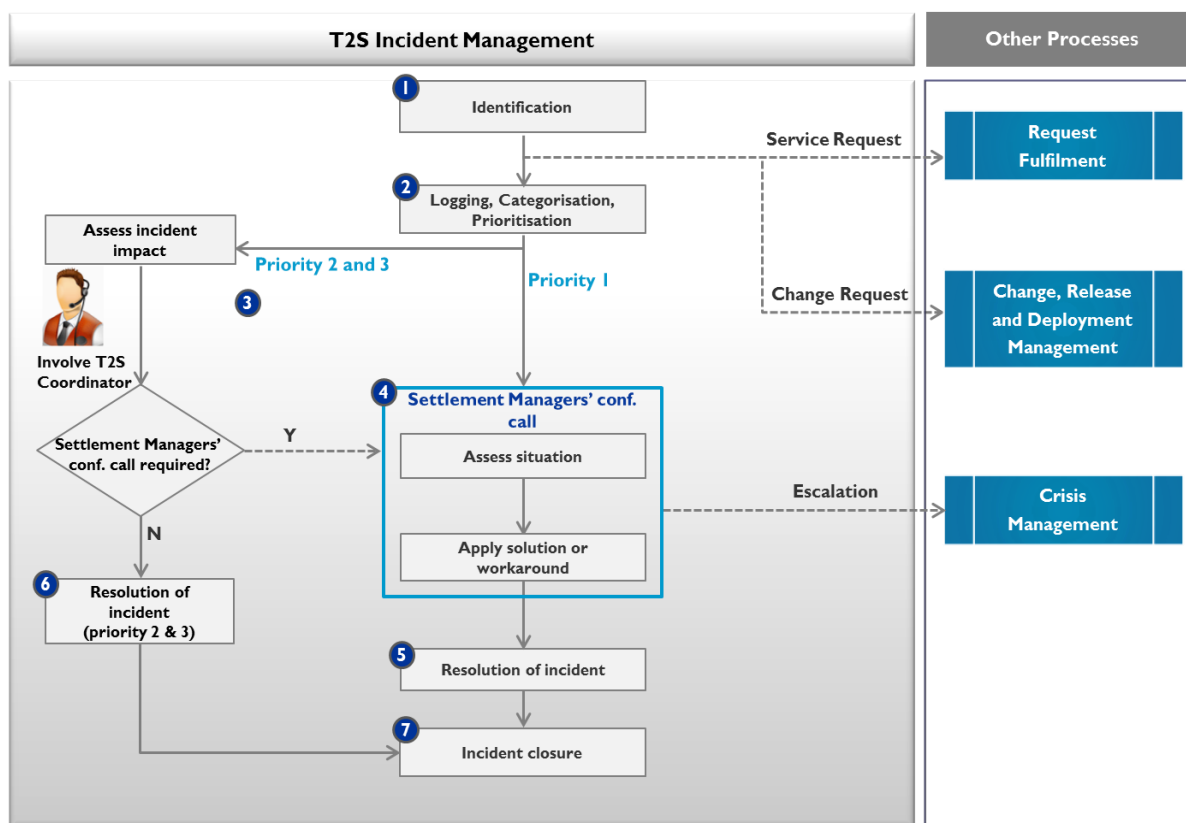
779 **2 INCIDENT MANAGEMENT**

780 **2.1 GENERAL INCIDENT MANAGEMENT PROCESS FLOW**

781 The general Incident Management process flow describes activities between the T2S Actors  
782 (excluding ICPs) and it is following the main principles of best practices. Some parts of this process  
783 flow are to be handled by the different T2S Actors. This is described in the respective tables, which  
784 refer to each of the steps.

785 The steps in the flow are numbered (1 to 7) in a sequence.

786 The incident scenarios 1-5 are based on the general Incident Management process flow, although only  
787 some of the steps are followed for each scenario. All steps are described per scenario allowing the  
788 usage of each of the scenarios on a stand-alone basis. The processes shown in *Figure 7* might have  
789 additional interfaces with other processes. In case a reported issue is identified as a Service Request or  
790 a Change Request, the relevant processes are triggered.



791

792 *Figure 7 - General Incident Management process flow*

793

Step	Description			
<p><b>1</b></p>	<p><b>Identification</b></p> <p>Incidents can occur at any level of the T2S Actors:</p> <ul style="list-style-type: none"> <li>◆ Scenario 1: Incident at the level of the T2S Platform (at 4CB as the T2S Operator);</li> <li>◆ Scenario 2: Incident at the level of TARGET2/ RTGS<sup>13</sup>;</li> <li>◆ Scenario 3: Incident at the level of one or more CSD(s);</li> <li>◆ Scenario 4: Incident at the level of DCPs or ICPs;</li> <li>◆ Scenario 5: Incident at the level of Network Service Providers (NSPs).</li> </ul> <p>Incidents are brought to the attention of the T2S Service Desk, preferably by phone, or by signed e-mail. Input is collected from T2S Actors (excluding ICPs) and from the TARGET2 Coordination Desk. The T2S incidents which are <u>communicated</u> to the T2S Service Desk might have been already categorised by the reporting T2S Actor (excluding ICPs). Therefore local/ national Service Desks shall align their procedures to ensure consistency with the MOP.</p> <p>The T2S Service Desk also identifies incidents by monitoring and using event management systems. The T2S Service Desk monitors the relevant IT systems as well as relevant non-IT information, e.g. the financial markets, which could have severe negative impact on the T2S Platform. Monitoring and event management are 4CB internal responsibilities and are not described in the MOP.</p> <p>If the reported issue is not an incident, it could e.g. be logged as a Service Request (SR) and is forwarded to the Request Fulfilment function (e.g. to establish a new T2S user) or, if it is a Change Request (CR), it is to be processed according to the Change, Release and Deployment Management process (e.g. if a new T2S feature is required), in the latter case the incident will be closed. If an issue is logged as a question or a SR, it will be automatically assigned a low priority (see FA/ CPA Schedule 6):</p> <hr/> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: left;">Priority 4</td> <td style="width: 33%; text-align: center;">Low</td> <td style="width: 33%; text-align: right;">Query or Service Request</td> </tr> </table> <hr/> <p>Some issues first require to be investigated in order to decide, if it is an incident or a Service Request (e.g. a call of a T2S user not being able to access a specific function, which might be caused by an application or network error, or by the users him/ herself (e.g. wrong credentials or wrong password, which triggers a SR).</p>	Priority 4	Low	Query or Service Request
Priority 4	Low	Query or Service Request		

<sup>13</sup> An incident identified at the level of a Central Bank is either related to TARGET2/RTGS (Scenario 2) or to a CMS failure for which the general incident handling process applies ().

Step	Description
<p><b>2</b></p>	<p><b>Logging, categorisation and prioritisation</b></p> <p>The categorisation and prioritisation is performed by the T2S Service Desk during logging of the incident. The steps preceding the logging may not be under the control of the T2S Service Desk but rather by the relevant T2S Actor (excluding ICPs), depending on the incident scenario.</p> <p>It is important to have any incident properly logged (and updated while handling), regardless whether it was raised first by a T2S Actor (excluding ICPs) or directly at the T2S Service Desk. The information provided enables a correct categorisation, prioritisation and handling. The information to be logged is shown as a list in the Annex (See <i>Annex, Section 5</i>).</p> <p>Once an incident is logged by creating a ticket in the Trouble Management System (TMS), the T2S Service Desk remains accountable for tracking it during the complete incident lifecycle until closing. The T2S Service Desk tracks, communicates and escalates as appropriate and only the T2S Service Desk closes the ticket, once incident is resolved as confirmed by the respective T2S Actor.</p> <p>At the level of the T2S Service Desk, the incident is then categorised. Categories are e.g. network, application, security, etc. and are drilled down in more detail. Within the T2S Service Desk organisation, the categorisation provides information to identify the same kind of issues and to later trigger other processes, e.g. Problem or Information Security Management. The prioritisation is done by the T2S Service Desk based on the agreed priority classes (see FA/CPA Schedule 6). The prioritisation scheme is applied, irrespective of which T2S Actor (excluding ICP) reports the incident.</p> <p>Queries or SRs (e.g. password reset procedure, adding users) may require a further differentiation of their priority in order to be handled with adequate timing. This is done by the Request Fulfilment process.</p>

Step	Description
<p><b>3</b></p>	<p><b>Activation of Settlement Managers’ conference call</b></p> <p><b>Priority 1 Incidents</b> mandatorily trigger the <b>Settlement Managers’ conference call</b>, whereas <b>priority 2 or 3 incidents</b> will not mandatorily trigger the Settlement Managers’ conference call.</p> <p>A T2S priority 1 incident can be of different nature, e.g. caused by the T2S application itself, its IT-infrastructure, but also a severe issue detected by the T2S Service Desk e.g. a disturbance in the financial markets or an issue occurring through the different information channels the T2S Service Desk is monitoring.</p> <p>The priority 2 and 3 incidents will be monitored closely by the T2S Service Desk for their impact and the timing of the resolution, in order to be ready for escalation, if required. The T2S Service Desk keeps the T2S Coordination function updated on the development. In case a priority 2 or 3 incident is expected to create a major or multilateral business impact, if not treated as an emergency, it can trigger a Settlement Managers’ conference call through a request to the T2S Coordinator or following an assessment by the T2S Service Desk and the T2S Coordinator. Furthermore, if the impact of the incident is higher than anticipated in the beginning, it will be possible to upgrade it to a higher priority for quicker resolution.</p>

