# T2S General Specifications

## General Specifications

## 1.0

Author 4CB and ECB

Version 1.0

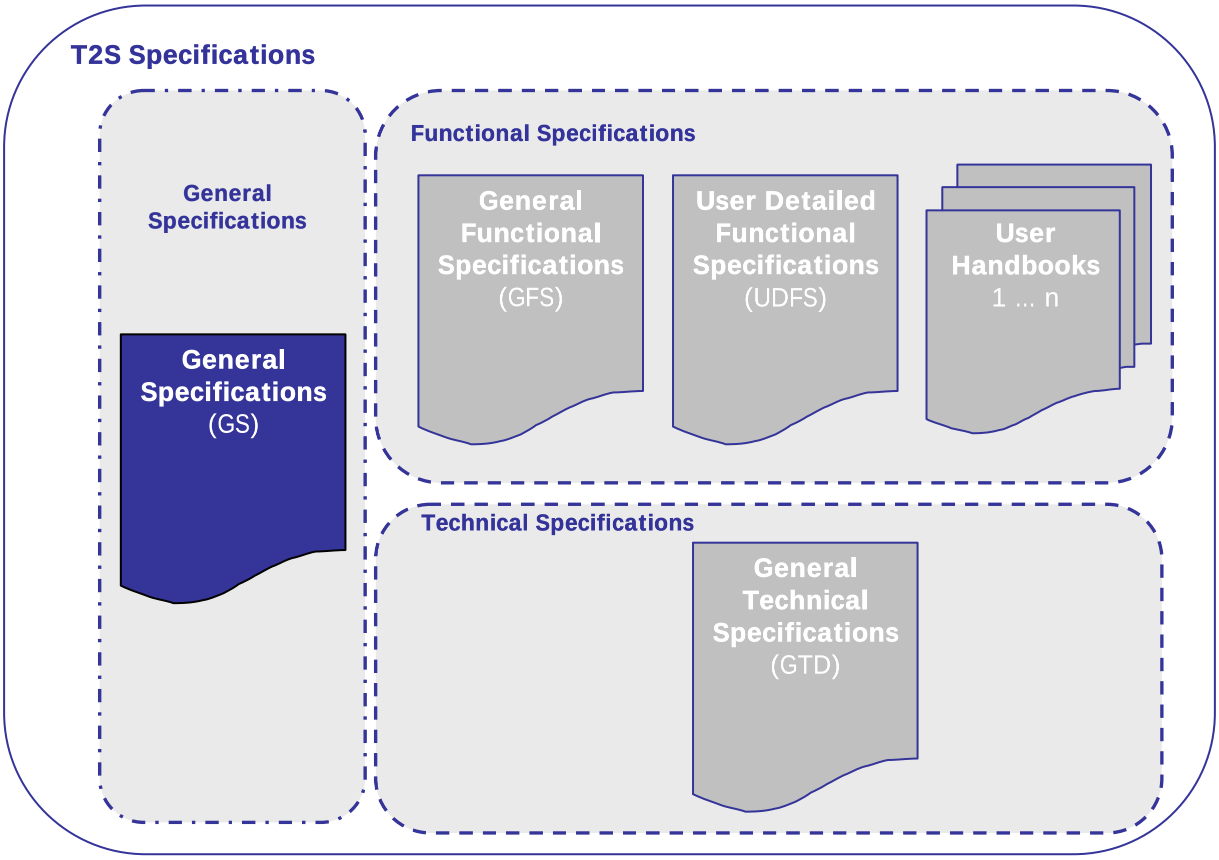
Date 28/01/2010

# Introduction

## Overview of the T2S deliverables for the specification phase

The T2S deliverables for the specification phase are considered as documents aiming at allowing users to understand how the T2S User Requirements Documentation will be implemented.

The diagram below presents an overview of the main T2S deliverables for the specification phase.


T2S Specifications
General Specifications
General Specifications (GS)
Functional Specifications
General Functional Specifications (GFS)
User Detailed Functional Specifications (UDFS)
User Handbooks 1 … n
Technical Specifications
General Technical Specifications (GTD)

## Objective of the present document

The General Specifications document (GS) presents the high-level description of T2S. It aims at giving to the T2S stakeholders a global and comprehensive picture of the T2S solution and at explaining how the User Requirements which are not covered by the General Functional Specifications (GFS) and General Technical Design (GTD) will be fulfilled. With respect to the latter documents, the General Specifications should be understood as an executive summary of those documents, which present in more details the T2S solution.

The General Specifications are based on the "General principles and high level proposals for the user requirements (April – June 2007)" and the "User Requirements Document" (URD) v4.2[1] both approved by the Governing Council. In addition, functional and technical aspects are derived from the TARGET2 Securities Feasibility Study.

## Content of the document

This present document is organised into six chapters:

- Introduction – presentation of the General Specifications document;
- Chapter 1: Overview of T2S;
- Chapter 2: Functional description – presents the overall functional design of the T2S platform and describes in general terms its functionalities per domain and module;
- Chapter 3: Technical description– describes in general terms the service level assumptions, the application and the infrastructure design, the connectivity services and the business continuity model;
- Chapter 4: Operational phase description – presents in general terms the service desk, the support organisation, the service management, the operating day and the calendar;
- Chapter 5: Information Security Management – presents the objectives, the scope and the organisation of the security policy;
- Chapter 6: User testing and migration process – presents in general terms the migration strategy, the migration support to the users, the organisation of the change-over and the external tests.

[1] Even if not specifically indicated, all references to the URD in this document are to be understood as references to URD v4.2, published on 3 July 2009.

# 1. Overview of T2S

On 17 July 2008, the Governing Council of the European Central Bank (ECB) took the decision to launch the TARGET2 Securities (T2S) project.

T2S is a major step towards a single integrated securities market for financial services, reinforcing the Lisbon agenda and in particular the Code of Conduct on Clearing and Settlement and the Giovannini harmonisation effort. It delivers a single borderless pool of Europe-wide securities, and a core, neutral, borderless state-of-the-art settlement process.

In line with the Governing Council's decision of July 2006, the proposed platform will be fully owned and operated by the Eurosystem. In addition, the Governing Council decided on 8 March 2007 that "the T2S service will be developed internally within the Eurosystem and operated on the TARGET2 platform in order to exploit synergies with TARGET2 to the fullest extent". Upon deciding to launch the project on 17 July 2008, the Governing Council also decided "to assign the development and operation of T2S to the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d'Italia".

The aforementioned group of central banks, denominated "4CB", will act as "Providing central banks" for T2S with the objective of reinvesting the experience gained from the development and operation of the TARGET2 Single Shared Platform (SSP) while incorporating expertise of Securities Settlement System (SSS), coming from central bank activities and from the support of the numerous T2S stakeholders.

In the context of this document, the acronym "SSP" represents the underlying technical infrastructure and the operational organisation that will enable the 3CB and 4CB to offer T2 resp. T2S services.

## 1.1. Scope of T2S

In order to have a global and comprehensive picture of the T2S system, the scope of T2S coming from the URD v4.2 (Management Summary) is hereafter recalled. In line with the fundamental objective of T2S – i.e. the provision of **harmonised and commoditised** securities settlement services in central bank money (CeBM) in euro (and in other currencies) for substantially all securities deposited in T2S connected Central Securities Depositories (CSDs), the scope of T2S can be defined as follows:

- T2S is a Europe-wide core securities settlement platform, since its design allows settlement in CeBM in euro and in other currencies, where the relevant central bank and the market wish to support such services;

- T2S maintains dedicated CeBM accounts representing a T2S party's payment bank claims and obligations in CeBM vis-à-vis a central bank. Each cash account is linked with a RTGS account held in TARGET2 and may be used to settle transactions relating to the account holder's or another T2S party's security accounts in one or more CSDs;
- T2S matches settlement instructions. It also accepts matched instructions from CSDs which apply the same matching rules;
- T2S provides securities settlement in real-time with auto-collateralisation and optimisation procedures, irrespective of which CSD and which central bank provide the respective underlying securities and CeBM accounts. It can do so by providing realignment in real-time, when securities issued in one CSD are settled in other CSDs;
- T2S offers direct technical connectivity services to CSD clients and to Central Counterparties (CCPs).

## 1.2. Concept of T2S on T2[2]

The Governing Council states that "the T2S service will be developed internally within the Eurosystem and operated on the TARGET2 platform in order to exploit synergies with TARGET2 to the fullest extent", which formed the basis for the now commonly used "T2S on T2" concept.

This concept means that the two distinct services, "T2" for large-value euro payments processing and "T2S" for securities settlement in CeBM, are based on the same infrastructure. This solution allows exploiting synergies between TARGET2 and T2S infrastructures while avoiding tight and risky dependencies between critical services.

### The reuse of the existing technical architecture designed for TARGET2

T2S can draw on the existing architecture designed for TARGET2, including a fully scalable central processing system, a storage sub-system with synchronous and asynchronous mirroring and a dedicated network connecting the different processing sites. Naturally, the existing components have to be resized in order to process increased activity volumes, but the SSP architecture guarantees that T2S services can be delivered optimally in terms of performance and overall resilience.

Finally, the homogeneous presentation layer for TARGET2 and T2S makes it possible to integrate (at user workstation level) the full set of services provided by TARGET2 and T2S through a "single window" access. The presentation layer will be enhanced in order to meet the T2S user requirements in terms of Graphic User Interface and to benefit from the evolution of technology.

[2] Being dealt in the principle 2 and the annexe 4 of the User Requirements.

### Direct synergies

The "T2S on T2" concept brings direct synergies, as it allows reusing or sharing resources currently available for TARGET2. For the technical architecture, the mutualisation of some components or the time-sharing of equipments and teams allows optimising the TARGET2 SSP resources by exploiting possible load-balancing between the services, and by improving the occupation rate of Test & Training environments, for example. This mutualisation of the infrastructure which excludes cross-subsidisation leads to lower costs for the users.

Sharing the same platform also allows common tools to be used for the two services (e.g. Change Management system, Trouble Management system, Technical Monitoring). Nevertheless there is no technical dependency between the two services.

**"T2S on T2" is an open concept that should not impose constraints on the user requirements, while allowing cost savings thanks to the synergies with TARGET2 and the reuse of the SSP architecture. This approach can ensure the timely delivery of a cost-efficient solution in the interest of Central Securities Depositories, Credit Institutions, CCPs and the Eurosystem.**

## 1.3. T2S, a step towards integration of European financial markets

### Interaction between TARGET2 and T2S

From a business perspective, TARGET2 and T2S are complementary to each other. While TARGET2 will bring euro central bank money to T2S for the settlement of securities transactions in euro, T2S will generate liquidity that can be used in TARGET2.

The "T2S on T2" concept[3] provides optimal conditions for easing this liquidity management and therefore makes it more efficient for the underlying businesses of both TARGET2 and T2S. For TARGET2, for example, it facilitates the provision of additional liquidity through the proximity of securities settlement features, while for T2S it allows an optimisation of the liquidity used in the securities settlement process.

### Interaction between T2S and non-euro RTGS systems

Despite the technical operation of T2S and TARGET2 on the same platformT2S shall be designed following an "open" concept, meaning that the same interface specifications can be used to connect other RTGS systems to T2S (particularly with the use of a set of standard messages) **{T2S.12.340}**, which ensures a comparable level of efficiency for liquidity management in other currencies.

Indeed, the potential to optimise central bank liquidity management is essentially not driven by the technical implementation, but by the efficiency of the interaction between T2S and the relevant RTGS systems, and by the operational framework allowing the respective central banks to control the use of their currency. Therefore, from the outset, T2S will be developed as a multi-currency system, allowing

[3] See 1.3

non-euro central banks to provide liquidity for the settlement of securities transactions in their currency, not only for the benefit of their local financial market, but for the European market as a whole. The Eurosystem is committed to working together with non-euro central banks, with the aim to agree on common conditions for the provision of non-euro liquidity in T2S.

### Interaction between T2S and collateral management systems

Given the possibility for central bank credit to be collateralised by securities that are settled on T2S, significant benefits exist by linking the central banks' collateral management systems directly to T2S. This will also facilitate the process of auto-collateralisation, via which central bank liquidity can be created automatically in case insufficient funds are available on the buyer's account. Together with the RTGS system, this creates a liquidity management "triangle", which promotes the internal integration of treasury functions of financial institutions and provides them with efficient tools to service their customers,

# 2. Functional description

## 2.1. Introduction

Starting from the external behaviour of the system described in the User Requirements, the 4CB have designed from the functional viewpoint the future T2S system. The goal of this chapter is to describe the functional architecture of the future T2S system to be implemented. It therefore includes a general description of (i) modules making up the system, (ii) data flows exchanged with the outside of the system, (iii) data flows exchanged between the modules and (iv) static data required for the functioning of the modules.

