TARGET2 contingency and business continuity testing

Version 0.1/ February 2008

WGT2/2009/032-rev

TARGET contingency and business continuity testing

Foreword

This document describes the testing and training of contingency and business continuity arrangements (tools and procedures) for TARGET2. The scenarios follow the principles used to describe abnormal situations in the chapters 4 and 5 of the TARGET2 Manual of Procedures (T2-MOP).

It is intended that after completion this document becomes part of the T2-MOP (chapter 7). In line with the approach chosen for the T2-MOP duplication of information provided already in other TARGET2 documentation is avoided to the extent possible. Following the general assumption under 1.4 the T2MOP cannot itself create commitments for the 3CB since these have been negotiated and are codified in the SLA.

The paper should be considered as a *living document*. Furthermore, practical lessons to be learnt from the first round of tests in 2009 will be taken on board.

TARGET2 CONTINGENCY AND BUSINESS CONTINUITY TESTING

TABLE OF CONTENTS

1. INTRODUCTION

This section provides general background information on testing.

1.1. Scope

This document aims at describing the testing of the contingency and business continuity procedures for use in abnormal situations in TARGET2 as described in chapter 4 and 5 of the T2-MOP. TARGET2 includes the Single Shared Platform (SSP), Proprietary Home accounts (PHAs) and other applications used by CBs, ancillary systems and banks[1] to connect to and operate with the SSP. Although the CRSS is a component on the SSP it is not regarded as a critical business functionality for the processing of payments and does for this reason not fall within the scope of this document.

The testing of business continuity measures by CBs (without a PHA), ancillary systems and banks are currently left outside the scope of this document.

The testing of a prolonged SWIFT failure does not fall within the scope of this document since the Governing Council of the ECB accepted the residual risk of such an outage[2].

1.2. Objective of testing

Processes in the Payments Module (PM) and other modules of the SSP undergo a strict testing and verification programme. This includes: Level3 internal acceptance, Level2 acceptance and T2 user testing. These processes are with the exception of the contingency module, afterwards regularly used in live operations. Contingency and business continuity measures have the objective to ensure that failures of TARGET2 components at SSP, CB and user level do not cause any disruption to the overall functioning of TARGET2. To maintain the highest standard TARGET2 provides for payment processing testing is of the utmost importance.

1.3. Roles and responsibilities

The **SSP service desk** is expected to provide and monitor the SSP and its infrastructure and stand ready to answer any query about the operations of the SSP, supporting the national service desks.

The **national service desks** are expected to organise the tests with its participants. They are expected to prepare a test schedule, collect the test reports from their participants and send a summary report to the TARGET2 coordination desk.

[1] Testing is only mandatory for critical players (see 2.6.1) and those banks that process payments falling under the concept of (very) critical payments.
[2] Sec/Govc/X/07/107

The **TARGET2 coordination desk** at the ECB will contribute to the organisation at the inter-member-state level, whenever needed, and collect the reports from all CBs. Based on the information received the TARGET2 coordination desk will prepare an overall test report summarising the outcome of the tests and to submit this to the Level 2.

1.4. Test environment

For the tests to be effective, they should either be performed in the production environment or, where this is not considered appropriate due to the additional operational risk, in a test environment as similar as possible to the production environment. For tests with users (CBs, banks, ancillary systems), the user test environment of the SSP (CUST) is considered as close to the production environment as a test environment can be. Occasionally, when new SSP releases are tested by the CBs and the users, the CUST environment may not use the same version as the PROD environment. Taking into account that such new versions are expected to be used in PROD environment soon after, this should be considered when evaluating the test results, but is in principle not expected to have a detrimental effect on the test results

With regard to the PHA environments, each CB providing a PHA is expected to provide a test environment that fulfils the requirements mentioned above (a test environment as similar as possible to the production environment).

1.5. Frequency and planning

Tests described in this document should be performed at least once every six months, i.e. once during each half year period. By exception, the SSP rotations will take place on average every nine months.