Step	Description
4	<p><b>Settlement Managers' conference call and possible escalation to Crisis Managers</b></p> <p>The T2S Coordinator at the ECB will call for the Settlement Managers' conference call (either mandatorily for priority 1 incidents or after analysis for priority 2 and 3 incidents). The T2S Coordinator leads the Settlement Managers' conference call and is supported by the T2S Service Manager. The coordination role includes assessing and coordinating the overall situation and taking a system wide view meaning the T2S coordinator is accountable</p> <p>Throughout the life cycle of an incident, it needs to be ensured that all relevant parties are kept informed about the status and required action. Possible delays need to be identified as early as possible and escalation needs to be triggered, when required.</p> <p><b>In case the issue is not leading to a crisis as specified below, the T2S Settlement Managers could agree on a preliminary communication for the market. Afterwards the T2S Coordinator communicates the agreed message(s) to wider market participants (or market data users) using the T2S-Info system (which is used to post information via Reuters/Bloomberg pages) and on the T2S website.</b></p> <p>If the Settlement Managers consider that a Crisis might occur, or if external triggers provide such information or the Settlement Managers cannot agree on a way forward, then the Settlement Managers escalate the incident to the Crisis Managers.</p> <p>A Crisis Managers' conference call shall however be launched mandatorily if one of the following issues arise:</p> <ul style="list-style-type: none"> <li>◆ A delayed closing of T2S is requested;</li> <li>◆ An incident has the potential to delay the start of the next day's phases;</li> <li>◆ A long-lasting failure of T2S Platform with the potential to cause major financial markets impact;</li> <li>◆ An event outside T2S perimeter causing systemic risk;</li> <li>◆ Issues that arise and are not entirely covered by the MOP;<sup>14</sup></li> <li>◆ In cases the Settlement Managers deem it necessary to initiate the Crisis Managers' conference call.</li> </ul> <p>In addition, each Settlement Manager should inform his/ her respective Crisis manager in the event of an intra-region or inter-region failover.</p>

<sup>14</sup> Such issues will be reviewed when updating the MOP.

Step	Description
<p><b>5</b></p>	<p><b>Resolution of incident</b></p> <p>Solutions/ workarounds which shall be applied for different situations. The T2S Actors (excluding ICPs) should foresee the following activities: assignment of specialists, invocation of a technical team, investigation and analysis, resolution and recovery, and as applicable incident reports.</p> <p>If necessary, the resolution of Priority 1 incidents may be a parallel activity to the Settlement Managers' conference call and will be carried out at 4CB Level and/ or at the level of T2S Actors (excluding ICPs) to whom the incident is related to.</p> <p>The procedure triggers immediately the Problem Management process when applicable, in order to resolve the underlying root cause(s) as soon as possible. For this, detailed input of T2S Actors (excluding ICPs) may be required.</p>
<p><b>6</b></p>	<p><b>Resolution of Incidents (priority 2 and 3)</b></p> <p>Incidents are resolved at the level of the T2S Actor (excluding ICP) to whom the incident is related to (depending on the scenarios as described in the following sections).</p> <p>The resolution shall follow the good practice principles (as described by ITIL® V3) and consider all relevant steps, such as: initial diagnosis, functional and hierarchical escalation (which will be applied at each T2S Actor (excluding ICPs) internally as required), investigation and diagnosis, making use of a prefilled known error/ solution database, applying work-around while not to forget the permanent resolution (via Problem Management, see end of step 7).</p> <p>While these steps are carried out the T2S Service Desk will manage to keep all relevant information updated and available, track the status according to service levels of resolution times. Updates are provided through the relevant communication means. If a committed resolution time cannot be reached, the waiting requestor shall be informed pro-actively through the TMS. The requestor can call the T2S Service Desk or query the TMS for an update to an existing incident.</p> <p>The reprioritisation of a priority 2 or 3 incident might be necessary during its lifecycle, since at the initial stage the full picture of the impact might not be visible. Even an escalation as priority 1 incident is possible.</p>

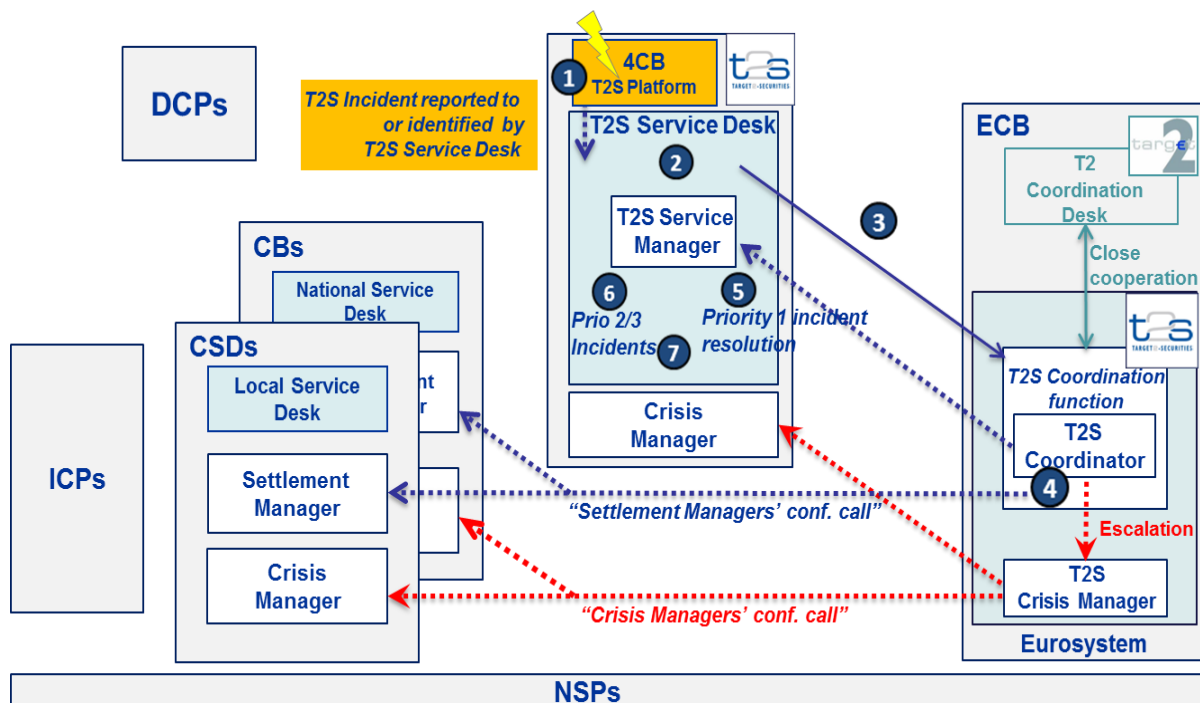
Step	Description
<b>7</b>	<p><b>Incident Closure</b></p> <p>Before the T2S Service Desk can close the ticket (incident), all required ticket-fields have to be updated by appropriate documentation. The T2S Service Desk has ownership and hence the exclusive rights to close a ticket which shall be done after communication with the ticket originator (i.e. relevant T2S Actor) to ensure the right resolution is in place and has been verified.</p> <p>However, if a work-around was applied but the underlying cause has not yet been solved, a problem ticket will be created if not existing problem within the framework of the Problem Management process.</p>

794



795 **2.2 SCENARIO 1: INCIDENT AT THE LEVEL OF THE T2S PLATFORM (AT 4CB AS**  
796 **T2S OPERATOR)**

797 **Overview**



798

799 *Figure 8 - Scenario 1 - Incident at the level of the T2S Platform (at 4CB as T2S Operator)*

800 **The Incident Management process flow - Scenario 1: Incident at the level of T2S Platform**

801 The individual Incident Management process flow for incidents at the level of the T2S Platform is  
802 described in below table. The steps 1 – 7 refer to the workflow as shown in *Figure 7, Section 2.1.*

803

Step	Scenario Description
<p><b>1</b></p>	<p><b>Identification</b></p> <p>A T2S incident happens at platform level and gets reported to or is identified by the T2S Service Desk.</p> <p>The detection of an incident is triggered by the following events: (i) monitoring by the T2S Service Desk or (ii) an issue raised by a T2S Actor (excluding ICP).</p> <p>As soon as an event is considered an incident (i.e. in some cases immediately, in other cases up to a maximum of 15 minutes after the triggering issue has been detected) the T2S Service Desk must – without further delay – inform the T2S Coordinator.</p>
<p><b>2</b></p>	<p><b>Logging:</b> Incident is logged by the T2S Service Desk.</p> <p><b>Categorisation:</b> Incident is categorised by the T2S Service Desk.</p> <p><b>Prioritisation:</b> The prioritisation is done based on the agreed priority classes (See step-2 of general Incident Management process flow by the T2S Service Desk).</p>
<p><b>3</b></p>	<p><b>Priority 1 incident?</b></p> <p>Incidents with a critical severity are handled as priority 1 incidents, and eventually escalated to the Crisis Management. Priority 1 incidents mandatorily trigger the Settlement Managers’ conference call.</p>
<p><b>4</b></p>	<p><b>Settlement Managers’ conference call</b></p> <p>During the Settlement Managers’ conference call, the T2S Service Desk will be invited to <b>report on the incident</b>, on the measures taken to address it, on the expected duration for resolution.</p> <p><b>If the Settlement Managers cannot agree on a measure or feel that the matter deserves to be escalated, the Crisis Managers’ conference call will be launched.</b> The Crisis Managers’ conference call should be held ideally ten minutes after a Crisis is declared. The Settlement Managers are responsible for informing their respective Crisis Managers of the forthcoming Crisis Managers’ conference call. After a Crisis Managers’ conference call a Settlement Managers’ conference call is held again in order to execute/debrief the decisions taken by the Crisis Managers..</p> <p>Given the dependencies between T2S and TARGET2/ RTGS systems, the T2S Coordinator has to mandatorily inform the TARGET2 Coordinator/ RTGS Operator at earliest possible, when such events occurs.</p>

Step	Scenario Description
<p><b>5</b></p>	<p><b>Priority 1 incident resolution</b></p> <p>In general this procedure follows the description as shown in step 5 of the general Incident Management process flow. Inside the 4CB organisation, the incident is worked on with highest priority (while incidents priority 2 or 3 are handled in the standard incident workflow; see point 6 below).</p>
<p><b>6</b></p>	<p><b>Resolution of incidents (priority 2 and 3)</b></p> <p>Incidents are resolved at the level of the 4CB. The T2S Coordination function and the T2S Service Desk may interact and coordinate with the T2S Actors (excluding ICPs) (e.g. for specific incidents). Functional and hierarchical escalation will be applied by each of the T2S Actors (excluding ICPs) internally as required. The T2S Service Desk shares the relevant information with the T2S Coordination function which, based on the available data, might decide to consider launching a Settlement Managers' conference call (see step 5 above).</p> <p>Reprioritisation of a priority 2 or priority 3 incident might be necessary during its lifecycle (see step-6 from general Incident Management process flow).</p>
<p><b>7</b></p>	<p><b>Incident closure</b></p> <p>A T2S incident shall only be closed, after confirmation from reporting party. In general step 7 of the <i>General incident management process flow (Section 2.1)</i> should be applied.</p>

805 **The RACI Matrix**

806 To ensure a clear understanding of who is performing what and to assign accountability and  
807 responsibility as agreed, for each incident scenario a RACI matrix is defined.