The functional description is based on a hierarchical description of T2S functionalities according to three levels: domains, modules and functions. The terminology “Domain/ Module/ Function” is specific to the T2S design and corresponds to the following definitions:

- The concept of “Domain” refers to the highest level of the hierarchical description of the T2S functionalities. Each of the seven domains identified for T2S covers several modules consistently grouped together according to their proximity of activity. The breakdown into domains has been done with a view to stick to the largest possible extent to the breakdown already identified in the T2S User Requirements;
- The concept of “Module” refers to the second level of the hierarchical description of the T2S functionalities. Each module covers several functions consistently grouped together according to their proximity of activity. For the provision of the T2S services identified in T2S User Requirements, each module can exchange information with T2S Actors as well as with external systems via the Interface domain and with other modules belonging to the same or different domains, as illustrated below in the High-Level Diagram;
- Finally, the concept of “Function” refers to the most detailed level of the hierarchical description of the T2S functional solution. In this context, a function is a process unit having access to static and dynamic data with a view to process and exchange data flows with other functions or external T2S Actors and systems via the Interface domain. The provision of services identified in the T2S User Requirements relies on the intervention of one or several functions pertaining to one or several module(s) and domain(s).

Only the levels Domains and Modules are described in the General Specifications.

The scope of the functional components covered in this functional design of T2S encompasses the following features:

- “Transversal functionalities”, being understood as derived from user requirements that do not necessarily lead to the implementation of a definite function but have an impact on the way the functions of T2S are implemented;

- Functionalities derived from user requirements regarding specific features of the future system as well as from requirements referring to the whole service provided, taking into account not only the system itself but also its operating conditions, i.e. non-functional requirements formulated.

At this stage, the GS propose a description at level of domains and modules and a first view of the data model, whereas the GFS will complement this description with higher granularity.

## 2.2. Overall high level diagram

The overall high-level diagram aims at providing a global vision of T2S, based on the breakdown of T2S in seven domains, each of these domains being split into a given number of modules. This overall diagram is a conceptual functional representation of the future system, irrespective of the technical choices for implementation.

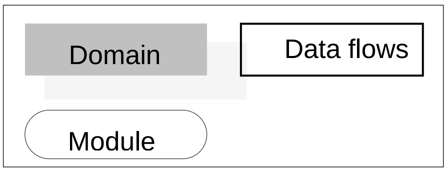
The User Requirements Document already provides some functional descriptions in order to illustrate and clarify the most complex requirements. Even though these descriptions are clearly not to be considered as binding for the future T2S design, it was deemed preferable to stick as far as possible to them, in order notably to allow an easier access for readers already familiar with the structure of the User Requirements.

The following mapping was performed:

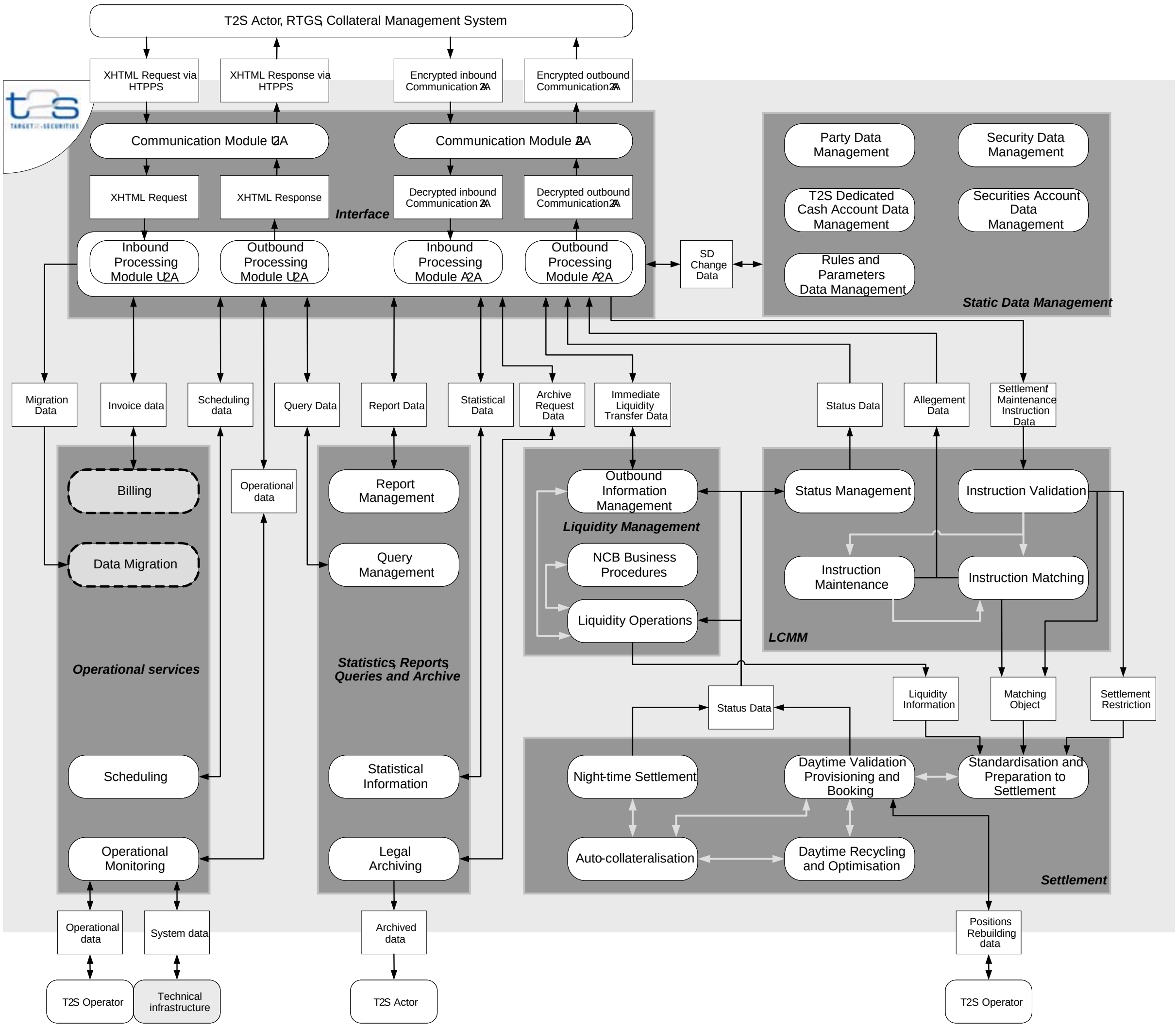
| HIGH LEVEL DIAGRAM DOMAIN | UR CHAPTERS | COMMENT |
|---|---|---|
| Interface | Part of Interface | This domain includes only the "technical" interfaces part of the UR document chapter and also includes the view on the A2A and U2A communication modes. |
| Static Data Management | Static Data Management and configuration requirements | Identical perimeters covered by the two chapters |
| Life Cycle Management and Matching (LCMM) | Life Cycle Management and Matching | Identical perimeters, but the integration of the Settlement Eligibility module into the Standardisation and Preparation to Settlement additional module (see below) |
| Settlement | Settlement | Identical perimeters; with two additional modules on Standardisation and Preparation to Settlement and on Night-Time Settlement |
| Liquidity Management | Provision of liquidity, collateral management and monitoring of liquidity | This domain includes the functions required for the management of liquidity transfers between T2S and the RTGS systems in charge of managing payments in Central Bank money for a T2S eligible currency. |
| Statistics, Queries, Reports and Archive | Part of Interface, Statistical Information, part of non-functional requirements on archiving | Modules providing the T2S users with several data exploration tools. |
| Operational Services | Part of non-functional requirements | This domain includes specific modules dedicated to support the operational management of the T2S platform. |

### *Conventions used for the presentation of the overall high-level diagram*

The organisation of the functionalities is described using three symbols: Domain, Module and data-flows exchanged between the modules.



## The High-Level Diagram



## 2.3. Description of functional domains

### 2.3.1. Interface

The T2S Interface domain handles all incoming and outgoing communication with all T2S Actors and other external systems (such as RTGS systems and Collateral Management Systems), manages the use of the appropriate communication medium and conducts the relevant technical entry checks. Communication from T2S Actors connecting to T2S must have to comply with the formats and specifications defined in T2S.

T2S supports the connectivity of CSDs and T2S parties as follows:

- T2S communication is available by using messages or files containing messages in Application-to-Application mode (A2A) that allows direct communication between software applications via XML messages as well as through online-screen based activities in User-to-Application mode (U2A) for activities performed by T2S users;
- For the T2S communication via messages the ISO 20022 is the single standard, concerning both inbound and outbound communication. In addition, the T2S Interface complies with Giovannini protocol recommendations. Therefore, all messages exchanged between T2S and T2S Actors are based on XML technology and comply with the ISO 20022 standards on messages. They are sent to T2S either individually or in a file containing one or several messages.

The T2S Interface services are available continuously during settlement days. However, their availability is restricted during the Maintenance Window and is not guaranteed during weekends and closing days (except in exceptional cases).

The T2S Interface domain includes three modules:

- Communication Module;
- Inbound Processing Module;
- Outbound Processing Module.

#### 2.3.1.1. Communication Module

The main purpose of the Communication Module is to ensure secure and reliable communication between the T2S platform and T2S Actors. T2S System Users can use Application-to-Application (A2A) and User-to-Application (U2A) communication channels to access the T2S platform. The Outbound Processing Module for Application-to-Application mode provides a single set of standard messages to facilitate communication with multiple external RTGS systems and with multiple external collateral management systems.

Additionally, the Communication Module ensures protection of the T2S platform against an intrusion and unauthorised access. It validates that only trusted party transmits the inbound communication through a secure channel. It provides an authentication functionality to verify the identity of the T2S System User.

The Certificate Management functionality is closely linked to the network providers and connectivity services. Detailed information will therefore be provided in a later version.

### 2.3.1.2. Inbound Processing Module

The Inbound Processing Module receives

- U2A - XHTML request,
- Stored inbound communication – A2A file or
- Stored inbound communication – A2A individual message

from the Communication Module and performs a series of technical verification checks. The processing of this module includes the Authorisation Check which is based on privileges.

As the availability of T2S is restricted during the maintenance window and the night-time settlement, the Inbound Processing Module for Application-to-Application mode includes queuing and restart functionalities, which allow the deferred processing of requests.

The Inbound Processing Module allows the initiation of resending of messages. This functionality can be used in contingency situations if the messages have been lost during the communication or due to technical problems on the receiver side.

The Inbound Processing Module includes the extraction of all relevant business data from the received request in order to structure them in an internal format, determines the relevant T2S back end modules and routes the structured data to them. In case of a rejection (e.g. the privilege for the requested action is not assigned to the T2S System User) the Interface creates the respective inbound processing rejection and delivers it to the Outbound Processing Module.

### 2.3.1.3. Outbound Processing Module

The Outbound Processing Module receives the data in the internal format from the processing modules of other domains. It generates the relevant messages in the necessary format and sends these messages via the Communication Module to the T2S System Users in U2A mode or to the Party Technical Address in A2A mode according to the specific message subscription preferences.

It is ensured that outbound communication reaches the appropriate party technical address and is delivered on due time to the receiving T2S actors.

### 2.3.2. Static Data Management

The Static Data Management domain provides T2S System Users with an integrated and consistent set of common information. It is the single access point for the creation, update and deletion of static data "relevant" for T2S in performing its functions, such as parties, securities, securities accounts and T2S Dedicated Cash Accounts among others.

T2S System Users of this domain belong to CSDs, NCBs, T2S parties, Payment Banks and the T2S Operator - each T2S system user accessing and using static data management facilities according to its own specific access profile. Different T2S system users have different roles assigned and, as a consequence, are allowed to see and possibly change different pieces of information.

T2S System Users of the T2S Operator belong to a specific user category devoted to system administration activities. With respect to static data management, they are responsible for entering and managing CSDs and NCBs data and a set of global rules and parameters. They can also act on behalf of other user categories in order to perform some specific actions or within some pre-defined contingency scenarios.

All changes in static data can be executed both in Two Eyes and Four Eyes mode, the actual mode to be adopted being established by the data owner. Proper functions are envisaged in order to allow each domain of the system to access the needed set of static data or to feed the other domains using some specific load procedures.

Versioning facilities allow the implementation of data history and data revision features, in order to keep track of all past data changes and to enter changes meant to become effective at a future date.