The CUST environment of the SSP is normally open every weekday from 06:30 until 19:00, except on Fridays when it closes at 17:00, even if the SLA envisages from 08:00 until 17:00 only..

In addition the SSP Service Desk will provide the NCBs and the T2 Coordination Desk at the ECB with a set of weekends where the PROD environment and the 3CB support can be available upon request according to the prescription contained in section 3.7 of the Service Level Annex (SLA) to the Agreement on the Single Shared Platform for TARGET2. These dates will be announced well in advance, i.e. by end November for the forthcoming year. A full calendar of the IT Service continuity tests is presented to the Settlement Managers Sub-Group (SMSG) on a yearly basis normally a the occasion of the first SMSG meeting/teleconference of the year

It is expected that the NCBs/ECB organising the tests provide the T2 Coordination Desk at the ECB with a test calendar with an overview of the scheduled activities for the next six months. This overview should arrive no later than 7 business days prior to the start of the next six month period (e.g.

20 June). The T2 Coordination Desk at the ECB will provide a general overview to all CBs and the SSP.

1.6. Test support from the SSP

For test and training activities both in the PROD as well as in the CUST environment the support service of the SSP service desk will be provided as defined in the section 3.7 of the Service Level Annex (SLA) to the Agreement on the Single Shared Platform for TARGET2 (PSSC/2007/482_rev3). Activities outside the agreed business hours in PROD are limited to the set of week-ends as stated above. In CUST activities normally take place during standard business timing. In case of incidents priority will be given to resume live operations while test and training activities related issues will be considered with lower priority.

1.7. Test results

Test results should be classified as either successful or unsuccessful. When the requirements are not met, the test result should be seen as *unsuccessful*. For *unsuccessful* tests a repetition of the test is expected within 3 months after.

1.8. Reporting

The test activities should be reported by the SSP and CBs on a half-yearly basis within 1 month following the last planned test activity, to the T2 Coordination Desk at the ECB. For tests where participants are involved CBs are expected to collect and summarise their reports and forward the summary to the T2 Coordination Desk at the ECB. The ECB will provide a comprehensive reporting form. The ECB test co-ordinator will prepare a report summarising the outcome of the tests and any deviations to the agreed plan and submit it to the level 2 on a half-yearly basis. The summary will cover the test activities performed as well as any follow-up items identified in previous periods.

2. INFRASTRUCTURE

This section provides background information on the infrastructure foreseen for testing.

2.1. Overview

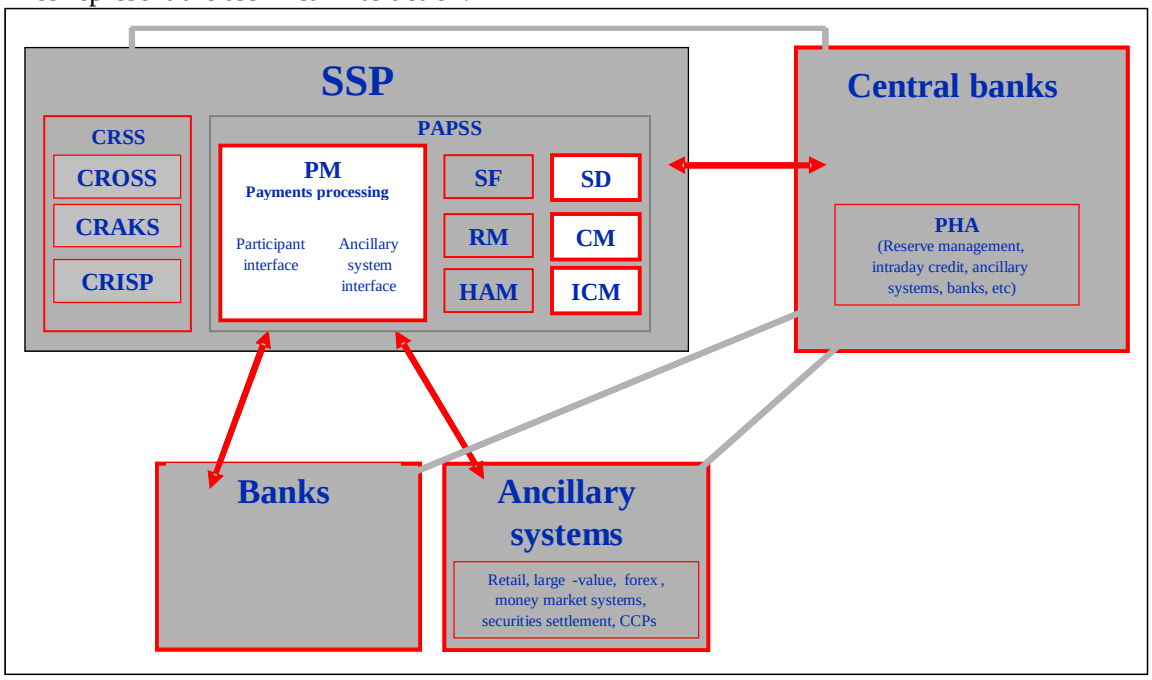
A modular approach has been taken for setting up of the TARGET2 SSP. Every module in the SSP is closely related to a specific service (e.g. the Payment Module for the processing of payments). Some of the modules (Home Accounting, Standing Facilities and Reserve Management Modules) are optionally used by the individual central banks.