808 RACI means:

809 **R** – Responsible: correct execution of activities

810 **A** – Accountable: ownership of quality and end result activity

811 **C** – Consulted: involvement through input of knowledge and information

812 **I** – Informed: receiving information about execution and quality

813 In the above, Accountable is the highest responsibility, followed by Responsible, Consulted and  
814 finally Informed.

Incident Management

Scenario 1 : Incident related to Failure at the T2S Platform (4CB)												
Process Step(s)	Process Sub-Step(s)	Key Activities	CSD		CB		4CB			ECB		
			CSD Settlement Manager	CSD Crisis Manager	CB Settlement Manager	CB Crisis Manager	T2S Service Desk	T2S Service Manager	4CB Crisis Manager	T2S Coordinator	T2S Crisis Manager	T2 Coordinator
<b>Step 1</b> Identification			R		R		R	A				
<b>Step 2</b> Logging, Categorization, Prioritization			C		C		R	A				
<b>Step 3</b> Activation of Settlement Managers' conf. call								A/R		C		
<b>Step 4</b> Settlement Managers conf. call	4 a) Settlement Managers' conf. call	4.1 Requesting	R		R			R		A/R		
		4.2 Initiating	I		I			I		A/R		I
		4.3 Participating <i>(for agreement on a standard resolution)</i>	R		R			R		A/R		I
	4 b) Escalation to Crisis Managers'	4.1 Requesting	R		R			R		A/R		I
		4.2 Initiating				I			I		A/R	I
		4.3 Participating <i>(for taking a decision)</i>				R			R	C	A/R	C
<b>Step 5</b> Priority 1 incident resolution		5.1 Incident leading to Settlement Managers' conf. call*	R		R			R		A/R		I
<b>Step 6</b> Resolution of incident (Priority 2 & 3)		6.1 Incident leading to Settlement Managers' conf. call*	R		R			R		A/R		I
		6.2 Resolve low impact incident <i>(No Settlement Managers' conf. call)</i>	I		I		R	A		I		I
<b>Step 7</b> Incident Closure			C		C		R	A				

\* Refer steps from 4a) for conf. call Requesting and Initiating. This only reflects the participating and hence agreement on resolution.

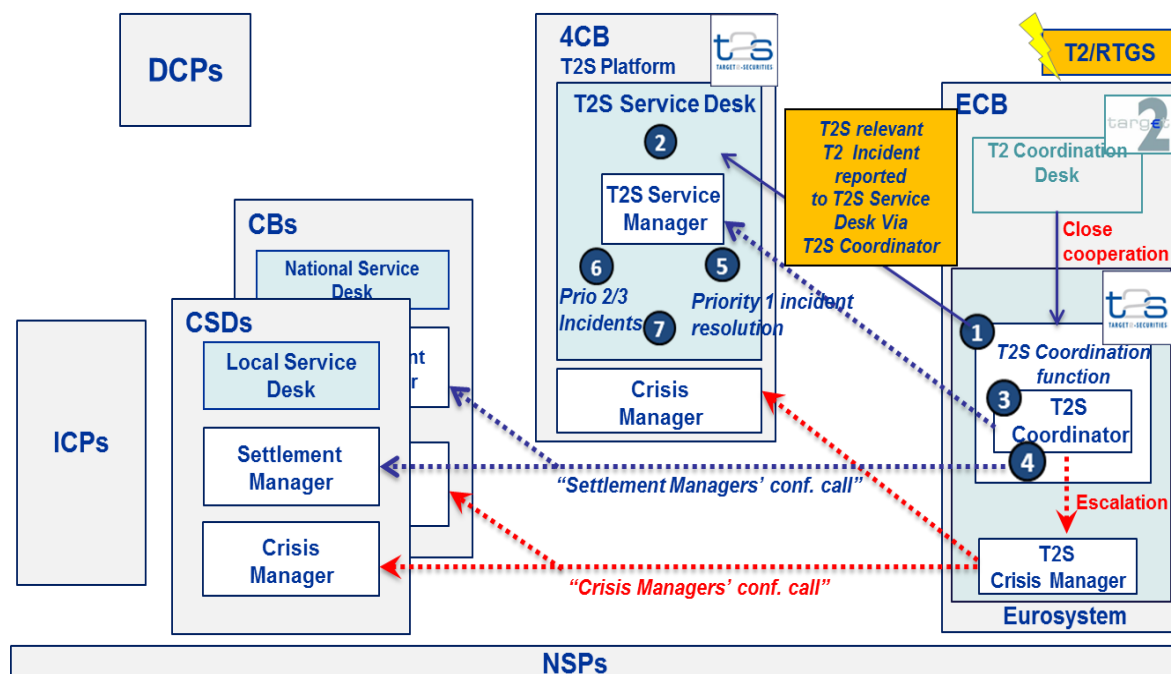
815

816

Table 4 - RACI matrix for scenario 1

Incident Management

817 2.3 SCENARIO 2: INCIDENT AT THE LEVEL OF TARGET2/ RTGS  
818 Overview



819

820 Figure 9 - Incident Management process flow - scenario 2: Incident at the level of TARGET2/RTGS

821 The individual Incident Management process flow for Incidents related to TARGET2/ RTGS is  
822 described in the table below. The steps 1 – 7 refer to the workflow as shown in Figure 7, Section 2.1.

Step	Scenario 2 description
1	<p><b>Identification</b></p> <p>If an event happens in TARGET2 or at RTGS system that may affect T2S, it shall be communicated by the relevant TARGET2 Coordinator/ RTGS Operator to the T2S Coordinator. Certain categories of incidents have to mandatorily trigger this information (see below: Events for escalation of TARGET2/RTGS Incidents).</p> <p>The TARGET2 Coordinator/ RTGS Operator informs the T2S Coordinator mandatorily when the following occur:</p> <ol style="list-style-type: none"> <li>1. Failure of the TARGET2/RTGS that could have an impact on T2S;</li> <li>1. Non-functioning of liquidity bridge between TARGET2/RTGS and T2S;</li> <li>2. There is a delayed closing or delayed opening of TARGET2/RTGS;</li> </ol> <p>The TARGET2 Coordinator/RTGS Operator shall inform the T2S Coordinator of an incident that could affect T2S as soon as possible.</p>

## Incident Management

Step	Scenario 2 description
<p>2</p>	<p><b>Logging:</b> Incidents are logged by the T2S Service Desk as reported by T2S Coordinator.</p> <p><b>Categorisation:</b> Incident is categorised by the T2S Service Desk as reported by the T2S Coordinator (eventually with preliminary categorisation as provided by TARGET2 Coordination Desk).</p> <p><b>Prioritisation:</b> The prioritisation is done by the T2S Service Desk based on information provided by TARGET2 Coordinator/ RTGS Operator and as per agreed priority classes (See step-2 of general Incident Management process flow).</p>
<p>3</p>	<p><b>Priority 1 Incident?</b></p> <p>Incidents with a critical severity are handled as priority 1 incidents and may eventually lead to a Crisis Management conference call. Priority 1 incidents mandatorily trigger the Settlement Managers' conference call.</p>
<p>4</p>	<p><b>Settlement Managers' conference call</b></p> <p>During the Settlement Managers' conference call, the TARGET2 Coordinator/ RTGS Operator will be invited to <b>report on the incident</b>, on the measures taken to address it, on the expected duration for resolution.</p> <p>The Settlement Managers cannot decide on issues which concern the cash side/ DCAs as such decisions are taken under the responsibility of TARGET2 Coordinator/ RTGS operator. TARGET2 conference calls at the level of Settlement and Crisis Managers can be held in parallel to the T2S calls. However, simultaneous conference calls should be avoided, if possible.</p> <p>If the <b>Settlement Managers cannot agree on a measure or feel that the matter deserves to be escalated, the Crisis Managers' conference call will be launched.</b> The Crisis Managers' conference call should be held ideally ten minutes after the crisis is declared. The Settlement Managers are responsible for informing their respective Crisis Managers of the forthcoming Crisis Managers' conference call. After a Crisis Managers' conference call a Settlement Managers' conference call is held again in order to execute the decisions taken by the Crisis Managers.</p>

**Incident Management**

Step	Scenario 2 description
<p><b>5</b></p>	<p><b>Priority 1 incident resolution</b> In general this procedure follows the description as shown in step 5 of the general Incident Management process flow.</p>
<p><b>6</b></p>	<p><b>Resolution of Incidents (priority 2 and 3)</b> Incidents are resolved at the level of the TARGET2 Actor (excluding ICP) where the incident occurred. The TARGET2 Coordination Desk, the T2S Coordination function and the T2S Service Desk may interact and align with the relevant parties. The T2S Coordination function shall provide a prefilled solution database (i.e. toolbox) on T2S related critical TARGET2 events, incl. act-upon rules and keep it updated.  The T2S Service Desk shares the relevant information with the T2S Coordination function which, based on the available data, might decide to launch a T2S Settlement Manager' conference call (see step 5 above).  Reprioritisation of a priority 2 or priority 3 incident might be necessary during its lifecycle (see step-6 from the general Incident Management process flow).</p>
<p><b>7</b></p>	<p><b>Incident Closure</b> A T2S Incident triggered by a TARGET2 incident can only be closed after TARGET2 closes its incident and when there is no more impact on T2S. In general step 7 of the general Incident Management process flow (<i>Section 2.1</i>) should be applied.</p>