The Static Data Management functions are grouped in five modules, each module being in charge of a given subset of static data objects: Party Data Management, Security Data Management, Securities Accounts Data Management, T2S Dedicated Cash Account Data Management and Rules and Parameters Data Management.

### 2.3.3. Lifecycle Management and Matching (LCMM)

The LCMM domain deals with instructions received through the Interface domain. It is responsible for (i) the validation and matching of settlement instructions, before they are submitted to the Settlement domain, and (ii) the management and execution of maintenance instructions.

This domain is also in charge of checking the possible impact of static data changes on pending instructions, managing the revalidation and the consequences of such impact when relevant, while keeping tracks of the changes in the lifecycle of instructions. The services provided by this domain are available continuously during the whole day T2S operating hours, with the exception of the maintenance window.

The LCMM domain encompasses four modules:

### 2.3.3.1. Instruction Validation

The Instruction Validation module checks the consistency of instructions sent to T2S by a CSD or directly connected T2S Party. These consistency checks ensure that each incoming instruction is consistent with T2S Static Data. No syntax (or format) checks are performed by this module, as this kind of validation is carried out by the Interface domain.

T2S validates all incoming instructions received during the settlement day, based on a harmonised set of validation rules. Maintenance instructions (which amend, cancel, hold or release settlement instructions) are validated as well.

### 2.3.3.2. Instruction Matching

The Instruction Matching module is responsible for matching Settlement Instruction that requires to be matched in T2S. It compares the settlement details provided by the buyer and the seller of securities to ensure that both parties agree on the settlement terms of the transaction. The Instruction Matching module matches trading instructions in a standardised way (compliant to ECSDA matching proposals).

The Instruction Matching module is also responsible to create the corresponding Matching Object for each pair of matched Settlement Instructions, assigning them a T2S Matching Reference.

Those instructions which do not require matching are forwarded from the Instruction Validation module to the Standardisation and Preparation for Settlement module for their processing, and therefore are not under the scope of the Instruction Matching module.

The Instruction Matching module routes each Matching Object and the related Settlement Instructions to the Settlement domain for further processing.

The Instruction Matching module is available continuously during settlement days, with the exception of the maintenance window.

### 2.3.3.3. Instruction Maintenance

The Instruction Maintenance module handles maintenance instructions that:

- Amend, cancel, hold or release a Settlement Instruction;
- Cancel, hold or release Settlement Restriction;
- Release or cancel a Settlement Instruction for Conditional Securities Delivery purpose;
- Cancel previous Cancellation Instructions.

This module is also in charge of the cancellation of unmatched Settlement Instructions that remain as such after a standard period beyond their Intended Settlement Day, or the date of their last status value change, and also those instructions which have reached the end of their recycling period. The module forwards all instruction status values updates to the Status Management Module.

#### 2.3.3.4. Status Management

The Status Management module receives status values changes information from the LCMM and Settlement modules, analysis it, collects the relevant data, and forwards it as Message Data to the T2S Interface domain for transmission to the directly connected T2S parties and CSDs as per the message subscription service in a consistent way. All the modules dealing with changes in the status values of the Settlement Instructions (and/or the Settlement Instruction itself) activate this module by providing it with relevant information on the changes carried out on the Settlement Instruction as Instruction Status Information or Maintenance Status Information.

### 2.3.4. Settlement

The modules belonging to this domain are in charge of the actual booking of Settlement Instructions, Settlement Restrictions and Liquidity Transfers received from the other domains. The settlement occurs on a continuous basis during the daytime, and in sequences, grouped in pre-defined cycles, during the night-time.

This domain creates settlement transactions in a standard format, taking notably into account specific use cases such as Cross-CSD Settlements and Conditional Securities Delivery. Settlement transactions are either submitted to the daytime settlement in real-time or made available for the night-time settlement (Standardisation and Preparation to Settlement module).

During the daytime, a first settlement is systematically attempted (module Daytime Validation, Provisioning and Booking). The outcome of the settlement always triggers Daytime Recycling and Optimisation functions. These functions identify settlement transactions to be submitted to another settlement attempt, with an expected success, due to settled transactions bringing new resources, or due to unsettled transactions resolving gridlocks (Daytime Recycling and Optimisation module).

During the night-time, settlement transactions are grouped into sequences, submitted to optimisation procedures in order to identify sets of settlement transactions that can settle successfully, and then booked (Night-time Settlement module).

Both for daytime and night-time, auto-collateralisation procedures are used in order to reduce the number of cases with lack of cash (Auto-collateralisation module).

Lastly, as the Settlement domain is in charge of the realignment, CoSD and auto-collateralisation processes, it creates the corresponding additional settlement transactions. Additional settlement transactions are also created by the Settlement Domain for corporate action liquidity rebalancing and auto-collateralisation reimbursement[4].

[4] For all the above mentioned cases, the corresponding Settlement Instructions are generated by T2S.

### 2.3.4.1. Standardisation and Preparation to Settlement

The Standardisation and Preparation to Settlement (SPS) module is the entry module in the Settlement domain for Settlement Instructions, Settlement Restrictions and Liquidity Transfers to be settled.

It analyses the context of the settlement to be processed (Cross-CSD, In/Out T2S, CoSD, Blocking/Reservation/Earmarking, or standard settlement) and creates accordingly, on the intended settlement date, the associated settlement transactions including the amount of cash and/or securities to be settled.

The SPS module also creates when relevant additional transactions for realignment and CoSD[5].

Lastly, the SPS module also includes complementary functions (Cut-off Processing and EOD/SOD Processing functions) that handle respectively cut-off and end of day/start of day events in order to trigger the relevant process in the Settlement domain.

### 2.3.4.2. Daytime Validation, Provisioning and Booking

The Daytime Validation, Provisioning and Booking module updates, in daytime, the securities positions and cash balances, with the cash and securities movements of the incoming collection of settlement transactions and on the basis of the resources available.

To that purpose, the module receives collections containing a set of settlement transactions, either for their first settlement attempt or following an optimisation or recycling process.

The module settles all the received settlement transactions of a collection in an “all or none” basis and does not attempt any selection or de-selection inside a collection.

### 2.3.4.3. Daytime Recycling and Optimisation

This module selects and submits to another settlement attempt in daytime, unsettled settlement transactions that previously failed to settle.

It is triggered by a Collection Status Information event and launches, either optimisation functions when receiving unsettled collections, or recycling functions, when receiving settled collections.

### 2.3.4.4. Night-time Settlement

This module performs the settlement, during the night-time period only, of settlement transactions which are selected through sequences grouped into a predefined number of cycles.

[5] In all cases, the corresponding Settlement Instructions are generated by T2S.

These collections are made of new settlement transactions, created before the beginning of the sequence, and, settlement transactions which failed to settle in a previous settlement attempt, notably the settlement transactions recycled at the Start of Day.

Each sequence runs a succession of optimisation procedures to identify settable collections which are booked in the module.

#### 2.3.4.5. Auto-collateralisation

This module implements the provision of intraday credit by creating additional collateral settlement transactions, in case of lack of cash identified at the settlement of settlement transactions,

Such collateral settlement transactions fit to each NCB context (pledge sub, pledge or Repo) through pre-defined collateralisation procedures.

Auto-collateralisation is offered both on stock and on flow for eligible counterparts and eligible instructions, both during night-time and real-time settlement windows.

In addition to this main feature related to lack of cash, the module also manages the dynamic reimbursement or automated substitution, in case of fail during settlement, due to a lack of securities already collateralised.

Lastly, this module handles the reimbursement of intraday credit, due to a decreased NCB limit during the settlement day, or due to the end of day intraday credit reimbursement process.

### 2.3.5. Liquidity Management

The Liquidity Management domain is responsible for all the activities related to liquidity transfers between RTGS accounts and T2S Dedicated Cash Accounts as well as between two T2S Dedicated Cash Accounts. The domain encompasses three modules and performs the overall preparation of immediate, predefined and standing liquidity transfer orders on the T2S Dedicated Cash Accounts. Furthermore it triggers the related communication between T2S and the involved RTGS system.

The initiator of a liquidity transfer order can be both a payment bank as the account holder of the T2S Dedicated Cash Account and another party which is authorised by the account holder.

When initiating a Liquidity Transfer between T2S Dedicated Cash Accounts and the RTGS system, the liquidity transfer order is checked and treated according to the specific features of the different liquidity transfer types by the Liquidity Operations module.

Liquidity transfers between an RTGS system and T2S are based on the exchange of inbound and outbound liquidity transfers and on the use of dedicated transit accounts (both in the RTGS system and in T2S) managed by the Outbound Information Management module in order to enable the other system to align its accounting.

At the end of the settlement day, liquidity available on T2S Dedicated Cash Accounts is automatically transferred to the relevant RTGS accounts and the specific end-of-day procedures are implemented by the NCB Business Procedures module.

#### 2.3.5.1. Liquidity Operations

This module ensures the checking and management of liquidity transfer orders between two T2S Dedicated Cash Accounts or towards RTGS system (and vice versa), taking notably into account the specific features of the different transfer types.

#### 2.3.5.2. Outbound Information Management

Liquidity transfers between an RTGS system and T2S require the use of technical transit accounts. This module manages inbound and outbound liquidity transfers in order to enable the other system to align its accounting. Moreover, it provides information on special booking events (ceiling, floor, and partial/no execution) to T2S Actors.

#### 2.3.5.3. NCB Business Procedures

This module is responsible for the end-of-day liquidity transfers between T2S and an RTGS system. It is in charge of the automated transfer of surplus liquidity at the end of the day as well as triggering linked liquidity transactions in case of insufficient liquidity (Pending Intraday Credit). Additionally it triggers the bookings at the end-of-day between the RTGS dedicated transit accounts and the “T2S technical account EOD”.

### 2.3.6. Statistics, Queries, Reports and Archive

This domain includes modules proposing data exploration services to the T2S System Users according to their needs in terms of time scope, nature of data accessed (detailed or aggregated), of flexibility of the tools, and of response time.

#### 2.3.6.1. Statistical Information

The Statistical Information module is expected to provide T2S System Users (i.e. the T2S operator and, on an optional basis, CSDs and NCBs) with a business intelligence tool to be used for statistical analysis and as a decision support system.

It stores information on accounts (including position changes and event information), on instructions and on queries and reports (including volumes generated).

The scope of this module is twofold:

- To provide statistics to the T2S operator and the CSDs for some operational purpose, on the level of use of the different components of the platform over time, to support the proper management of the system. Such statistics are based on a “short term” repository including data up to three months and the whole instruction life history (including all status changes and relevant timestamps) .

- To offer to CSDs and NCBs on an optional basis wider scope statistics for analysis and regulatory reporting purposes. These statistics are based on a “long term” repository storing data with their final status. These statistics are available on data older than three months.

Both repositories are separated from the live data repositories, in order to provide an easy access to high quality and business oriented data without the risk of impacting the performance of the operational settlement environment.

In the present document, both dimensions are covered within the scope of the single Statistical Information module. Nevertheless, this general description will be followed, during the next phase of the project, by detailed specifications aiming at serving as a basis of the design of the technical (development and infrastructure) solution(s): (i) one covering the statistics needed for the monitoring and management of the platform by the T2S Operator and (ii) the second covering wider scope statistics for analysis and regulatory reporting purposes by CSDs and NCBs, on an optional basis.

The Statistical Information module provides functions to perform statistical query and reporting and multi-dimensional analysis.

The specific set of available statistical data and functions depends on the specific privileges of each T2S System User.

### 2.3.6.2. Query Management

The Query Management module allows different categories of real-time queries and historical queries on the production data (e. g. settlement instructions, securities positions, cash balances, static data, and audit trail). All requested data are extracted from the respective data stores and then delivered back to the Interface domain.

### 2.3.6.3. Report Management

This module provides T2S Actors with a number of reports for periodical information (settlement instructions, balance and static data reports) which, however, do not have to cover the regulatory reporting. These reports are set up as XML messages and comply to the largest possible extent with ISO 20022 standard.

All reports are available for all CSDs in T2S, T2S parties and NCBs. Reports can be sent to CSDs and directly connected T2S parties, containing information on one or several accounts, considering the privileges of the requesting Party. T2S reports can either be created based on a business event or be sent at a fixed time.

### 2.3.6.4. Legal Archiving

The Legal Archiving module aims at storing for a given period static data (including revisions and history) and transactional data . The module is triggered daily during the maintenance window, and on arrival of a request from the Interface domain.

## 2.3.7. Operational Services

This domain includes modules providing functions specific to the T2S operational teams.