Central banks that do not use these modules may offer the respective services via proprietary home account (PHA) applications in their domestic technical environments.

SWIFT standards and services are used (FIN, InterAct, FileAct and Browse) to enable standardised communication between the TARGET2 system and its participants.

2.2. Logical components

The graph below provides a general overview of the logical components as defined in the TARGET2 documentation. In general a distinction can be made between systems (SSP, PHA) and actors (CBs, Banks and Ancillary Systems). The grey lines in the overview represent the communication and red lines represent the technical interaction.



2.3. Systems

While most or all of the TARGET2 functionality is provided by the SSP, in some countries this is complemented by additional services provided by the respective CB (e.g. the PHAs).

2.3.1. The SSP

The SSP with all its components includes the PAPSS (Payment and Accounting Processing Services Systems) and the CRSS (Customer Related Services System). As mentioned in section 1.1 the CRSS does not fall within the scope of this document.

2.3.2. The PHAs

The proprietary home accounting (PHA) applications maintained by some individual central banks are primarily used to manage minimum reserves, standing facilities or cash withdrawal, but also to settle interbank or ancillary system transactions for a maximum transition period of four years from the time the central bank has connected to TARGET2.

2.4. Actors

The system is used by different types of participants, which are further described in the next three sections.

2.4.1. Banks

Banks are by far the largest group of actors in TARGET2. Liquidity wise the smooth functioning of TARGET2 depends to a large extend on banks falling within the scope of critical players and those banks that process payments falling under the concept of (very) critical payments. The Info guide (Section 3.5.2) specifies which TARGET2 participants are considered critical. The testing of contingency arrangements is only mandatory for them.

2.4.2. Ancillary systems

The group of ancillary systems is composed of organisations in the field of securities clearing and settlement, retail payment systems (systemically important retail payment systems (SIRPS), prominently important retail payment systems (PIRPS) and other retail payment systems), and other large-value payment systems (e.g. CLS and EURO1). The Info guide (Section 3.5.2) specifies which TARGET2 ancillary systems are considered critical. The testing of contingency arrangements is only mandatory for them.