823



Incident Management

Scenario 2 : incident related to TARGET2/RTGS

824	Process Step(s)	Process Sub-Step(s)	Key Activities	CSD		CB		4CB			ECB		
				CSD Settlement Manager	CSD Crisis Manager	CB Settlement Manager	CB Crisis Manager	T2S Service Desk	T2S Service Manager	4CB Crisis Manager	T2S Coordinator	T2S Crisis Manager	T2 Coordinator
825	<b>Step 1</b> Identification										I		A/R
826	<b>Step 2</b> Logging, Categorization, Prioritization			I		I		R	A				C
827	<b>Step 3</b> Activation of Settlement Managers' conf. call								A/R		C		
828	<b>Step 4</b> Settlement Managers conf. call	4 a) Settlement Managers' conf. call	4.1 Requesting	R		R			R		A/R		
829			4.2 Initiating	I		I			I		A/R		I
830			4.3 Participating (for agreement on a standard resolution)	R		R			R		A/R		C
831		4 b) Escalation to Crisis Managers'	4.1 Requesting	R		R			R		A/R		C
			4.2 Initiating			I		I		I		A/R	I
			4.3 Participating (for taking a decision)			R		R		R		C	A/R
832	<b>Step 5</b> Priority 1 incident resolution		5.1 Incident leading to Settlement Managers' conf. call*	C		C		R	A		C		
833	<b>Step 6</b> Resolution of incident (Priority 2 & 3)		6.1 Incident leading to Settlement Managers' conf. call*	R		R			R		A/R		I
834			6.2 Resolve low impact incident (No Settlement Managers' conf. call)	I		I		R	A		I		I
835	<b>Step 7</b> Incident Closure			I		I		R	A				C

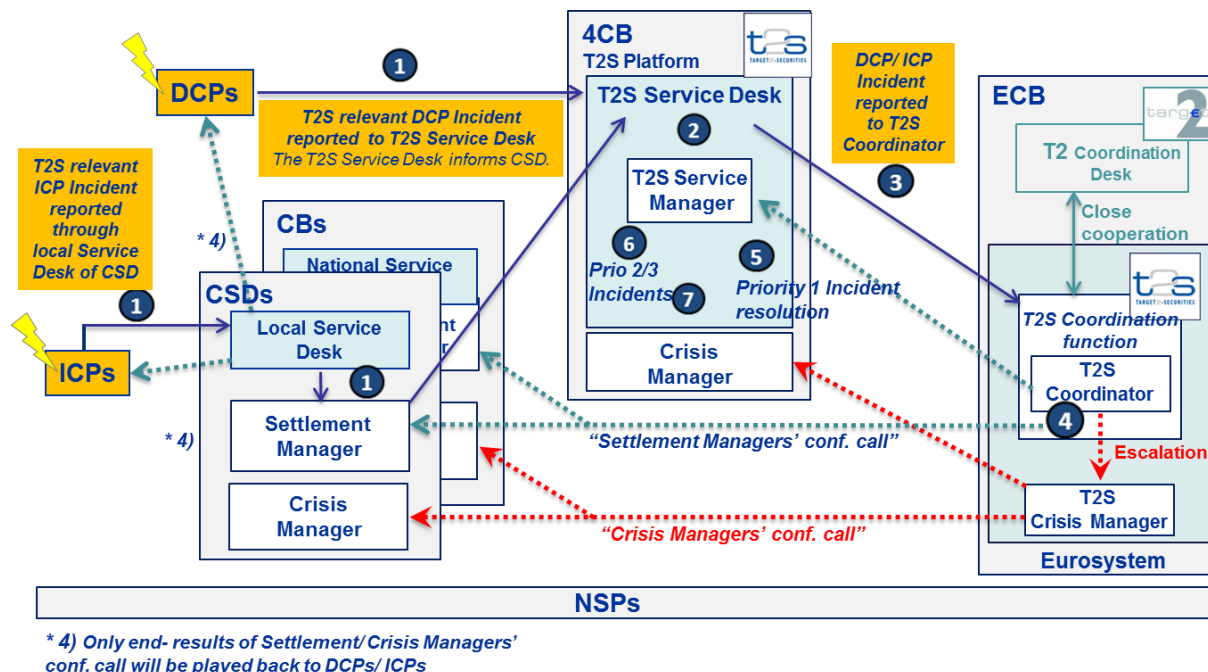
\* Refer steps from 4a) for conf. call Requesting and Initiating. This only reflects the participating and hence agreement on resolution.

Table 5 - RACI matrix for scenario 2

Incident Management

837 2.4 SCENARIO 4: INCIDENT AT THE LEVEL OF DCPs OR ICPS

838 Overview



839

840 Figure 10 - Incident Management process flow - scenario 4: Incident at the level of DCPs or ICPS

841 The individual Incident Management process flow for T2S relevant incidents at the level of DCPs and  
842 ICPS is described in the table below. The steps 1 – 7 refer to the workflow as shown in Figure 7,  
843 Section 2.1.

## Incident Management

Steps	Scenario 4 description
<p><b>1</b></p>	<p><b>Identification</b></p> <p>If a T2S relevant incident (except technical connections to T2S) happens at one or more of the DCPs, it is first reported to the local Service Desk (at the respective CSD or its National Central Bank). It shall be flagged as such and be communicated to the respective Settlement Manager, who will report this Incident to the T2S Service Desk.</p> <p>In case of incidents related to technical connections to T2S as defined in FA/ CPA Art. 12, DCPs directly report to the T2S Service Desk. The technical issues that are related to connectivity (e.g. unable to retrieve/ receive report from T2S, connection issues with T2S etc.).</p> <p>If a T2S relevant incident happens at one or more of the ICPs, it is first reported to the local Service Desk (at the respective CSD). It shall be flagged as such and be communicated to the CSD’s Settlement Manager, who will report this incident to the T2S Service Desk.</p> <p>The local Service Desk has to differentiate between incidents, Service Requests and Change Requests (CRs). The SRs and CRs to be forwarded to the T2S Service Desk as appropriate. However, if an incident is relevant for T2S, it shall be flagged as such and is reported to the Settlement Manager. The Settlement Manager would call the T2S Service Desk for reporting the incident.</p>
<p><b>2</b></p>	<p><b>Logging:</b> Incident is logged by the T2S Service Desk.</p> <p><b>Categorisation:</b> Incident is categorised by the T2S Service Desk based on information received from local Service Desk of DCP or their respective CSD/Central Bank Settlement Manager.</p> <p><b>Prioritisation:</b> The prioritisation is done by T2S Service Desk based on information provided by local Service Desk or their Settlement Manager reporting Incident on behalf of DCPs/ ICPs or local Service Desk of DCP (if directly reporting), as per agreed priority classes (See step-2 of the general Incident Management process flow).</p>

**Incident Management**

Steps	Scenario 4 description
<p><b>3</b></p>	<p><b>Priority 1 incident?</b></p> <p>If incident is Priority 1 then T2S Service Desk reports it to the T2S Coordinator.</p> <p>Incidents with a critical severity are handled as priority 1 incidents. The Priority 1 Incidents will trigger a Settlement Managers’ conference call and eventually the Crisis Management</p>
<p><b>4</b></p>	<p><b>Settlement Managers’ conference call and possible escalation to Crisis Managers</b></p> <p>The T2S Coordinator, if needed sets up a conference call between the CSDs’/ Central Banks’ Settlement Managers and the T2S Service Manager.</p> <p>During the Settlement Managers’ conference call, the Settlement Manager of the respective CSD/Central Bank, which reported the incident, will be invited to <b>report on the incident</b>, on the measures taken to address it and on the expected duration to resolution.</p> <p>If the <b>Settlement Managers cannot agree on a measure or feel that the matter deserves to be escalated, it is then escalated to the Crisis Managers, to launch a conference call.</b></p> <p>In case of need the respective DCP will be invited to the Crisis Managers conference call. The Crisis Managers’ conference call should be held ideally ten minutes after the Crisis is declared. The Settlement Managers are responsible for informing their respective Crisis Managers of the forthcoming Crisis Managers’ conference call. After a Crisis Managers’ conference call a Settlement Managers’ conference call is held in order to execute the decisions taken by the Crisis Managers</p>
<p><b>5</b></p>	<p><b>Priority 1 incident resolution</b></p> <p>The resolution of Priority 1 incidents may be triggered parallel with the Settlement Managers’ conference call.</p>

**Incident Management**

Steps	Scenario 4 description
<p><b>6</b></p>	<p><b>Resolution of incidents ( Priority 2 and 3)</b></p> <p>Incidents are resolved at the level of the T2S Actor (excluding ICP) where the incident occurred. At complex incidents the T2S Coordination function and the T2S Service Desk interact and align with the relevant parties. Functional and hierarchical escalation will be applied by each of the parties internally as required. The T2S Service Desk provides a prefilled known error/ solution database on T2S related critical events, including act-upon rules and to keep it updated.</p> <p>The T2S Service Desk shares the relevant information with the T2S Coordination function which, based on the available data, might decide to launch a T2S Settlement Managers’ conference call (see step 5 above).</p> <p>Reprioritisation of a priority 2 or priority 3 incident might be necessary during its lifecycle (see step-6 from General Incident Handling).</p>
<p><b>7</b></p>	<p><b>Incident closure</b></p> <p>The T2S Service Desk is in charge of closing the ticket for tracking purpose following confirmation by the reporting T2S Actor. In general step 7 of the <i>General incident management process flow (Section 2.1)</i> should be applied.</p>