### 2.3.7.1. Operational Monitoring

The aim of this module is to support the T2S Operator and, for some specific tasks, other T2S System Users (e.g. online access to the Trouble Management System for CSDs and authorized T2S parties) in the monitoring of T2S, from two different angles:

- The operational monitoring for the detection of functional or operational problems in real-time, the monitoring related to the SLA indicators, and the information provisioning for crisis management scenarios;
- The technical monitoring for the detection of hardware and software problems via real-time monitoring of all the technical components involved in the processing, including the network connections.

Furthermore, this module provides an overview of the message flows in the whole system to the T2S operator.

### 2.3.7.2. Scheduling

This module contains a set of functions for the management of operating day events and related business processes. The current business date event schedule can be changed at run-time, in order to insert, update, time-shift and close an event instance or a set of events. The broad categories of events are EOD/SOD events, End of cycle events, Maintenance events and Dynamic events.

### 2.3.7.3. Billing

This module automatically or on request produces monthly bills containing all billable events (e.g. events related to the lifecycle of an instruction), fixed and variable fees. At the end of a billing period, an invoice is sent to the CSDs and sums up all the relevant billing information per T2S Party. All invoices are stored electronically and are available for later inquiries.

### 2.3.7.4. Data Migration

The Data Migration module provides the migration functionality which will allow the CSDs and the NCBs to automatically transfer the major part of relevant data (e.g. securities account data, party master data, securities positions, securities master data) from the securities settlement systems of the respective CSD and relevant data from NCBs to T2S. For the transfer and upload of the migration data any kind of means is envisaged: flat file, excel file, paper and in any case GUI to key in or correct static data. A standard fall-back plan is established, made available before the first migration period and the fall-back plan and the roll-back procedures are tested before the beginning of the migration.

The Data Migration module is used for setting up test environments before go-live of T2S and before an additional CSD joins T2S (e.g. in later migration windows). There is no migration of any historical data of the CSDs.

# 3. Technical description

## 3.1. Service level assumptions

The following assumptions are used to design the application and to scale the infrastructure:

### 3.1.1. Volumetric assumptions

This chapter describes the main assumptions on T2S volumes. The figures include volumes for Central Securities Depositories (CSDs) of the Eurosystem plus the total settled volumes of UK, Denmark, Sweden, Estonia, Latvia, Lithuania and Romania and will be amended if needed during the project phase. For the present volumetric forecasts, T2S considered the year 2008 figures of the ECB Bluebook 2009 and complementary elements communicated by CSDs and National User Groups (NUGs) to estimate yearly trend and peak days.

By the year 2014, the annual transactions volume[6] should be around 268 966 007, with an average daily volume[7] of 1 042 504 operations. Other figures, like the average day[8] and night[9] time volumes, peak day[10] and night time workloads, have also been taken in consideration for a first estimation of the technical resource needs, in terms of processing power and storage. However, from a technical point of view, the T2S infrastructure and application are scalable to deal with future requested changes in the above listed figures, but in this case, a new cost assessment will be needed.

### 3.1.2. Availability

The planned level of availability defined by the URD for T2S is above 99.7%, calculated on annual basis **{T2S.20.320}**. The ability of T2S to satisfy this requirement will be assessed in the context of the business continuity tests (refer to § 6.4.3) as well as other resilience tests.

According to the Information Technology Infrastructure Library (ITIL®), availability is “the ability of a configuration item or IT service to perform its agreed function when required. Reliability, maintainability, serviceability, performance, and security determine availability. The calculation of availability is usually on a percentage basis with reference to an agreed service time and downtime. It is a best practice to calculate availability using measurements of the business output of the IT Service.”

[6] Countries included: Euro-Zone, United Kingdom, Denmark, Sweden, Estonia, Latvia, Lithuania, Romania.

[7] Average daily volume: Annual Volume of Transactions divided by 258 operating days in a year.

[8] Average day time volume: Day time volume is estimated to be 30% of the daily total.

[9] Average night time volume: Night time volume is estimated to be 90% of the daily total.

[10] Peak day workload: Peak day workload is calculated as the average daily volume multiplied by a peak load factor which is provided in most markets by CSDs.

In compliance with ITIL® standards, the main Availability criteria that T2S has to fulfil can be classified as described hereafter:

- Reliability;
- Maintainability;
- Serviceability;
- Performance;
- Security.

### 3.1.3. Performances

T2S is a business critical system that will be used by different organisations in different countries and therefore must provide a high level of performance.

In particular, T2S is able to handle the estimated settlement volume running real-time settlement in parallel to a continuous optimisation algorithm without degradation of the service level **{T2S.17.030} {T2S.17.040}** and does not have any performance impact on TARGET2 activities, and vice versa **{T2S.17.050}**.

In compliance with the response time requirements defined in the URD,

- T2S responds to 95% of the basic queries[11] User-to-Application (U2A) or Application-to-Application (A2A) mode within 3 seconds **{T2S.17.140}**;
- Any data to be created, modified, deleted via the user to application interface is updated in real time **{T2S.17.160}**.

Business monitoring tools will check that T2S is compliant with the Service Level Agreement (SLA) and produce corresponding reports.

Performances and throughput will be assessed in the context of the stress test campaign).

## 3.2. Technical design

### 3.2.1. Application design

#### 3.2.1.1. Characteristics of the platform

The T2S system makes use of the infrastructural services currently available for TARGET2 **{T2S.19.010}.**

[11] Queries to retrieve a single object (status of one instruction, static data for one ISIN etc.) Any other query can be considered as a complex query.

Therefore the T2S “core business” applications (e.g. Life Cycle Management and Settlement), running on the mainframe, using IMS/DC as a transaction manager and DB2 as relational database management system. The T2S “front-end application” (U2A interface) is based on the Java Enterprise Edition platform, using an IBM WebSphere application server. XML facilities for message parsing, transformation and routing will handle the A2A traffic.

Whenever possible, a single data-model, common to all the application modules, is implemented in order to avoid data replication. Nevertheless in some circumstances, some kind of data replication or data model separation can prove to be a valid option to improve the performances.

Communication with the end users and to their IT systems is done via dedicated networks and network providers using standard communication technologies and protocols which adhere to the ISO 20022 XML standard. {T2S.19.230}

The Graphical User Interface (GUI) features uniform screens which provide a consistent look-and-feel to the end user.

### 3.2.1.2. Main development principles

From the application point of view, the User Requirements for the T2S system should fulfil the following main development principles:

- The system must meet high performance and high volume requirements and thus must be scalable and enable parallel processing **{T2S.19.180} {T2S.19.100};**
- The system requires highly efficient optimisation algorithms for settlement purposes **{T2S.08.040} {T2S.08.050};**
- The system must be designed to minimise the risk of contentions between different processes;
- Parameterisation at CSD or even at user level, in order to cope with non-harmonised features but also in order to be able to implement user roles **{T2S.04.010};**
- The system must provide strong security and business continuity requirements **{T2S.18.*} {T2S.20.*};**
- Requirement for integration with other ESCB systems (e.g. TARGET2 for functions such as cash transfer between own accounts) **{T2S.06.440} {T2S.06.450} {T2S.03.070}**

The main development principles are defined to cope with these highly demanding requirements:

First the application is composed, at the lowest level of granularity, of components loosely coupled in order to benefit at the maximum of parallel processing capabilities. These components interact with a set of specifically designed interfaces and are synchronised, when needed, by a scheduler.

Special care is taken for the data base technical design to cope with Input/Output (I/O) components needs.

Finally, specific security features are implemented at the application level to have a fine control of information access and update.

### Components of the application

The T2S application is comprised of a set of modular and independent technical components. Each component is dedicated to the fulfilment of a specific task. The actual choice of technology used for the implementation (i.e. the programming languages) and the hosting (i.e. the runtime environments) of the components are based on the "T2 on T2S" concept, the functional and non-functional User Requirements and follow a best-fit approach.

All components which make up the T2S system are loosely coupled and are capable of acting independently from each other. Each component offers functions to other components via dedicated interfaces and hides their internal data representation and implementation details behind so called facades **{T2S.19.130}.**

### Database design and storage

In general, the design of the data model will follow a relational approach. As the T2S system is required to be capable of dealing with a large amount of data and the efficient and effective processing of very high numbers of transactions, special attention must be paid to the design of the technical database model and the storage of data. In particular, all efforts put into an optimised implementation provide a great benefit for the most critical parts of the whole application (e.g. the settlement engine and the optimisation algorithms).

The design of the database on both a logical and physical level takes into account the needs to guarantee performance consistent with the SLA and the goals of the service provisioning. The technical design of the database relies on a central repository for the system data (meta data) and is optimised to deal with data accessed in real-time and data used in a less frequent way **{T2S.19.160}**.

Each domain maintains a dedicated part of the technical data model and the physical database according to the business processes belonging to this domain. Data residing in a different domain can be accessed via dedicated technical interfaces. The data integrity is ensured by the functional design of the application (data ownership: eg. SD data can only be changed by SD domain).

### Application security

T2S implements a Role Based Access Control (RBAC) to manage the role of the user and to check that the sender of an incoming T2S query or instruction is entitled to perform T2S related business operations consistently with the business roles assigned to him/her.

The application security design of the T2S system foresees a highly flexible and powerful management and enforcement of user roles. It enables authorised end users to setup their own user roles to suit their needs.

Additional permission checks are implemented and enforced to ensure the data is always read, updated and displayed according to the prevailing business rules.

Audit logs record all user activities, exceptions and information security events are collected and kept for an agreed period to assist in any future investigations, and for system and access control monitoring under the control of the system owner.

Access to the T2S system, the programme executables and the data itself by internal users is restricted by RACF (Resource Access Control Facility) and other state of the art technologies.

In conjunction with the security mechanisms provided by the chosen infrastructure, this leads to a highly secured software application.

The enforcement of security mechanisms is based on standardised industry-proven mechanisms. This allows the usage of a trusted relationship with third party providers as well as methods for user identification, security and permission checks provided by the T2S system itself.

All communication with the user is encrypted using state-of-the-art strong encryption techniques. Furthermore, in case of U2A, the enforcement of the roles is based on checks on the server side as well as on the client side. Additional client-side checks improve the overall usability and user experience and allow for personalised and role-based views of the application for the user (i.e. users are only allowed to see and access functionalities in the front-end for which they own the appropriate roles).

### 3.2.1.3. High level application design

#### Application design overview

The application is designed to enable easy scalability on both the hardware/system level and at the software level.

The hardware/system level scalability is achieved by the use of separate logical partitions (LPAR) in a parallel Sysplex[12] environment, adding more processors (CPU) or even more machines in order to match the increasing requirements related to processing performance and throughput.

The software level scalability is achieved by an application design featuring loosely coupled software components that makes use of the additional CPUs available and allows the parallel execution of multiple instances of certain modules or functions. This parallelisation is necessary in order to gain the full range of benefits provided by the hardware/system level scalability.

[12] **Parallel Sysplex** provides horizontal scaling with a cluster of IBM mainframes acting together in a single system image. It combines data sharing (same disk under control of sharing structures in a Coupling Facility) and parallel computing to allow a cluster of up to 32 computers to share a workload for high performance and high availability.

The different components of the application are developed with special focus on performance, throughput and scalability. Reusability, demarcation of responsibility and encapsulation of functionality also play a major part in the overall application design.

### Processing principles

The T2S system supports straight-through-processing (STP) capabilities for the processing of all instructions. This means that the system validates matches and settles settlement instructions without the need of manual intervention.

The design of the system foresees the usage of a set of technical interface technologies that enables a flow of information through the system as seamlessly and efficiently as possible.

By the utilisation of logging and auditing functionalities all changes done within the system are traceable and the flow of data through the system is made transparent.

Every step of processing occurs under the supervision of a transactional monitor and thus is covered by transactions. Consequently, in case of an unforeseen failure, all previous changes made to the data are rolled back instantly and the system is left in a consistent state.

### Interfaces

The T2S system requires a number of interfaces internally (to connect the internal modules with one another) and externally (to communicate with the outside world).

The design of T2S foresees to minimise the number and nature of interface mechanisms used for both internal and external communications. For example, a unique communication mechanism among all the modules is used for all asynchronous communication requirements in order to achieve an easy maintainable application. The communication mechanism takes into account the performance and throughput requirements, and all interfaces are implemented by using robust and reliable market standard technology.

T2S utilises and provides asynchronous and synchronous ways of communication, both for the outside world (i.e. to end users like CSDs, NCBs, directly connected T2S parties) and internally.

### External interfaces

The Interface domain is responsible for handling the bi-directional communication with the outside world, brokering of incoming and outgoing communication traffic.