2.4.3. CBs

Central banks are also falling under the scope of the "Information security policy for TARGET2" approved by the Governing Council (SEC/GovC/X/06/270a.final) and thus have the responsibility to ensure that their infrastructure is operated in a secure and reliable manner. Each CB has the status of a direct participant. In practical terms, this means that each CB is:

•directly addressable in TARGET2 in order to receive payments from other participants

•able to submit payments on its own behalf or on behalf of its customers to TARGET2 (eg state agency, supranational organisation)

In general, CBs maintain all contacts and provide any kind of support to their participants (credit institutions, ancillary systems)

From an operational viewpoint CBs are responsible for:

•Inclusion and exclusion of participants

•Monitoring the activity of their participants

•Provision of intraday liquidity necessary for the smooth running of the system

•Initiating payments on behalf of their own or on behalf of their participants

•Billing to their participants

•Handling of local contingency

3. CONTINGENCY ARRANGEMENTS

In general, the procedures that apply to abnormal situations can be found in the MOP. These procedures do apply to all TARGET2 participants. Each participant using the SSP should at first rely on its own back-up measures. The SSP offers three measures to overcome short interruptions on the side of the participants itself, NCBs operating a PHA or the SSP. The next three sections give a short description (from the UDFS) of these measures. They aim at processing a limited number of payments falling within the concept of (very) critical payments in TARGET2, see MOP. Additionally CBs may offer their participants other arrangements such as; AS contingency tool, mandated payments).

In this respect each participant and each CB should identify and keep up-to-date information about the maximum number of (very) critical payments to be processed per hour and the respective channels that may be used to perform these payments in contingency. CBs should take into account their own processing requirements plus those of the participant with the highest possible hourly number of such payments.

3.1. Contingency arrangements for failing participants

3.1.1. Backup payments

Participants may use two slightly different types of back-up payments to initiate payment orders via the ICM in a situation where their normal payment processing ability is interrupted.

- Back-up contingency payments are used to fulfil obligations arising from CLS, EURO1 or STEP2 payments on time. They replace the original payment.
- Back-up lump-sum payments allow the participant to redistribute liquidity accumulating on its account and accordingly to minimise interest and damage claims.

For details on the back-up payments functionality please see the UDFS, book 1, section 2.4.5.

3.1.2. Additional arrangements offered by CBs

CBs may offer their participants other arrangements (such as; AS contingency tool, mandated payments).

3.1.3. Test Scenarios

Each participant (including each CB and each AS) intending to use the back-up payments feature or an additional arrangement offered by its CB should perform one of the following four test scenarios at least twice a year following pre-agreement of the date with the respective CB (or in case of a CB with the SSP service desk):

- Requesting the activation of the back-up functionality in live operations via its CB (or in case of a CB via the SSP service desk) and the sending of the respective back-up payments as low value payments (less than 10€, but different amounts) to pre-agreed accounts. CBs may offer its account to be used as addressee for payments, when no other test partner is available. CBs should agree between themselves on reciprocal use of CB accounts for such tests,
- Alternatively, if the risk of tests in the live environment is considered to be too high, the same type of test may be performed in the CUST environment. Then no limits apply to the amount.
- AS contingency tool, CBs offering their AS this option are expected to test its operational functionality.
- Mandated payments, CBs may offer mandated payments in addition to the options mentioned above.

3.1.4. Organisation

For both scenarios CBs may decide – in cooperation with their national user community - to limit the number of days and time when such tests are possible or may keep this as a permanent option accessible on each day when the respective environment is operating. When limiting the number of days or the time, CBs shall ensure that sufficient opportunities are provided allowing each participant to schedule respective tests at least every two months.

3.2. Contingency Module

The Contingency Module (CM) is the common mandatory tool for the CBs to manage an emergency situation where the normal PM functionality is not available, but still critical and very critical payments have to be preformed. Only CBs have access to the CM and can perform payments on behalf of their users.

Further information on this feature can be found in the UDFS book 1 chapter 4.

3.2.1. Test scenarios

Although only CBs have direct access to the CM, also all users involved in the processing of (very) critical payments shall be involved in this test, i.e. the delivery of the respective payment orders and payment information between the CB and its users is part of the test scenario.

The scenario consists of the delivery and processing of the hourly maximum of (very) critical payments by the users to the CB and the respective processing in the CM. Where inter-member-state payments are part of the scenario and the counterparty is not available for testing, the respective CB shall replace the external counterpart with one of its own accounts.