844

Incident Management

845 **Case 1: DCPs/ ICPs report incident to T2S Service Desk via their CSDs**

846 Scenario 4 : INCIDENT AT THE LEVEL OF DCPS OR ICPS - Case 1 - DCPs/ ICPs report incident to T2S Service Desk via their CSDs

Process Step(s)	Process Sub-Step(s)	Key Activities	CSD		CB		T2S Service Desk	4CB		ECB		
			CSD Settlement Manager	CSD Crisis Manager	CB Settlement Manager	CB Crisis Manager		T2S Service Manager	4CB Crisis Manager	T2S Coordinator	T2S Crisis Manager	T2 Coordinator
847 <b>Step 1</b> Identification			A/R									
848 <b>Step 2</b> Logging, Categorization, Prioritization			C		I		R	A				
849 <b>Step 3</b> Activation of Settlement Managers' conf. call								A/R		C		
850 <b>Step 4</b> Settlement Managers conf. call	4 a) Settlement Managers' conf. call	4.1 Requesting	R		R			R		A/R		
		4.2 Initiating	I		I			I	I	A/R		I
		4.3 Participating (for agreement on a standard resolution)	R		R			R	R	A/R		I
	4 b) Escalation to Crisis Managers'	4.1 Requesting	R		R			R		A/R		I
		4.2 Initiating			I		I			I	A/R	I
		4.3 Participating (for taking a decision)			R		R			C	A/R	C
853 <b>Step 5</b> Priority 1 incident resolution		5.1 Incident leading to Settlement Managers' conf. call*	C		C		R	A		C		
854 <b>Step 6</b> Resolution of incident (Priority 2 & 3)		6.1 Incident leading to Settlement Managers' conf. call*	R		R			R		A/R		I
		6.2 Resolve low impact incident (No Settlement Managers' conf. call)	R		I		R	A		I		I
855 <b>Step 7</b> Incident Closure			C		I		R	A				

856 \* Refer steps from 4a) for conf. call Requesting and Initiating. This only reflects the participating and hence agreement on resolution.

857 Table 6 - RACI matrix for scenario 4, case 1

858

Incident Management

859

860 **Case 2: DCPs directly report incident to T2S Service Desk (related to technical connectivity to T2S)**

861

Scenario 4 : INCIDENT AT THE LEVEL OF DCPS OR ICPS Case 2 - DCPs directly report incident to T2S Service Desk (related to technical connectivity to T2S)													
Process Step(s)	Process Sub-Step(s)	Key Activities	CSD		CB		4CB			ECB			DCP
			CSD Settlement Manager	CSD Crisis Manager	CB Settlement Manager	CB Crisis Manager	T2S Service Desk	T2S Service Manager	4CB Crisis Manager	T2S Coordinator	T2S Crisis Manager	T2 Coordinator	Service Desk
Step 1 Identification													A/R
Step 2 Logging, Categorization, Prioritization			I		I		R	A					C
Step 3 Activation of Settlement Managers' conf. call								A/R		C			
Step 4 Settlement Managers conf. call	4 a) Settlement Managers' conf. call	4.1 Requesting	R		R			R		A/R			
		4.2 Initiating	I		I			I		A/R		I	I
		4.3 Participating (for agreement on a standard resolution)	R		R			R		A/R		I	I
	4 b) Escalation to Crisis Managers'	4.1 Requesting	R		R			R		A/R		I	I
		4.2 Initiating			I		I		I	I	A/R	I	I
		4.3 Participating (for taking a decision)			R		R		R	C	A/R	C	C
Step 5 Priority 1 incident resolution		5.1 Incident leading to Settlement Managers' conf. call*	C		C		R	A		C			
Step 6 Resolution of incident (Priority 2 & 3)		6.1 Incident leading to Settlement Managers' conf. call*	R		R		R			A/R		I	I
		6.2 Resolve low impact incident (No Settlement Managers' conf. call)	I		I	R	A			I		I	I
Step 7 Incident Closure			I		I	R	A						C

\* Refer steps from 4a) for conf. call Requesting and Initiating. This only reflects the participating and hence agreement on resolution.

872

Table 7 - RACI matrix for scenario 4, case 2

---

## Access Management

### 873 **3 ACCESS MANAGEMENT**

#### 874 **3.1 PREREQUISITES AND COMMON PRINCIPLES APPLIED TO ALL REQUESTS**

875 Prior to requesting access to T2S Services:

876 ▶ DiCoAs (excluding DCPs and ICPs ) need to exchange information with the T2S Operator in  
877 regard to their business needs, arrangements with NSP and other requirements, where relevant;

878 ▶ DCPs need to inform the CSD/ Central Bank of their intention to connect directly with T2S;

879 ▶ The T2S Operator sets up T2S Static Data for all CSDs/ Central Banks as DiCoA;

880 ▶ Each CSD/ Central Bank defines up to 3 authorised approvers to process DCP access requests;

881 ▶ Each CSD/ Central Bank defines potential reasons for rejecting DCP access requests;

882 ▶ The T2S Operator registers with each of the licensed NSP the list of authorised approvers and the  
883 list of potential rejection reasons;

884 DiCoAs can request U2A access for their internal end-users and A2A access for their applications.



## Access Management

### 885 3.2 REQUESTING ACCESS RIGHTS

#### 886 3.2.1 General pattern of DiCoA requests (common to DCP/ CSD/ NCB)

887 In order to get access to T2S Services, a DiCoA needs to follow the following steps to obtain:

- 888 ▶ Digital Certificates used for authentication and signing purposes;
- 889 ▶ The technical configuration of the NSP services;
- 890 ▶ The proper configuration of T2S Static Data (Parties, Securities and Accounts).

Step	Action
1	Select the NSP of choice and join the related services
2	Select the NSP's offer and related products
3	Subscribe to the NSP's Services for T2S (e.g. inclusion into the CGU)
4	Request for the NSP digital certificates
5	Connectivity setup with NSP
6	Create the Party in T2S Static Data according to the T2S registration procedure
7	Link the Party to the Network Service of choice in Static Data
8	Create the users, set up the related Certificate-DN links, and assign role/ privileges to them according to their functions
9	Set up statements and reports in Static Data
10	Connectivity test with T2S

891 *Table 8 - Steps for Granting T2S Access to DiCoAs*

#### 892 3.2.2 DCP Requests

---

##### Step 1 Select the NSP of choice and join the related services

---

- 893 ▶ Please see the NSP documentation and licence agreement.

894

---

##### Step 2 Select the NSP's offer and related products

---

- 895 ▶ Please see the NSP documentation and visit the NSP website.

896

---

##### Step 3 Subscribe to the NSP's Services for T2S (e.g. Inclusion into the CGU)

---

- 897 ▶ Via the VA-NSP website, select the appropriate scenario and the environment(s) for which access  
898 is requested. Please see the NSP documentation. Access can be requested to each of the licensed

## Access Management

899 NSP either for the T2S production environment for processing T2S Live Operations, or at once  
900 for all the relevant T2S test environments. Two registration scenarios are possible:

T2S Actor	CGU (2 scenarios)	Environment(s)
CSD/ Central Bank/ DCP	U2A only	Test
		Production
	U2A + A2A	Test
		Production

901 *Table 9 - Environments Available to T2S Actors*

- 902 ▶ This step requires the dual approval of the relevant CSD/ Central Bank and of the T2S Operator;
- 903 ▶ The requester is informed via e-mail of any change in the status of the request. If the request is  
904 rejected, the rejection cause is provided. If it is accepted, a final confirmation is provided to the  
905 requestor once the implementation date is defined;
- 906 ▶ If a DCP is customer of more than one CSD/ Central Banks this step must be performed only  
907 once. Upon request the T2S Service Desk can confirm to the CSD/ Central Bank if a DCP is  
908 already registered to the T2S Connectivity Services.

909

---

### Step 4 Request for the NSP digital certificates

---

- 910 ▶ The NSP Certificate Authority can issue certificates:
- 911 ♦ on USB token for the U2A access of end-users; or
- 912 ♦ on HSM for the A2A access of applications.

913 *Please see the NSP documentation.*

914

---

### Step 5 Connectivity setup with the NSP

---

- 915 ▶ On the implementation date, the NSP performs service provisioning activities according to the  
916 request form, after which a final confirmation is sent to the requester.

917

---

### Step 6 Create the Party in T2S Static Data according to the T2S registration procedure

---

- 918 ▶ If the party is a CSD Participant or external CSD, the relevant CSD is responsible for this step;
- 919 ▶ If the party is DCA holder or Payment Bank, the relevant Central Bank is responsible for this  
920 step;

---

## Access Management

- 921 ▶ Please see the T2S Registration Guide and UHB V2.0 *Section 3.8 “Party Management”*;
- 922 ▶ Please also see *UDFS V2.0 Sections 1.2 “Configuration of Parties, Securities and Accounts” and*  
923 *1.3 “Access to T2S”* the party is a CSD Participant or External CSD, the relevant CSD is  
924 responsible for this step.

925

---

### Step 7 Link the Party to the Network Service of choice in Static Data

---

- 926 ▶ Please see the UHB V2.0 Sections 3.8.1 “Administration of Participants” and 3.17.1  
927 “Configuration of a Technical Address” to configure one or more technical addresses and create  
928 technical address service links.

929

---

### Step 8 Create the users, set up the related Certificate-DN links, and assign role/ privileges to them according to their functions

---

- 930 ▶ Only registered users have access to the T2S GUI, therefore registration in T2S reference data and  
931 to the network is necessary prior to the first GUI access;
- 932 ▶ Please see UHB V2.0 Section 3.2 “Access Rights”. See also *UDFS V2.0 Sections 1.2*  
933 *“Configuration of Parties, Securities and Accounts” and 1.3 “Access to T2S”*;
- 934 ▶ In order to create the users, set up the related certificate-DN links, please see the UHB V2.0  
935 Section 3.2.4 “Configuration of a User” and follow the procedure described in the T2S  
936 Connectivity Guide Section 4.3 “Setting up Parties and Users”;
- 937 ▶ In order to assign roles and privileges according to the parties’ and users’ functions, please see the  
938 UHB V2.0 Sections 3.2.1.3 “Assign a Role to a User” and 3.2.1.4 “Assign a Role to a Party”.