Many different types of interfaces and connectivity requirements exist, like for example:

- Real time synchronous requests (user interface, queries);
- Asynchronous batch processing (sending messages to T2S in batch);
- Asynchronous message sending and receiving.

- File transfer

All external communication is encrypted by the means of TLS/SSL (transport layer security / secure socket layer). Such encryption prevents fraudulent activities like eavesdropping, tampering with data and attempts of forgery while data is in transit from its source to its destination. Additional security mechanisms ensure that both parties in such communication (i.e. the client and the T2S system) identify themselves to each other, so each party knows with whom it is communicating.

Communication with the outside world is achieved by providing dedicated interfaces for enabling end users (T2S actors) and their IT systems to interact with the T2S system in both User-to-Application (U2A) and Application-to-Application (A2A) mode.

## 3.2.2. Infrastructure design

### 3.2.2.1. Infrastructure summary description

T2S infrastructure is deployed over three Regions. Two Regions (Region 1 – Banca d'Italia – and Region 2 - Deutsche Bundesbank) host the T2S core business applications (e.g. instructions settlement); the third Region (Banque De France – Region 3) hosts other T2S functions (e.g. Legal Archiving and Statistical Reports provisioning). To allow continuous operations without service interruptions (e.g. in the case of a power outage), each of the 3 regions consists of a primary and a secondary site which run independently from each other. Each site is established as a high availability data-centre for operations (e.g. redundant connections for power supply and use of Uninterruptible Power Supply (UPS).

The workload of the core business applications is distributed between Regions 1 and 2; in fact, while Region 1 is hosting T2S production, Region 2 is hosting T2S Test &Training and vice-versa. Regular swaps ("rotation") ensure proper precaution against regional disaster and keep technical and operational staff skilled in each region. Rotation activities in Regions 1 and 2 do not impact systems in Region 3. The technical independency between Target2 production and T2S production is assured by the fact that they always run in different regions.

The system and the application software in Regions 1 and 2 are kept aligned by means of a functionality of the disk storage subsystem (asynchronous remote copy). After each rotation, the system is able to restart with the same customisation (i.e. naming convention, security policies, management rules etc.).

Like TARGET2, T2S offers its users a single interface, meaning they do not perceive in which Region the service is running. Moreover, rotation is fully invisible to CSDs, National Central Banks (NCBs), users and market infrastructures, thus no configuration changes in customer systems are envisaged.

Different logical environments support maintenance, development, integration, acceptance, testing and production of the T2S system.

The main components of the architecture envisaged for T2S are outlined in the following paragraphs according to the hosting regions.

### 3.2.2.2. Main components of Region 1 / Region 2

#### Central Processing System

All logical environments of the T2S core system are hosted by a central server (one per site) running z/OS Operating System, which ensures full coverage of the demanding workload and compliance with the availability and scalability requirements.

A Parallel Sysplex configuration (multiple independent logical partitions working concurrently in cooperative mode, sharing data with high performance read/write operations and total data integrity) will be implemented in case a single logical partition is not able to manage the whole workload and the system software maintenance without impacting the availability.

#### Open Systems

Regions 1 and 2 also host Open Systems providing a set of specialized services, e.g.:

- T2S services for the provision of statistics (based on the short term storage i.e. up to 90 days) in order to complement the operational monitoring tools to properly manage the system
- Operational Monitoring System for real-time detection of functional or operational problems and monitoring of SLA indicators;
- Technical Monitoring System, based on continuous monitoring of the platform’s technical components and an alerting system to highlight any unusual occurrences;
- Trouble Management System (TMS) handling the workflow for any incidents or problems and reporting on the respective status; the on-line access to the tool is provided for reporting purposes to CSDs and T2S parties authorized by CSDs;

The Open Systems will also host the functionalities relating to the Network Gateway.

#### Storage Subsystems

Regions 1 and 2 (both primary and secondary sites) can rely on a Storage Area Network (SAN) and a set of disk and tape subsystems.

T2S storage infrastructure is completely separated and thus fully independent of the domestic storage infrastructure of Banca d’Italia and Deutsche Bundesbank. All components of this storage infrastructure are installed and configured following the same standards in the 4 sites. T2S SAN provides basic connectivity to z/OS systems, Open systems, Tape subsystems (for both z/OS and

Open systems), Intra-region Synchronous replication for disk subsystems, and Inter-region Replication for both disk and tape subsystems.

#### 3.2.2.3. Main components of Region 3

**Open Systems**

The Legal Archiving function and the provision of statistical reports are hosted on Open systems deployed at the Banque de France Region. Here are stored all business operations performed by T2S legal archiving and statistical purposes, enabling the provision of statistical reports, the retrieval of data on user request and purge of archived data after its expiration period. T2S archiving is foreseen to draw as much as possible on the existing TARGET2 infrastructure. Logical environments are deployed for production, development, integration, internal acceptance and recovery purposes.

Access of T2S participants to the archiving system only takes place through the Network interface.

**Storage**

Like in Regions 1 and 2, both primary and secondary site of this Region rely on a Storage Area Network (SAN) and on a set of disk and tape subsystems. All components of the storage infrastructure are installed and configured following the same standards in the two sites. This includes redundant connections to power supply and use of UPSs.

Region 3 also hosts on its Open systems T2S services for the provision of statistical reports (based on the long term storage i.e. more than 90 days) to be offered to T2S users on optional basis. These components will lean as much as possible on the existing TARGET2 infrastructure.

### 3.2.3. Connectivity services

#### 3.2.3.1. Network Interface

T2S Network Interface is a set of hardware and software elements allowing interactions between the various T2S actors (CSDs, NCBs, T2S parties, ECB, other collateral managers), the systems (CCBM2, TARGET2, other RTGS systems and collateral management systems), and the relevant T2S modules, both for inbound and outbound communication. The Network Interface is the functional layer directly attached to the External Networks and consists of two basic components, the Network Gateway (more external one, and direct front-end to the External Networks) and the Interface Subsystem (internal one).

From a logical point of view, each access via External Networks passes through the Network Gateway and Interface Subsystem layers.

T2S Network Interface handles communication in browser-based U2A mode and in A2A mode. Standards in use will be HTTP/HTTPS (HyperText Transfer Protocol) for U2A interactions and XML for the A2A mode. All communications established through the Network Interface are compliant with the ISO20022/UNIFI standard, and also with Giovannini protocol's recommendations in the particular case of file transfers.

The Network Gateway is intended to increase the security of the T2S system by operating a logical separation between the networks and infrastructure. The Interface Subsystem mainly supports the decoupling of the internal T2S service protocols from the external communication protocols.

### 3.2.3.2. External networks

Although no compelling need can be identified for T2S to take any commitment on connectivity to T2S beyond its own network access point within its data centres, the Eurosystem recognizes that network connectivity has an impact on the overall T2S service and on business continuity. In case of an outage in the network or in the interface, the user may perceive this as a T2S service unavailability. Furthermore, inter-region rotation and regional disaster recovery both require the network providers to implement special arrangements to make them transparent to the users. For these reasons, the specification by T2S of an appropriate set of value-added network services is very important. These services are supplied in part by the network providers, and in part by specific arrangements on the T2S platform.

T2S shall ensure the confidentiality, authenticity and integrity of the traffic in transit and guarantees the authentication of end-devices**.**

For this purpose, the "basic" value-added network services are defined as follows

1. closed user group management;
2. access control to guarantee connections for allowed users only;
3. User authentication for external connections;
4. non-repudiation of sent messages;

The communication services provided by network providers are U2A (User to Application) and A2A (Application to Application). A2A supports both guaranteed delivery, even if the receiver is off-line, and real time transmission, it operates in push and pull mode for both files and messages transfers.

They are expected to scale up or down according to central T2S application requirements. Security, resilience and coverage objectives will be included in the SLA.

### 3.2.3.3. Internal Network

The existing Internal Network (3CBNet), connecting the six operational sites of the SSP in the 3 Regions, and the related DMZ interface**,** have been enhanced with network links to provide a stable network connection for Banco de España teams too. This enhanced network (4CBNet) is to be considered as a unique telecommunication and security infrastructure to be upgraded and managed as a whole.

Five main types of flows are foreseen:

- storage;
- external network;
- traffic from external networks to region3 for the access to long term statistics and legal archiving;
- development and file transfer;
- voice and video over IP;
- management, monitoring and internal support

### 3.2.3.4. User Identification and Access Management

T2S provides specific services for user identification and access management, featuring centralised security policy and security logging, in compliance with the ESCB Password Policy. Authentication and Access Management are performed by the Network Gateway on the basis of digital certificates, relying on Public Key Infrastructure (PKI) technology. In addition to the identity management, T2S offers Role Based Access Control (RBAC) with different user roles granting access to the various business operations .

Access (successful or not) to T2S internal components (business and administrative use also) is logged to the maximum convenient extent.

Connections from specific locations and equipment are secured based on certificate identification mechanisms.

Different zones are defined inside T2S network domain, each segregate from the others depending on the security level required.

Various routing controls are implemented in T2S. The use of dynamic routing protocols is limited to the internal network. The connections with the external networks handle different controls of the routing protocols and border firewalls.

.

## 3.2.4. Business continuity model

### 3.2.4.1. Introduction

Business Continuity is the ability to adapt and respond to risks in order to maintain continuous business operations. The provision of Business Continuity involves three main aspects:

- High availability is the capability to guarantee a service regardless of local failures in business processes, physical facilities and IT hardware or software;

- Allowing Continuous operations is the capability to guarantee a service also during scheduled backups or planned maintenance;
- Disaster Recovery is the capability to recover a data centre at a different site, in the event a disaster destroys the primary site or otherwise makes it inoperable. The distinctive feature of a disaster recovery solution is that processing resumes at a different site and on different hardware.

### 3.2.4.2. Business continuity design for Region1 /Region 2

Like in TARGET2, the architecture of T2S core system is based on the concept “2 regions / 4 sites”.

The four sites are fully equivalent and each of them has to be equipped with the same technical resources: processor, storage, network interface, software, etc.

The business continuity design involves different levels of the overall architecture requiring various technical solutions. The main elements for the design are:

- **Redundant hardware components**. Hardware systems will have redundant components in terms of power supply, memory and processor to assure service continuity also in case of failure of a single component ;
- **Scalable central processing system**. Parallel Sysplex implementation assures dynamic load balancing and additional business continuity in case of failure of a single logical partition ;
- **Cluster configuration** for Open Systems running critical applications assures continuous service ;
- **Storage Area Network Extension**. An extended SAN increases the geographic distance allowed for SAN storage operations, in particular for data replication and copy. This is especially relevant for the protection of data in the event of disaster at the primary site ;
- **Recovery Technologies**. The following technologies support data recovery with increasing effectiveness (minimization of data loss):
    - Tape backup and restoration;
    - Periodic replication and backups;
    - Asynchronous replication for disk subsystems;
    - Synchronous replication for disk subsystems

**Data Replication and disaster recovery scenarios**

Data replication has two primary objectives:

- To copy data to a recovery site and minimize the RPO (Recovery Point Objective);

- To enable rapid restoration.

Disk-based replication uses modern intelligent storage arrays, which can be equipped with data replication software. Replication is performed transparently to the connected servers (hosts) without additional processing overhead. Replication products can be categorized as synchronous or asynchronous:

- **Asynchronous replication** is a nearly real-time replication method in which the data is replicated to the remote array some time after the write operation is acknowledged as complete to the host. That means application performance is not impacted but loss of replicated data is possible (RPO >0). The system can therefore locate the remote array virtually at any distance away from the primary data centre without any impact on performance, but the bigger the distance, the greater the risk of data loss in case of disaster;
- **Synchronous replication** is a real-time replication method in which the data is written to the local storage array and the remote array before the write operation is considered complete or acknowledged to the host (zero data loss or zero RPO).

Synchronous and asynchronous replications allow fulfilling T2S business continuity requirements.

In detail, synchronous and asynchronous replications are active independently and simultaneously for the various T2S environments. Replication is synchronous between primary and secondary site of each region and asynchronous between Region 1 and Region 2.

In order to enable the system to restart on a remote site in the event of disaster, consistency between the two remote copies (synchronous and asynchronous) is guaranteed by the storage infrastructure.

In the case of a regional disaster, some data may be lost due to the above-mentioned asynchronous replication mechanism. The recovery of the delta data loss would be managed with help of the users or by the network providers (if these offer a specific retrieval service), provided that clear requirements are expressed in this regard.