The SSP Service Desk should test the same scenario acting on behalf of a CB performing the highest hourly volume of (very) critical payments foreseen for any CB.

In addition, every three months, the ECB will organize live trial sessions for the contingency module . Each session will involve a group of NCBs and – upon these latter's choice – also users. On those days the SSP Service Desk will activate the CM in the PROD environment in parallel to normal operations with the twofold aim to verify both the connectivity to the CM itself and the adequate set-up of users for live CM operations, but not for volume testing.

3.2.2. Organisation

The SSP Service Desk activates the CM in CUST on a weekly basis already from the TARGET2 Level2 Acceptance Tests phase.. Based on this CBs should offer this possibility to all their customers on a regular basis including the delivery of payment order and payment information between the CB and its participants. Tests should be organised by the CB in coordination with its user community and coordinated with the SSP service desk. Also cross border cooperation between several CBs performing such tests in a coordinated manner should be possible. CBs should be able to act on behalf of their participants to process critical and very critical payments.
Participants are expected to exchange their hourly maximum number of critical payments. CBs are expected to confirm payments executed using a secure channel.
Participants are expected to find counterparts with whom they can exchange payments.

For CM trials in the live environment activities at the CB level will follow a script to be prepared by the ECB, the involvement of users has to be organised by each CB for its users.

3.3. Contingency measures by PHAs

PHAs with payments functionalities are expected to execute the identified critical payments on behalf of their own user community. Therefore contingency tests should be carried out to verify that contingency measures are technically and operationally effective, even without involvement and/or exposure to external parties.

3.3.3. Scenarios

I. Failure at the start of the day trade phase, requiring transferring of liquidity for "critical players" to the PM.

II. Failure at the end of the day requiring the manual processing to the reserve management module and/or PHA accounts.

3.3.4. Organisation

For both scenarios CBs may decide – in cooperation with their national user community - to limit the number of days and time when such tests are possible or may keep this as a permanent option accessible on each day when the respective environment is operating. When limiting the number of days or the time, CBs shall ensure that sufficient opportunities are provided allowing each participant to schedule respective tests at least every six months. Whenever possible the regular CLS and EBA testing activities should be taken into account as they would fulfil the requirements. .

4. BUSINESS CONTINUITY

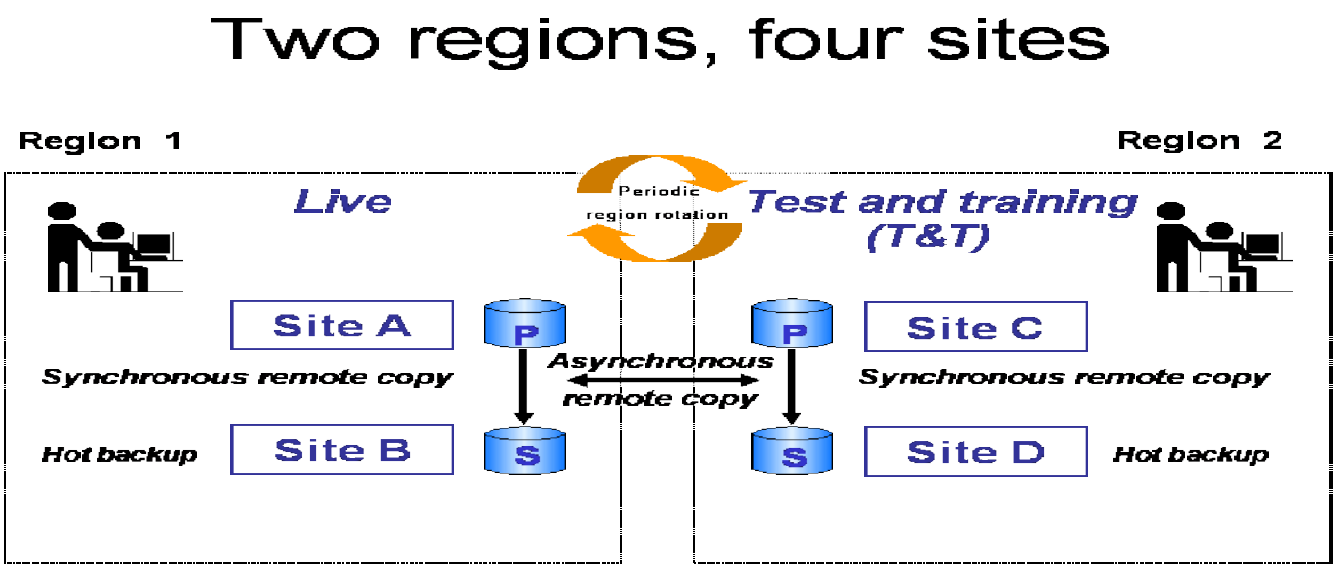
Business continuity comprises the procedures and infrastructures in place with the SSP, which allow in case of a normal failure or disaster, to failover to the hot backup site within the same region or to the second region, see 2.3 PAPSS. CB providing a PHA and at least critical participants are expected to have similar procedures and infrastructures in place.