939

---

### Step 9 Set up statements and reports in Static Data

---

- 940 ▶ Please see UHB V2.0 Sections 3.7 “Cash and Settlement Monitoring” and 3.9 “Report”.

941

---

### Step 10 Connectivity test with T2S

---

- 942 Please see User Testing documentation and to the T2S Connectivity Guide.

---

## Access Management

943 **3.3 REQUESTING CHANGES TO EXISTING ACCESS RIGHTS**

944 The change of the existing access rights follows in general the same steps envisaged for the initial  
945 registration. For details please see the T2S Registration Guide and the NSP documentation.

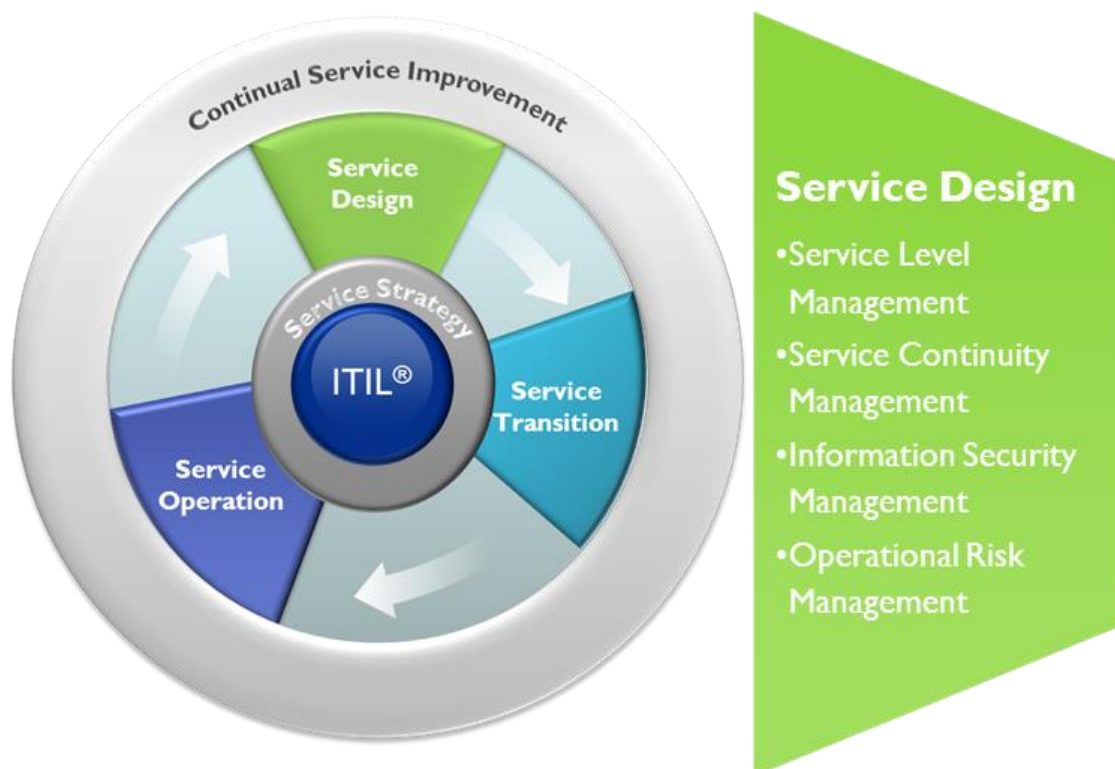
946 **3.4 REQUESTING REMOVAL OF EXISTING ACCESS RIGHTS**

947 The removal of the existing access rights follows in general the same steps envisaged for the initial  
948 registration. For details please see the T2S Registration Guide and the NSP documentation.

949 **3.5 SUPPORTING THE PROCESS**

950 Further information as well as electronic workflows is available on the websites of the NSP, the  
951 CSDs, NCB, ECB/ T2S and or via the GUI.

952



## 953 **4 SERVICE CONTINUITY MANAGEMENT**

### 954 **4.1 PURPOSE AND SCOPE OF SERVICE CONTINUITY MANAGEMENT**

955 According to the FA/ CPA, the terms “business continuity” and “disaster recovery” mean the set of  
956 rules and procedures aimed at resuming normal T2S Services in compliance with the Service Levels  
957 as described in FA Schedule 6 (T2S Service Level Agreement), after the occurrence of an incident  
958 which triggers a Crisis or disaster, as well as at mitigating the impact of such an incident.

959 In terms of ITIL® V3, Business Continuity Management (BCM) deals with the analysis, mitigation  
960 and prevention of risks, which may lead to an interruption in the business process regardless of what  
961 root-cause (e.g. non-IT issues as earth quakes, or IT-related service breakdowns).

962 BCM aims to reduce the probability of down-time risks of critical business processes to an acceptable  
963 level and to devise measures to ensure that business processes can be resumed within a previously  
964 determined period of time and scope. The Service Continuity Management (SCM) is a component of  
965 the BCM process and focuses on restoring and protecting the required services (in this case: T2S  
966 Services).

967 BCM and SCM would be expected to generate a policy and strategy in order to define the Vital  
968 Business Functions (VBFs) of the entire relevant organization (in this case: the Eurosystem). While  
969 BCM is a holistic management process of the Eurosystem which goes beyond T2S, the real SCM  
970 tasks, which focus on the T2S Services, are provided by the 4CB.

971 The Service Continuity Management assures that T2S Services Provider (4CB) undertakes all means  
972 to implement and maintain service assets that will provide the agreed level of contingency and  
973 recovery. The T2S Services have to be supported through major failures or disruptive events in order  
974 to return to normal operations after a Crisis event, (a situation that is affecting a large metropolitan or  
975 geographic area and the adjacent communities that are economically integrated with it). The nature of  
976 the Crisis event may be of “non-IT origin” or of “IT origin”, still in both cases the IT services most  
977 probably will be impacted, because in the event of a Crisis the complete operational and  
978 organizational set-up will follow an emergency plan for a certain applicable Crisis scenario.

979 Specialised systems and processes within the organisation of the Service Provider (4CB) will kick in  
980 to ensure that the service levels do not fall below the levels defined in the FA/ CPA. Continuity is  
981 assured primarily through redundancy and providing alternative resources that are dedicated to  
982 delivering services during contingencies and that are not impacted by the original event.

983 T2S SCM falls under the primary responsibility of the T2S Service Provider (4CB). Therefore the  
984 following Sections and paragraphs provide only the customer relevant description of the processes  
985 and are focused on describing the interfacing operations with the T2S Actors (excluding ICPs).

#### 986 **4.2 BCM AND SCM PRINCIPLES AS REFERRED TO IN THE FA/ CPA AND** 987 **RELATED DOCUMENTS**

988 The principles for the BCM and SCM for T2S can be found in the FA, the CPA and related  
989 documents.

990 ▶ In the FA/ CPA Schedule 5 (Service Description) some descriptions of the services for BCM,  
991 disaster recovery and Crisis Management services are provided;

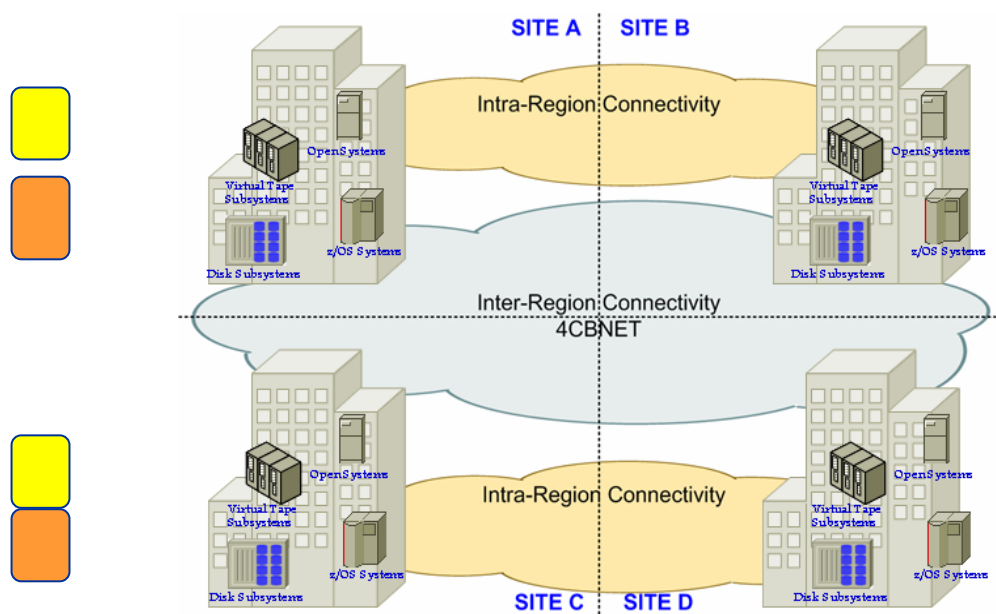
992 ▶ In the FA/ CPA Schedule 6 (Service Level Agreement) the mutual obligations between the  
993 Eurosystem and the CSDs/ Central Banks with respect to such services are defined together with  
994 the indication of the relevant Key Performance Indicators;

995 ▶ In the FA/ CPA Schedule 10 (Information Security), BCM refers explicitly to a wide scope which  
996 is much broader than SCM. This should be considered in an own BCM process (Annex 2 Security  
997 requirements and controls Ch. 13). More specifically, Ch. 11.6 of the Schedule 10 of Annex 2  
998 (Security Requirements and Controls) describes the Technical Vulnerability Management. This  
999 aims to reduce risks resulting from exploitation on technical vulnerabilities and must be  
1000 implemented in an effective, systematic and repeatable way with measurements taken to confirm  
1001 its effectiveness. These considerations must include operating systems, and any other applications  
1002 in use. This task is very strongly intertwined with Security, SCM and Risk Management  
1003 requirements and should be considered together in a common approach and risk and threats.