### 3.2.4.3. Business continuity model for Region 3

As the Legal Archiving and statistical reporting are less business critical than the other T2S components, the business continuity model follows the “1 region/2 sites” scheme. The internal mechanism of the storage units covers up data loss, in case of hardware problems (RAID technology). Major failures are handled through intra-region recovery, therefore data is transferred daily from primary to secondary site. Possible lost data in the secondary site will be retrieved from Region 1/2. For the SAN, standard replication mechanisms (database replication and disks replication) will be used depending on the amount of data to replicate.

#### Backup (storage on Tapes)

Backup is provided with standard tools and methods.

For security reasons, tapes are duplicated; one copy is kept at the premises of a Banque de France external provider specialized in this activity.

In the case of a regional disaster causing unavailability of the Legal Archiving systems, the business-critical components of T2S are able to operate fully without them.

# 4. Operational phase description

## 4.1. Service Desk and support organisation

### 4.1.1. Service desk

According to UR **{T2S.20.040}**, the T2S service provider – i.e. the Eurosystem – is expected to establish a T2S Service Desk acting as a single contact point for CSDs. The precise implementation of this requirement will be defined in the context of the operational framework.

Within and for the benefit of the Eurosystem, the 4CB – in their capacity of T2S operator – will establish such T2S Service Desk which is meant to act as a single contact point for any kind of operational and technical issues for both live and test environments. Considering the envisaged system functioning hours for the live production (see above) the Service Desk will be available round the clock but with different availability and reaction times depending on the time of the day. The Service Desk consists of a unique team spanned over two sites in Banca d'Italia and in Bundesbank and based on the so-called active-active service desk concept. The latter business model entails that while one of the regions where the Service Desk is established follows the live environment, the other has the responsibility for the Test and Training. At the same time each of them acts also as a back-up for the other. Such model allows on one side to always have the whole team in both regions fully in touch with the day-to-day business and, on the other, to save cost related to a secondary site office for the Service Desk. In fact, like the operational staff members themselves, offices and equipment will be backed-up in the other region.

In order to fulfil its duties, the Service Desk will be equipped with a number of tools such as operational and technical monitors, Trouble Management System, document management system, cooperative applications (document management, advanced instant messaging, shared desktop)and telecommunication systems (teleconference, videoconference, satellite phones)[13].

The T2S Service Desk guarantees a response time to the issues submitted by the CSDs and other parties on which it will be committed according to the service level agreement. Such response time varies according to the time of the day and the severity of the issue **{T2S.20.050}.**

T2S Service Desk support is conducted only in English. Therefore all related communications using telephone, fax, e-mail or other means are in English only **{T2S.20.080}**.

In order to be able to trace all issues submitted by CSDs and other T2S parties, the T2S Service Desk uses a Trouble Management System (TMS) through which the whole workflow of any topic dealt with therein is covered. This gives people enabled to access such system a wide knowledge on the status

[13] A non-exhaustive list can be found in chapter 3.2.2.2 (Main components of Region 1 / Region 2) under sub-chapter "Open Systems".

of the incident/problem/service request as well as on parties involved, solutions and other details **{T2S.20.070}**. CSDs and T2S parties authorised by the CSDs have selected online access to the above information. **{T2S.20.080}.**

The Eurosystem reports to the authorised parties on the performance of T2S vis-à-vis the agreed service level (SLA reporting). In order to cope with such requirement, the T2S Service Desk has access to the whole T2S database and has query tools available in order to concretely fulfil the requirement. The number of days which have to be kept available on line for such purpose will be defined at a later stage.

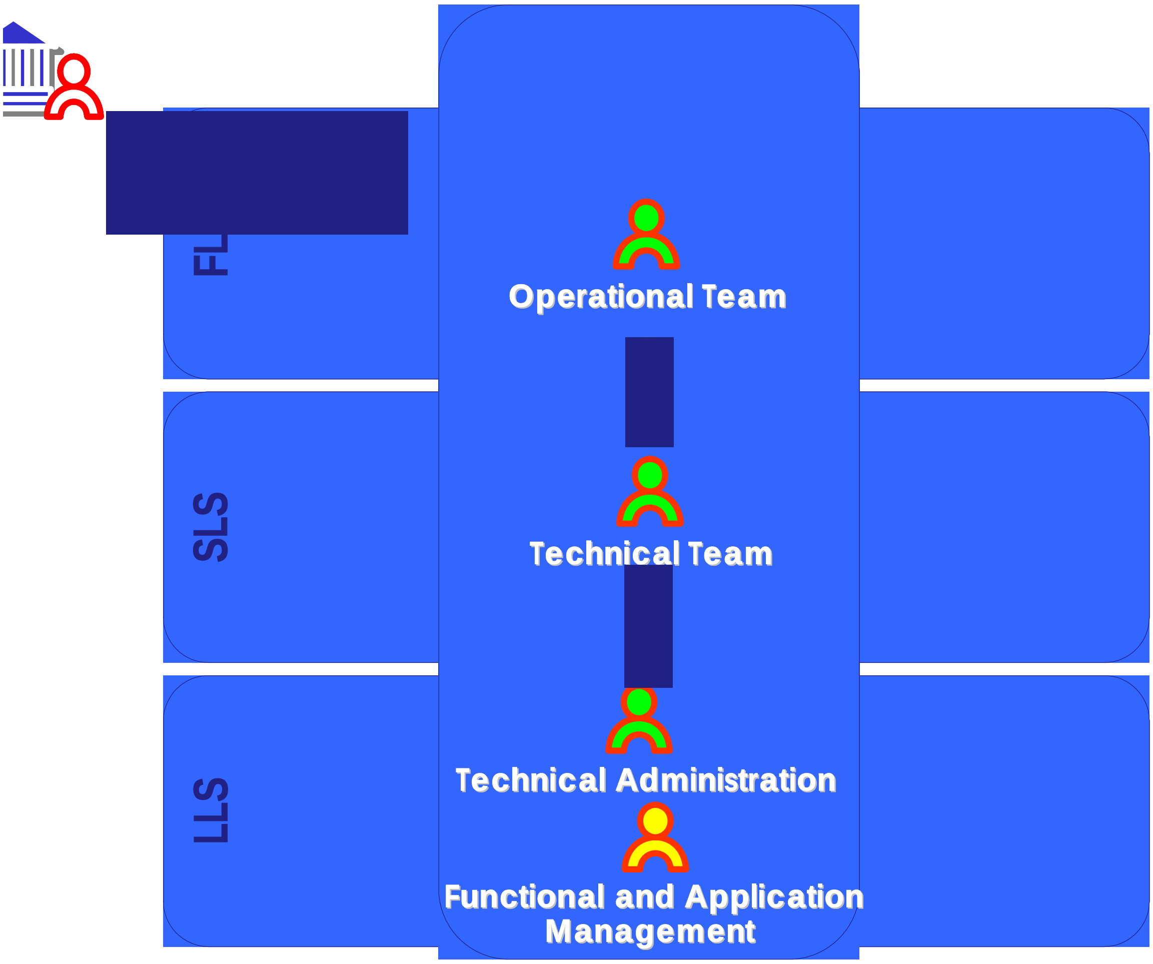
On a monthly basis the T2S Service Desk reports to the CSDs on the type and number of enquiries received, their counterpart, the solution given, the number of unresolved enquiries and the time elapsed **{T2S.20.090} {T2S.20.100}**. The T2S Service Desk is in charge for producing the reports (including key performance indicators) as defined in the Service Level Agreement which have to be provided to the governance structure and to the T2S users **{T2S.20.110}.**

A T2S Manual of Procedures (T2SMOP) describes all procedures relevant in normal and abnormal situations.

### 4.1.2. 4CB Support organisation

In order for the T2S Service Desk to be able to provide the required level of support, the Eurosystem has in place an organisational structure that is commensurate to the operational needs, which is identified by the Subgroup on Operational Issues, established by the T2S Advisory Group.

Such support organisation, provided by the 4CB, is based on three levels as shown in the picture below.



The Operational Team (OT) is responsible for the First Level of Support (FLS) and acts as a single contact point for any kind of operational and technical requests for both live and test environments. The Technical Team (TT) covers the Second Level of Support (SLS) and is composed of a group of hardware and software specialists in charge of managing the day-by-day T2S infrastructure and applications. Moreover, the Technical Team is in charge of providing technical help desk functionalities vis-à-vis the FLS. The Technical Administration and the Functional and Application Management are composed of experts at the 4CB for both infrastructural and software issues who act as Last Level Support vis-à-vis the FLS and SLS for those issues requiring specific and adequate expertise.

The relationships among the three support groups are governed by bilateral agreements aiming at ensuring at any time the consistency with the Service Level Agreement as far as both the services provided and the reaction times are concerned.

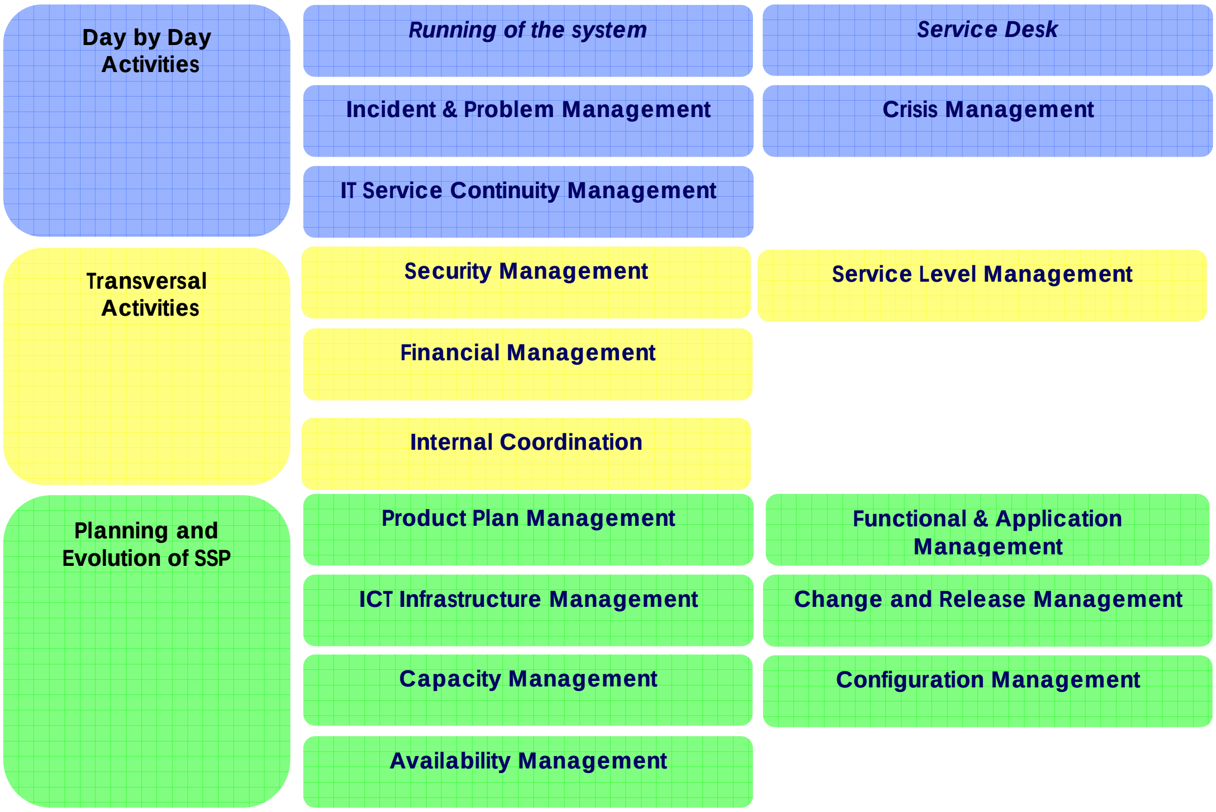
## 4.2. Service Management

T2S is technically built on the SSP where the TARGET2 service is also located and is managed following the same organisational and procedural schemes, thus allowing for a maximum of synergies between the two systems. Contrary to TARGET2, T2S is open to different currencies, thus enlarging its scope and, consequently, the risks linked to possible partial or complete system unavailability. To this extent T2S has to be able to cope with a variety of unpredictable events, ranging from local equipment failure to region-wide disasters and, owing to such requirement, also has to be integrated de facto into the crisis management organisation set up by the Eurosystem for TARGET2.

The technical platform on which the system is planned to run as well as the procedures covering all the different aspects need skilled teams supporting it on a day-to-day basis. The 4CB organisation, largely derived from the 3CB model for TARGET2, constitutes a solid basis for the very high levels of service expected from a platform as critical to business as T2S.