Furthermore the business continuity oversight expectations for systemically important payments systems (SEC/GovC/X/06/173b) have to be taken into account

4.1. Business Continuity on the PAPSS

The PAPSS central processing system business continuity is based on two regions/four sites. In each region two sites are located at a distance of some kilometres in order to present different risk profiles. The two sites are fully equivalent and are connected by means of fibre optical channel; the same technological resources are installed in each centre: i.e. CPU, storage, network interface, software, etc.; the recovery within a region is assured by synchronous remote copy (SRC) active on the whole SSP environment between the two sites of the same region. The SRC guarantees real-time data updates in both sites; it means that each written operation is completed only when both sites are updated. Intra-regional recovery shall occur within a maximum period of 1 hour (without taking into account decision-making time) with no loss of data updates.

Recovery of a regional disaster is based on region sites located at long distances from each other (hundreds of kilometres) each with a different risk profile. As in the intra-region recovery, the sites of the two regions are fully equivalent.



4.1.1. Scenarios

Following the above two recovery options have to be considered for testing purposes:

a. intra-regional failover

b. inter-regional failover

Considering the half-year requirement stemming from the T2SRC and the nine month average period envisaged for rotation, intra- and inter-region could be both considered as valid business continuity exercises. The scenarios are run in the PROD environment during week-ends. Depending on the phase of the business day during which the SSP is, settlements can be tested as well.

During the normal business days and hours, similar exercises can be executed in CUST. Of course no actual failover is performed in such cases being the situation tested in PROD. It is however possible to simulate a major failure including the activation of the CM and usage according to scenario 3.2.1. and the delay of the closing time.

4.1.2. Organisation

The SSP will announce the dates when the testing scenarios are envisaged as part of the calendar mentioned in section 1.5

The NCBs and the ECB can candidate for participating. Participants are expected to find counterparts to exchange payments with.

4.2. Business Continuity for PHAs

PHAs with payments functionalities are expected to maintain a secondary site. Therefore business continuity tests should be carried out to verify that business continuity measures are technically and operationally effective, even without involvement and/or exposure to external parties.

4.2.1. Scenarios

PHAs with payments functionalities are expected to carry out a intra-regional recovery test in the CUST environment. With regards to the time of performing the test no additional requirements have to be met.

The same scenario can be tested in the PROD environment.

4.2.2. Organisation

The CB will organise the tests themselves and are expected to inform the TARGET2 Coordination desk and the SSP service desk in advance.

4.3. Business Continuity for CBs, banks and AS

Section will be completed once the critical players have been identified and potential additional test requirements resulting from the respective oversight expectations have been discussed. The Info guide (Section 3.5.2) specifies which TARGET2 participants are considered critical. The testing of contingency arrangements is only mandatory for them.