1004 More details on the technical implementation of the principles defined in the FA/ CPA are illustrated  
1005 in the document T2S General Technical Specifications. Additionally the non-functional test  
1006 documentation defines how the T2S Services are to be verified and accepted (during the project phase  
1007 and for subsequent releases).

#### 1008 **4.3 T2S SERVICE CONTINUITY**

1009 Like in TARGET2, the architecture of the T2S core system is based on the concept of “2 regions/ 4  
1010 sites”. The four sites are fully equivalent and each of them is equipped with the same technical  
1011 resources: processor, storage, network interface, software, etc. The two sites in each region are located  
1012 at a distance that is sufficient to have a distinct risk profile. The two regions are located at  
1013 geographical distance of several hundreds of kilometres.



1014

1015

*Figure 11 - T2S service continuity*

1016 The service continuity design involves different levels of the overall architecture requiring various  
 1017 technical solutions. A detail description of the technical solution can be found in the document T2S  
 1018 General Technical Specifications v2.2.0.

1019 The service continuity design for the region hosting the Long Term Statistic and Archiving services is  
 1020 based on the one-region/ two sites model due to the lower availability requirements.

1021 **4.3.1 Major Failure**

1022 Each region has the capability of a local recovery; the two sites in each region are located at a distance  
 1023 of a few kilometres from each other. The recovery within a region is assured by Synchronous Remote  
 1024 Copy (SRC) activated on the whole environment between the two sites of the same region. The SRC  
 1025 guarantees real time data updates in both sites; i.e. each write operation is completed only when both  
 1026 sites are updated. Major failure or disaster is meant to indicate a serious service interruption which is  
 1027 solved by relocation of T2S operations to a second site (intra-region failover), physically separate  
 1028 from the primary site. As a synchronous mode is applied, the databases at both sites are exactly the  
 1029 same, and no reconciliation is required after a failover.

1030 An intra-region failover can be conducted by the 4CB if they decide so following an appropriate  
 1031 technical assessment. Both the problem identified and its envisaged solution must be reported to the  
 1032 T2S Coordinator as a priority 1 incident, and will follow standard Incident and Crisis Management  
 1033 process.

1034





1035

1036

*Figure 12 - Communication flow during Crisis: initiating Crisis Managers' conference call*

1037

An intra-region failover ensures the continuation of normal business within a maximum of one hour.

1038

The processing is interrupted during the failover, but the T2S Actors are encouraged to keep on

1039

sending messages/ files, which will be queued, to the T2S System and processed when the System

1040

restart. The GUI interface is unavailable during the recovery.

1041

The activation of the intra-region recovery on the TARGET2 System will cause the unavailability of

1042

the T2S test environments, resuming will be done on a best effort basis.

1043

### **4.3.2 Regional Disaster**

1044

Recovery from a regional disaster is based on the presence of an alternate region located at a long

1045

distance away from the primary one (hundreds of kilometres). Due to the long distance, the recovery

1046

from one region to the other is only possible by Asynchronous Remote Copy (ARC), activated on the

1047

whole environment. The ARC cannot guarantee real time updates in both regions. As write operations

1048

in the remote region are asynchronous, it is possible that some data updates are lost if a regional

1049

disaster occurs. The amount of lost updates depends on the workload. The databases in the two

1050

regions show the processing status with a time discrepancy of a maximum of two minutes.

1051

The recourse to inter-region recovery may be triggered by a number of events, including a wide-area

1052

disaster having a high impact on the region operating T2S; to be effective even in a worst-case

1053

scenario, the plan for recovering the operating region avoids any dependency (decisional, personnel,

1054

technical, etc.) from that region; i.e. the alternate region is able to take over the operation without

1055

relying at all on the impacted region.

1056

If both sites within Region 1 become unavailable at the same time or if the asynchronous copy facility

1057

has problems, then, a loss of data would occur. In such a situation, there is no alternative but anyway

1058

failing over to Region 2 and reconciling the missing traffic. Still the resumption of the business in

1059

Region 2 should be enabled within two hours in Region 1, excluding the time between informing

1060

service users and the service users' response, i.e. the time they need to reconcile the lost data.

1061

Should the type of incident (e.g. in case of the so-called rolling disaster) allow an orderly and

1062

progressive external connections closure so to complete smoothly the asynchronous copy towards

1063 Region 2, the inter-region failover and the resumption of operations in Region 2 would result in no  
 1064 loss of data and it will be done within two hours, in line with the SLA commitment<sup>15</sup>.

1065 Not just processing, even access to GUI may also be interrupted during a failover. The users should  
 1066 not send new traffic to the system during a failover.

1067 Given the severe circumstances leading to an inter-region failover, both the Settlement and Crisis  
 1068 Managers will be kept informed all through the process, and accompanying conference calls will be  
 1069 held. More precisely, communication in the event of an inter-region failover is as follows:

- 1070 ▶ Regular reporting of the incident from detection onwards to the T2S Coordination function  
 1071 with a Settlement Managers’ conference call and subsequent a Crisis Managers’ conference call;
- 1072 ▶ After the successful failover a Crisis Managers’ conference call is held to discuss next steps or  
 1073 approve the opening of the system for normal processing; afterwards there is a Settlement  
 1074 Managers’ conference call to execute decisions taken by the Crisis Managers.



1075

1076 *Figure 13 - Communication flow during Crisis: initiating Crisis Managers’ conference call*

1077 The activation of the intra-region recovery on the TARGET2 System could cause the unavailability of  
 1078 the T2S test environments, resuming will be done on a best effort basis.

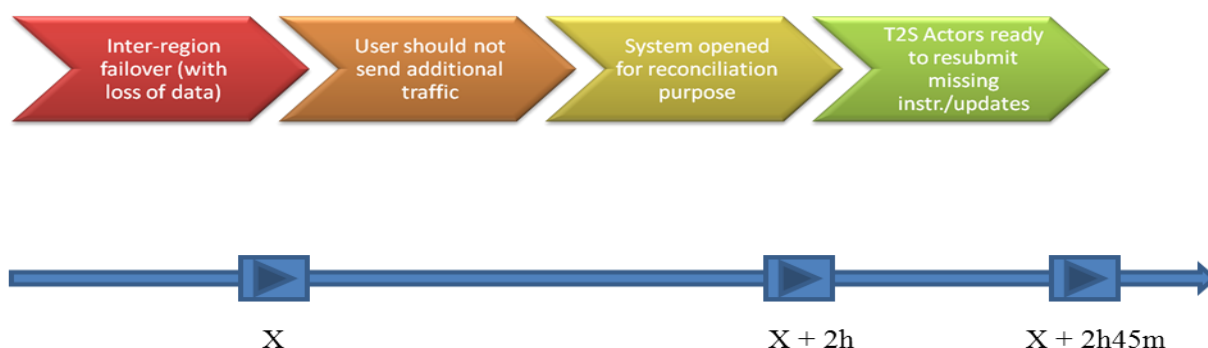
1079

---

<sup>15</sup> As from the FA/ CPA Schedule 6, Ch. 4.1.1.4) “the time between informing the service users and the service users response time is excluded from the recovery time. As is the time needed for reconciliation of lost data.”

1080 **4.3.3 Rebuilding Process**

1081 In case of regional disaster with loss of data, the rebuilding process is conducted by the T2S Actors  
 1082 (excluding ICPs) that have submitted instructions via every channel in the last 10 minutes before the  
 1083 consistency point with the support of the T2S Service Desk. Even if the triggering event falls clearly  
 1084 under the responsibility of the Crisis Managers, the steps related to the rebuilding process are  
 1085 conducted within the Settlement Managers’ forum. More information on the reconciliation by the  
 1086 CSDs, Central Banks and their respective DCPs for settlement instructions and/ or liquidity transfers  
 1087 is detailed in Annex (*Section 18 - Reconciliation for Restart After Disaster*).



Where ‘X’ is the point in time that -T2S is no longer available due to inter-region failover with loss of data

1088

1089 *Figure 14- Rebuilding after Crisis*

1090 When the fail-over activities on the 4CB side have been completed, the T2S Service Desk informs the  
 1091 T2S Coordination function at the ECB via phone. Such communication “stops the clock” as regards  
 1092 the RTO (Recovery Time Objective), which has to be less than 120 minutes as envisaged in the FA  
 1093 (Schedule 6, paragraph 4.2.1).

- 1094 1. The system is opened for the purpose of reconciliation only, meaning that it will not be possible  
 1095 to send new instructions in A2A mode (technically enforced) and the users have to avoid to  
 1096 send new instructions in U2A mode (not technically enforced);<sup>16</sup>
- 1097 2. To avoid receiving new instructions via U2A mode, the CSDs/ Central Banks will  
 1098 communicate and instruct their respective T2S GUI users (using U2A mode for sending  
 1099 instructions to T2S) to not use the T2S GUI to submit new instructions;

---

<sup>16</sup> The OMG has issued a Change Request (CR446) that aims at technically enforcing that no new U2A instructions can be submitted.

1100 3. They can start the verification process using the standard query tools (both in U2A and in  
1101 A2A);

1102 4. The next cut-offs are put forward of 12 hours to prevent their unwished triggering.

1103 The ICPs will be informed after the conference call by the relevant CSD/ Central Bank.

1104 The underlying rationale of point 1) is the clear need that the post fail-over status quo does not have to  
1105 be polluted. To ensure that only those instructions previously settled or still unsettled in Region 1 are  
1106 in the same status in Region 2, the T2S Actors (excluding ICPs) can send “hold” instructions to  
1107 prevent some instructions to be settled according to its evidences. Afterwards a release instruction per  
1108 settlement instruction is needed by the T2S Actors (excluding ICPs). The Central Banks and Payment/  
1109 Settlement Banks are also responsible to verify the coherence of the auto-collateralisation related data.