The T2S activities are broken down into generic processes, based on international standards (i.e. ITIL® framework) **{T2S.20.010}.**

They can be split into three main categories, namely the day-to-day activities, the transversal activities and the planning and evolution activities of T2S.



## 4.3. Operating day and calendar

T2S operating day consists in a sequence of events where each event triggers a specific schedule status which corresponds to the specific ongoing period or process of the settlement day. This is done in a sequential order **{T2S.03.010}**.

The T2S URD (v4.2) provides, today, an indicative settlement processing timetable. This timetable covers night and day-time settlement, the start- and end-of-day periods and the most important deadlines thereof **{T2S.03.030 – T2S.03.300}.** Further consultation with the T2S relevant stakeholders will allow for the stabilisation of this timetable. The implementation of the timing of the events and statuses as parameters in the T2S IT platform, allows for a flexible IT architecture which does not impede further business analysis and consultation as required in parallel.

Although it is understood that the current URD requirements were agreed on the basis of best market practice and minimum interference with the securities settlement industry requirements, further clarification is required as to the exact impact on the liquidity provision needed to support such requirements (as currently in the T2S URD v4.2) and the need for aligning T2S and TARGET2 critical times and events. The cost implications of any agreement on these topics both for the support services of the T2S operator and the operational costs of the involved stakeholders (CSDs, their participants and NCBs) require further clarification.

The events of the operating day are assigned a **planned time**, which corresponds to the standard timing in which the event is normally triggered and is used as a default **{T2S.03.016}**. In case an event has to be triggered at a different time than the planned one, the T2S operator can adjust the revised time in the table "T2S operating day", which corresponds to the one envisaged for that specific day leaving the planned time unchanged **{T2S.03.017}**. In addition, the T2S Operator might have to change the planned time as well due to special circumstances. In such cases this is done according to the standard procedures agreed with the users. When an event takes actually place it is assigned an effective time **{T2S.03.018}**. The three times (planned, revised and effective) are visible by the users in the relevant ICM[14] screen.

- T2S opens the new business date in the evening of the previous one at 18:45 **{T2S.03.020}**. The opening of the new business day can be checked by the users on screens in U2A mode and is notified by an automated message broadcast **{T2S.13.136}**. After the new business day event is triggered, the Start-Of-Day period begins. The aim of this phase is to prepare the events of the new business day and in particular of the upcoming night-time settlement **{T2S.03.030**}. During the SoD period, the settlement instructions eligible for settlement during the new business day are identified and validated against the static data which are becoming valid as from the new business day. The settlement instructions are valuated using the market prices of the previous business day. During the SOD liquidity transfers from T2 and other RTGS systems (whose currencies are managed in T2S) to T2S are executed either by standing liquidity transfer orders or on an ad hoc basis via immediate liquidity transfer orders.
- There are no restrictions on the transactions types which can be settled during the NTS **{T2S.03.080}**. Settlement is attempted on transactions following a definite sequence.

The duration and the number of night-time cycles is indicative, as it is not possible to define them at this stage **{T2S.03.100}**. However it is possible for the T2S Operator to adjust them if need be.

During day-time phase specific deadlines are set to uniform their settlement. DVP instructions for same day settlement must be received by the T2S platform by 16:00 at the latest **{T2S.03.250}**. Bilaterally agreed instructions for same day settlement, free-of-payment (FOP) and central bank operations must be received by the T2S platform by 18:00 at the latest **{T2S.03.270}**, **{T2S.03.280}**, **{T2S.03.290}**.

The End-of-Day procedures are scheduled to take place between 18:00 (end of day time settlement) and 18:45. This phase is mainly dedicated to reporting needs. During this phase no settlement takes place and as a consequence both securities and cash balances are kept unchanged. **{T2S.03.170}**. The other core activity within this phase is dedicated to the automated transfer of liquidity from the T2S dedicated cash accounts towards TARGET2 and the other RTGS systems possibly connected with T2S **{T2S.03.180 }**.

In order to guarantee a consistent treatment of the flows (securities and cash), T2S has per each T2S currency a calendar for DVP settlement in CeBM according to the opening days of the relevant central bank **{T2S.03.320}**. For Euro CeBM settlement this calendar is the TARGET2 calendar as published on the ECB website **{T2S.03.310**}. For the settlement of FOP transactions T2S is open every day from Monday to Friday {T2S.03.305}.In the interest of cost-effectiveness, it remains to be decided whether it is meaningful to keep T2S open when all connected markets have a common public holiday (e.g. 1 January and 25 December).

The maintenance period of T2S includes any public holiday or weekend that falls in between **{T2S.03.340}.**

Should the system have to be opened during normally closed days (week-end or public holiday) for special purposes, this has to be requested in due time to the T2S Service Desk. **{T2S.03.360}.**

After the migration period, two test environments will be available, one as a replica of PROD (UTEST) and another one for testing new releases (EAC) respectively. The Eurosystem reserves the right to block one of the two environments for its own regression testing of new releases for the time periods required to complete these activities.

# 5. Information Security Management

## 5.1. Objectives

Weaknesses in Securities Settlement Systems (SSSs) could potentially be a source of systemic disturbances to securities markets and to other payment and settlement systems. Moreover, a disruption within a SSS settling cross-border transactions like T2S could trigger disruptions or transmit shocks amongst the financial system domestically or internationally[15].

Considering the risks of such a system, information security management is a crucial aspect of the T2S project and appropriate protection of the confidentiality, integrity and availability of T2S information shall be guaranteed. Furthermore, other security properties such as authentication, accountability, non-repudiation and reliability must be ensured as well.

The main objective of information security is to protect T2S information from a wide range of threats, whether internal or external, deliberate or accidental, and to minimise the impact on the continuity of T2S business of any threats, which, despite all measures taken, do materialise.

Information security is achieved by implementing suitable security controls. In this context it is important to note that information security is not only based on technical solutions. The organisational framework is equally important.

The URD chapter 18 contains a list of high-level, standards based requirements concerning information security that have to be addressed. In order to ensure the provision of T2S services in a secure and resilient manner these high-level security requirements will be complemented with detailed policies and the specification of specific security controls which are for internal use only.

The definition of adequate risk management processes embedded into a comprehensive framework will make sure that all aspects of information security related to T2S are addressed in an effective, dynamic and reassuring manner.

## 5.2. T2S Risk Management Framework

To meet all requirements concerning information security the internationally recognised ISO standard 27001 and 27002 as well as recommendation from regulators[16] has been taken into account when developing the T2S Risk Management Framework.

Following the overarching principle corroborated by the internationally recognised ISO/IEC 27002:2005 standard according to which *"information is an asset that,...., is essential to an*

[15] See "The interdependencies of payment and settlement systems" June 2008 – Committee on Payment and Settlement Systems report

[16] for example "Recommendations for securities settlement systems" (Recommendation XI) published by the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions in November 2001

*organisation's business and consequently needs to be suitably protected",* a holistic information security risk management framework is being developed for T2S. Using this framework will ensure that confidentially, integrity and availability of T2S information is preserved effectively. In simple terms, the T2S risk management framework (T2SRMF) is following a process logic as outlined below:

1. **Requirements specification and design process** (before establishing the infrastructure): creating a high-level policy with which management sets clear objectives and demonstrates its support for and commitment to information security. Potential threats are analysed, security requirements are specified and suitable security controls that should be implemented to prevent threats from materialising are defined.

2. ***Core* process** (prior to going live): check which security controls are actually in place, assess the weaknesses and their possible consequences [in terms of likelihood and impact]. Identified risks are reported to management requesting a decision whether a risk can be accepted or mitigating measures should be implemented as a follow-up activity.

3. **Dynamic *review* processes** (during live operations): in order to ensure that the framework is kept up-to-date and changes in the risk situation are properly addressed various features like incident reporting, change management, identification of new threats and action plan monitoring are integral parts of the overall concept. Whenever the risk situation changes this is presented to management and they are invited to give guidance on how to proceed.

The above is a brief description of the comprehensive T2SRMF which is following a hierarchical, three-layer structure ranging from a high-level policy to operational procedures.

The first layer comprises an information security policy for T2S, which embraces at a generic level the security policy principles and further relevant aspects related to information security management.

The following deliverables belong to the second layer:

- The Threat Catalogue listing all relevant threats to T2S.
- The specification of the necessary T2S Security Requirements and Controls addressing the identified threats.
- The Glossary ensuring a common definition of all terms.
- The Compliance Check Tool defining the questionnaire used for the core and the review processes.

The third layer contains all deliverables that describe the implemented guidelines and procedures:

- The T2S Risk Management Manual describing in detail the risk management processes.
- The Methodology for scoring risks.
- The Risk Scoring Matrix and Risk Tolerance definition.

- The allocation of Roles and Responsibilities in the risk management process.

Due to the fact that the criticality of TARGET2 and T2S are broadly similar, some robust and reliable security mechanisms and services already implemented, tested and operated by the 3CB for TARGET2 might be reused.. However, owing to the fact that T2S business is different from TARGET2 adaptations might be necessary to ensure the information security meets T2S specific needs.

## 5.3. Responsibilities

The common governance structure of T2S comprises a number of different stakeholders whose roles and responsibilities with respect to information security are outlined in the following.

### 5.3.1. Governing Council of the ECB

The TS2 platform is fully owned and operated by the Eurosystem [see T2S user requirements - Principle 1]. In their role as highest Governance level of the Eurosystem, the Governing Council of the ECB is responsible for safeguarding the public function of T2S. In this context the Governing Council has the ultimate responsibility for deciding on the general security policy and framework for T2S information security risk management, the definition of the risk tolerance and acceptance of remaining risks.

### 5.3.2. T2S Programme Board

The T2S Programme Board is responsible for defining and implementing an effective organisational framework to address information security issues. Furthermore it is responsible for verifying that all requirements specified in the information security policy and the T2S User requirements are fully implemented in T2S.

### 5.3.3. 4CB

The 4CB are directly responsible for ensuring that the agreed information security requirements are fully implemented, security controls are effective, and that their personnel adhere to the security rules and procedures. In support of meeting its information security review responsibilities the 4CB shall provide the T2S Programme Board with all relevant information.

### 5.3.4. Third party service providers

Third parties providing necessary or additional services to the T2S platform are directly responsible for ensuring that the agreed information security requirements, as far as their part is concerned, are fully implemented. In addition they have to provide the T2S Programme Board with all relevant information for its information security review responsibilities.

# 6. User testing and migration process

## 6.1. Introduction

The user requirements with respect to migration are covered in chapter 21 of the URD v4.2. These user requirements cover the migration planning, communication, some aspects of user testing (including compliance certification), and the availability of data migration tools and training opportunities.

User testing and migration are typically processes that require a close co-operation between the service user (CSDs and directly connected T2S Actors), the service provider and the relevant central banks (as operators of central bank money accounts). Consequently, within the governance structure that has been established for the specification phase, the T2S Advisory Group has mandated a group of representatives from the ECB, 4CB, CSDs and other T2S users to prepare the general approach for these processes, in particular in view of fulfilling the relevant user requirements.

Taking into account the limited lifetime of the current governance arrangements until the end of 2009, the mandate of this Subgroup on Testing and Migration has accordingly been defined as follows:

> *The Sub-group's responsibilities concerning the user testing work stream consist of the definition of the testing strategy, and the preparation of generic acceptance and user testing plans and procedures on the T2S test environment for CSDs, directly connected participants and NCBs.*
>
> *The Sub-group's responsibilities concerning the migration process cover the definition of the migration strategy, as well as the preparation of a generic migration plan for those CSDs and directly connected CSD participants that will have committed to join T2S.. Furthermore, the group should also prepare the appropriate communication framework aimed at informing all stakeholders about all relevant aspects of the migration process.*

## 6.2. The T2S Migration process

### 6.2.1. The T2S Migration according to the URD

The Eurosystem is ready to offer a comprehensive support to the CSDs and other T2S Actors in order to prepare them for starting their business on the T2S system. Moreover, the Eurosystem will support them during their migration process by giving advice and information.

The preparative support will be defined and described in a training framework.

Although the precise training modalities have to be agreed with the T2S users, the migration support to the T2S users encompasses the following aspects:

- Informational and specific interactive training sessions for CSDs, Central Banks and directly connected Parties (based on a priority order) covering the whole range of T2S issues which are of relevance and of interest for their migration process to T2S (e.g. connectivity issues, data transfer during the change-over weekend, usage of migration tools, use of specific T2S functionalities) **{T2S.21.380}, {T2S.21.390}, {T2S.21.400}, {T2S.21.410}, T2S.21.430};**
- In addition, subject to more precise requirements still to be defined by the T2S Actors, web-based training courses on the issues mentioned above could be offered **{T2S.21.400}, {T2S.21.410};**
- Setting-up of a service desk/single contact point at the Eurosystem in due time for migration related questions.