1110 The reconciliation process will last 45 minutes (to be confirmed after the results of the first testing  
1111 activities). After this time frame, another Crisis Managers' conference call is held, where  
1112 CSDs/Central Banks are invited to confirm that all T2S Actors finished their evaluation and that they  
1113 are ready to resubmit the missing instructions/ updates. Should anyone need more time, the Settlement  
1114 Managers could escalate to the Crisis Managers if such further delay impacts dangerously the  
1115 following phases.

1116 Once the confirmation that everyone is in a position to submit the possibly missing instructions given,  
1117 the system is reopened in full mode, i.e. including instructions and updates processing. In  
1118 resubmitting instructions the T2S Actors (excluding ICPs) have to ensure, to the maximum possible  
1119 extent, that this is done using the same business reference as before (in Region 1) but not the same  
1120 network reference. This would allow the standard double-entry check at T2S central system level to  
1121 properly discriminate possible duplicated messages and to consequently avoid double bookings/  
1122 updates. Same concept applies for possibly missing liquidity transfers from T2S where the standard  
1123 resending functionality available via GUI (refer UHB V2.0 paragraph 3.3.2.1) has to be used.<sup>17</sup> When  
1124 the internal evidences of all impacted T2S Actors (excluding ICPs) have been re-established as they  
1125 were in Region 1, the system can be again used for normal operations. As envisaged in the Schedule 6  
1126 of the FA, this needs a Crisis Managers' conference call to be held. During such conference the Crisis  
1127 is declared closed (if no other uncertain elements remain). The following Settlement Managers'  
1128 conference call agrees that the normal cut-offs schedule are restored.

1129

---

<sup>17</sup> TARGET2 Coordinator will liaise with the TARGET2 Service Desk to ensure that TARGET2 will wait to ensure that Liquidity Transfers can be resubmitted.

## 1130 **4.4 SERVICE CONTINUITY TESTING**

1131 This Section provides understanding of the key elements constituting the service continuity  
1132 procedures in T2S.

1133 The T2S Actors (excluding ICPs) (except for the DCPs connected to T2S only via U2A) are subject to  
1134 service continuity testing procedures.

1135 For the tests to be effective, they are either performed in the production environment or, where this is  
1136 not considered appropriate due to the additional operational risk, in a test environment as similar as  
1137 possible to the production environment.

1138 Although statistical and archiving services are a component of T2S, they are not core business  
1139 functionalities for this reason they will be performed by the T2S service provider (4CB) without the  
1140 involvement of CSDs/Central Banks.

1141 The testing of the business continuity procedures of the NSPs do not fall within the scope of the MOP  
1142 and their testing requirements are described in the NSP User Documentation.

### 1143 **4.4.1 Objective of Testing**

1144 Service continuity measures aim to ensure that failures of T2S components at any level do not cause a  
1145 disruption to the overall functioning of the system.

1146 All T2S users need to first rely on their own backup measures. T2S offers only limited contingency  
1147 arrangements to overcome interruptions happening at the side of the T2S Actors (excluding ICPs) in  
1148 the connection with the T2S System, aiming at processing a limited number of transactions.

### 1149 **4.4.2 Roles and Responsibilities**

1150 The T2S Service Desk assists in the testing and verification programmes of T2S. This includes  
1151 internal, Eurosystem acceptance and user testing.

1152 The CSDs are expected to organise the tests alongside with their respective DCPs. They will be  
1153 expected to prepare test schedules, collect test reports<sup>18</sup> from their participants and send the reports to  
1154 the T2S Coordinator.

1155 The T2S Coordinator will facilitate the organisation, whenever needed, and collect the reports from  
1156 all CSDs/ Central Banks and the T2S Service Desk. Based on the information received the T2S  
1157 Coordinator will prepare an overall test report summarising the outcome of the tests and submit the  
1158 same to the OMG.

---

<sup>18</sup> The format of the report would be simple and will be specified separately.

1159 **4.4.3 Frequency and Planning**

1160 Each of the three types of the T2S System service continuity test (see Section 10.4.6) is performed  
1161 twice per year (see FA/ CPA Schedule 10, Annex 2) between two annual regional rotations.

1162 The frequency of service continuity testing of the CSDs and their DCPs is decided by the Relevant  
1163 Competent Authorities.

1164 The T2S Service Desk provides the CSDs/Central Banks and the T2S Coordinator with a set of  
1165 weekends where the T2S production environment and the 4CB support can be made available upon  
1166 request. These dates need to be announced well in advance, together with the full calendar of the  
1167 service continuity tests, including back up dates for test repetition, presented to the OMG on a yearly  
1168 basis, normally at the occasion of the first OMG meeting/ conference call of the year.

1169 It is expected that the CSDs/Central Banks organising the tests provide the T2S Coordinator with a  
1170 test calendar with an overview of the scheduled activities for the next six months. This overview  
1171 needs to be submitted in principle by 31st December and by 30th June. The T2S Coordinator provides  
1172 a general overview to all CSDs/Central Banks and the T2S Service Desk.

1173 **4.4.4 Test Results and Reporting**

1174 Test results should be classified as either successful or unsuccessful. When the test objectives are not  
1175 met, the test result should be seen as unsuccessful. For unsuccessful tests a repetition of the test is  
1176 expected to be performed within 3 months.

1177 The test results are reported to the T2S Coordinator within 1 month following the last planned test  
1178 activity. For tests where DCPs are involved CSDs/Central Banks are expected to collect and  
1179 summarise their reports and forward the summary to the T2S Coordinator. The T2S Coordinator will  
1180 provide comprehensive reporting form for this end. The T2S Coordinator will prepare a report  
1181 summarising the outcome of the tests and any deviations to the agreed plan and submit it to the OMG  
1182 on a half-yearly basis. The summary will cover the test activities performed as well as the test results  
1183 and any follow-up items identified in previous periods.

1184 **4.4.5 CSDs'/ Central Banks'/ DCPs' Service Continuity Test**

1185 T2S offers to CSDs, Central Banks and their DCPs two weekends each year to support their service  
1186 continuity testing. The OMG defines on a rolling two year basis in the OMG Release Calendar, which  
1187 weekends are available for CSD/CB service continuity testing. Such tests will be conducted in the  
1188 T2S production environment during the weekends (normally on Saturdays).

1189 Since also TARGET2 is open on two weekends each year in the production environment to allow  
1190 TARGET2 participants to validate the effectiveness of their service continuity arrangements, these

1191 two weekends coincide, i.e. T2S and TARGET2 are open on the same day/during the same time if  
1192 needed. In the event the OMG recognises the need to have both T2S and TARGET2 open on other  
1193 weekends, the OMG will send a request to the 4CB which will assess this request and cooperate with  
1194 the relevant TARGET2 Governance bodies. The request for making the two platforms jointly  
1195 available on those additional weekends for such validation has to be made by the beginning of a  
1196 calendar year excluding the first two months of this particular calendar year.

1197 The participants need to align the validation of their service continuity arrangements on one of those  
1198 planned weekends. CSDs', Central Banks' and DCPs need to share their validation requirements  
1199 (duration, schedule, etc.) with T2S Service Desk and T2S Coordinator three (3) months in advance for  
1200 ensuring efficient planning and support. The T2S Service Desk will prepare a consolidated schedule  
1201 based on the input from individual CSDs and CBs that will participate in the service continuity  
1202 validation on the agreed weekend. The consolidated schedule will show who will be interacting when  
1203 with T2S (and TARGET2, if applicable) during the agreed service continuity validation window. The  
1204 OMG must approve this consolidated schedule for the entire service continuity validation window two  
1205 (2) months in advance. The CSDs', Central Banks' and DCPs have to report on their completion.

#### 1206 **4.4.6 T2S Service Continuity Test**

1207 The service continuity comprises the procedures and infrastructures to allow the T2S, in the event a  
1208 failure or disaster, to failover to the backup site within the same region or to one in the second region.

1209 The scenarios required to be tested are:

- 1210 1. Intra-regional failover;
- 1211 2. Inter-regional failover with no loss of data;
- 1212 3. Restart After Disaster (RAD) test, covering the inter-regional failover with loss of data  
1213 scenario.

1214 The scenarios 1 and 2 are run in the T2S production environment during week-ends and settlement  
1215 can be tested as well.

1216 The scenario 3 is always executed in the pre-production environment during the normal T2S  
1217 settlement days and hours. The T2S Service Desk simulates the system crash and the resuming on the  
1218 other region with loss of data by:

- 1219 ► Stopping some communication components at the central system level; Asking T2S Actors  
1220 (excluding ICPs) volunteering for the RAD session to submit some instructions (e.g. DVP, FOP,  
1221 liquidity transfers);
- 1222 ► Closing the system to the T2S Actors (excluding ICPs);

- 1223 ▶ Intercepting those instructions/ transactions to prevent them to reach the settlement engine;
- 1224 ▶ Re-opening the system to the T2S Actors (excluding ICPs) for reconciliation purposes only;
- 1225 ▶ Assisting the involved T2S Actors (excluding ICPs) to re-submit the “lost” instructions/  
1226 transactions.
- 1227 The T2S Service Desk announces dates when the testing scenarios and rotations are envisaged. The  
1228 T2S Actors (excluding ICPs) can candidate for participating.
- 1229 The table below describes the T2S service continuity test scenarios conducted between the two  
1230 regions twice a year:

Test scenario	Location
1st test: site recovery	Region 1
2nd test: regional recovery	Failure region 1 and recovery region 2
3rd test: RAD	Region 1
4th test: site recovery	Region 2
5th test: regional recovery	Failure region 2 and recovery region 1
6th test: RAD	Region 2

1231 *Table 10 - T2S Service*