As requested in the URD, support to the T2S Actors is given for the following migration-related tasks:

- Establishment of standard and weekend migration plans, for the general tasks to be performed during each migration weekend **{T2S.21.170}, {T2S.21.190}, {T2S.21.350}** as well as the establishment of specific plans tailored and detailed for each of the migration weekends **{T2S.21.200}, {T2S.21.210}**;
- Definition of static data from the CSDs and Central Banks to be transferred to the T2S system in the weeks before the go-live date as well as the updating of static data which have changed in the meantime, **{T2S.21.250}**;
- Coordination of dynamic data input, i.e. pending settlement instructions and account balances;
- Identification and usage of migration tools to support the transfer of data to the T2S system **{T2S.21.300}**;
- Definition and implementation of a certification procedure with regard to the task completion during the change over weekends **{T2S.21.330}, {T2S.21.340}**.
- Definition and testing of fallback scenarios and roll-back procedures for each of the change over weekends **{T2S.21.180}**, **{T2S.21.230}**, **{T2S.21.240}**, **{T2S.21.245}**;
- Definition of contingency and escalation procedures dealing with unforeseeable problems, in particular in case the migration process has to be stopped and deferred to a later stage **{T2S.21.220}**.

After the completion of the migration to T2S a continuing increased support will be offered in the early weeks of live operations **{T2S.21.140}**, **{T2S.21.150}**, **{T2S.21.160}**, **{T2S.21.360}**.

### 6.2.1. The T2S migration approach

The migration approach is described in a document entitled "T2S Migration Strategy", adopted by the T2S Advisory Group on 9 December 2009 and which can be accessed via the following link: http://www.ecb.europa.eu/paym/t2s/progress/pdf/ag/mtg7/Item_6_2_T2S_Migration_Strategy.pdf?f0392db1c5740ec73e81ab50e0c31fc4.

The objective of the T2S migration is to enable a smooth transition to the T2S system for all involved T2S Actors, which – according to the URD – means a relocation of data by a CSD to the T2S infrastructure and the associated changes in the processes and technical environment of a CSD on a mutually agreed date.

In terms of activities, the scope of the migration is defined as the complete set of activities that prepare, steer and monitor the migration process into the T2S production environment. With regards to the users, the T2S migration perimeter consists of all T2S Actors who will join T2S during the migration period, i.e. CSDs, central banks, directly connected T2S parties and (other) holders of T2S dedicated cash accounts.

The migration to T2S will follow a phased approach which gives more flexibility for the planning and coordination of the migration activities and allows a gradual build-up of volumes to ensure system stability from a functional and technical perspective throughout the migration process. Although a big bang would be simpler and less costly than a phased migration, the risk of a significant business impact on the day(s) after go-live is too high and cannot be adequately mitigated by any measures, and hence cannot be accepted.

The migration will be organised in 3 migration waves targeting a period of 6 months. The first migration wave concentrates on the functional stabilisation with limited business impact while a balanced volumetric approach should be adopted for the next migration waves to safeguard the performance of the system. This phased approach will be implemented via a migration "by CSD", which is the preferred option both from a project management and business operations perspective.[17] The migrations will take place during weekends and will be driven by settlement date.

The life-cycle of the migration process consists of four phases: conceptual, planning, implementation and closing. It has started with the elaboration of the migration strategy and the generic migration plan and will from now on continue with the activities related to the preparation of the migration activities that need to be planned in advance in order to mitigate the migration risks. This relates in particular to the composition of the migration waves, the standard migration plan and detailed migration weekend plans, including the necessary fall-back and roll-back procedures. The implementation phase consists of the actual preparations for live operations. These include in particular the registration and the timely uploading of static data prior to the migration[18], as well the

[17] In this sense the T2S Advisory Group confirms it earlier agreement, laid down in the "General Principles and High-level Proposals for the T2S User Requirements (April-October 2007)", of which Proposal no. 66 states that "Migration to T2S will be performed on a CSD or group of CSD basis".

[18] Some static data (e.g. securities reference) should be uploaded prior to the go-live of T2S, irrespective of a CSD's migration wave.

transfer of dynamic data during the migration weekend. After each migration, a closing report aims at improving the next migration based on lessons learned from the previous one.

In order to ensure a successful migration to T2S according to the pre-agreed plans, the readiness of the CSDs, the central banks and their communities is of utmost importance. While the Eurosystem will be responsible for the overall co-ordination of the planning and implementation of all migration activities, the actual readiness for the migrations are a shared responsibility of the Eurosystem and each individual CSD and non-euro central bank that committed to join T2S. In particular, while the CSDs are responsible to ensure the readiness of the securities accounts for their community according to the agreed migration plan, the euro area central banks have the responsibility to create and manage the dedicated cash accounts in T2S as of the start of the first migration wave (i.e. the go-live). For the non-euro area central banks, the readiness of the dedicated cash accounts should be ensured prior to the first settlement of securities transactions in their currency. Directly Connected T2S Parties (DCPs) will connect to T2S under the responsibility of their CSD(s), either simultaneous with their CSD(s) or at the end of the stabilisation period after the migration of the CSD's activity, taking into account any relevant risks. Directly connected holders of T2S dedicated cash accounts will connect to T2S under the responsibility of their respective Central Bank(s).

In order to ensure the timely readiness of the whole market, every T2S stakeholder in the settlement chain should be aware of its responsibility vis-à-vis its user community, as well as its service providers, and should take action in order to ensure its readiness for T2S migration according to its responsibility.

A communication framework will be set up in order to support the migration activities and to facilitate the optimal implementation of the any corrective measures that need to be taken during the migration process. Communication regarding the migration process and individual migration waves will be prepared jointly by the Eurosystem, non-euro central banks and CSDs, in accordance with the applicable governance arrangements.

## 6.3. The T2S User Testing process

### 6.3.1. T2S User Testing according to the URD

The Eurosystem will support the T2S Actors with regard to the coordination and preparation of user testing activities as well as the provision and operating of the technical test environments, as requested in the URD.

Furthermore, the Eurosystem will support them during their testing activities and before in order to prepare them for the tests (based on a priority order) by offering informational and specific interactive training sessions focusing on the upcoming testing activities **{T2S.21.380}, {T2S.21.390}, {T2S.21.420} and {T2S.21.430}**.

The relevant functional T2S documentation (UR Document, GFS, UDFS) is the basis for the test preparation. Furthermore, the technical infrastructure for the testing processes, including telecommunications, applications, technical help desk and reports will be available **{T2S.21.080}.** The testing infrastructure supports testing during a specific period of settlement days (e.g. five consecutive settlement days) **{T2S.21.090}.** Multiple CSDs, Central Banks and directly connected T2S Parties will be able to test in parallel already at an early stage during the testing process **{T2S.21.100}.**

In co-operation with the CSDs and other T2S Actors, the Eurosystem will take responsibility for the preparation of the test framework, including

- A test plan which allows CSDs and directly connected T2S Parties to coordinate their testing activities **{T2S.21.020}**;
- Test scenario and test case specifications including the input values used and the expected results, they will also allow for integrated tests, e.g. with TARGET2 and the external network providers **{T2S.21.070}**;
- Test procedure specifications describing the testing process in detail.

In addition, changeover activities are tested during the community testing phase at CSD community level and again for a complete migration date during the business day testing phase. **{T2S.21.110}.**

For audit and control purposes, testing documentation and testing results are archived **{T2S.21.120}**. The archiving duration may differ between countries due to national regulations, whether or not to have a common archiving period has to be defined at a later stage **{T2S.21.130}**.

### 6.3.1. General approach to User Testing

The User Testing approach is described in a document entitled “T2S User Testing Strategy”, adopted by the T2S Advisory Group on 9 December 2009 and which can be accessed via the following link: http://www.ecb.europa.eu/paym/t2s/progress/pdf/ag/mtg7/Item_6_2_SGTM_T2S_User_Testing_Strategy.pdf?9bb9243e8aa9060566e29bb54503d473.

In order to ensure a secure and smooth transfer of settlement activity from the CSDs’ proprietary IT environments to T2S, a thorough testing of T2S – in combination with the IT systems of the T2S Actors – must be carried out. The T2S User Testing Strategy document provides a high-level overview of the user testing endeavour. It defines user testing objectives, the scope, the stakeholders, the organisation and the life-cycle.

The objectives of the user testing are to ensure that the T2S platform fully meets user requirements together with functional and technical specifications, and to guarantee the readiness of the T2S Actors for their migration to and operation on T2S. The successful completion of the user testing is indeed a prerequisite for the migration of CSDs and Central Banks to T2S.

Two categories of tests are in the scope of the user testing, i.e. functional and non-functional. The functional tests will be executed by the T2S Actors after the successful acceptance by the Eurosystem and are aiming at ensuring that the user requirements are correctly and completely covered, both in the T2S software application and in the T2S Actors’ internal systems. The major part of the non-functional tests is related to the T2S technical infrastructure and will be performed by the Eurosystem (see also section 6.4 below). Although test plans and test coverage will be reviewed by, and agreed with, CSDs and non-euro Central Banks, no active involvement of the CSDs and the non-euro Central Banks in the execution of the non-functional tests is foreseen.

In order to achieve the objectives the execution of the user testing is divided conceptually into three (overlapping) activities: user certification, T2S verification and free testing.

The aim of the user certification is for the Eurosystem to ensure that a directly connected T2S Actor creates no adverse effects on others or T2S itself by migrating when its internal systems and interfacing procedures are not compatible with T2S. The T2S Actors subject to certification testing are the CSDs, the Central Banks, the DCPs and the directly connected holders of T2S dedicated cash accounts.

The aim of the T2S verification is for every CSD and non-euro Central Bank to obtain certainty that T2S delivers the expected services as described in the URD and as further described in the functional and non-functional specifications. The CSDs and non-euro Central Banks are free to execute any functional tests for the purpose of their T2S verification. They may as well capitalise on test results of other T2S Actors and the Eurosystem.

The aim of the free testing is for all directly connected T2S Actors to verify that their internal systems and operational and business processes are well designed to efficiently interact with T2S in order to be able to provide the expected services.

In order to effectively manage the user certification and T2S verification activities, the user testing execution will be based on an approach that gradually expands the perimeter of testing activities, resulting in increasing complexity throughout the testing activities. The interoperability testing stage will involve CSDs and Central Banks only and will focus on verifying individual T2S functionality. Community testing will allow CSDs and Central Banks to execute more business-oriented tests with their communities, in particular the DCPs. Prior to the business day testing, the testing of the migration processes will be also covered for which a precise organisation will be defined during the planning phase. Finally, business day testing will bring together all CSDs, in particular those of the same migration group and will verify that all end-to-end business processes, including the migration process itself, runs smoothly.

The whole T2S User Testing endeavour life-cycle is planned in four phases: conceptual, planning, execution and closing. The conceptual phase ends with the adoption of the User Testing Strategy by the Advisory Group and will soon move on to the planning and preparation stage. The implementation stage will consist of actually performing the planned test activities until the T2S platform is verified and directly connected T2S Actors are certified. The possible impact of testing activities on the pace of the migration (i.e. test cycles required between the waves) will also require further assessment.

## 6.4. Non-functional tests

As specified in section x.x above, the major part of the non-functional tests is related to the T2S technical infrastructure and will be performed by the Eurosystem. This concerns a series of technical, performance, business continuity and security tests. Besides these tests to be performed by the Eurosystem, the CSDs will have to perform connectivity tests (including re-connection and failover capability) on the T2S production environment. This is a pre-condition to start the migration activities. Such tests are not required in the test environment. The only pre-condition to start functional testing is the establishment of a connection with T2S.

### 6.4.1. Technical tests

Technical tests are performed in order to check the availability and the correct setup of single hardware and software components. They are conducted in the test environment and in the production environments, before the go-live and after relevant changes. These tests make use of tools and techniques to simulate failures, e.g. missing components, wrong input messages, etc.

### 6.4.2. Performance Tests

The main objective of these tests is to check that the T2S production environment is able to handle the estimated volume of transactions in the peak hour in terms of number of settlements and a certain number of concurrent interactive users in compliance with a defined response time.

The test plan includes a global system test aimed to measure throughput, response time and resource consumption of the whole system (infrastructure and applications) and also other tests conducted on specific parts of the system in order to optimise the behaviour of these T2S components (volume tests).

Different test cases will be performed aiming to simulate the expected daily workload profiles for U2A and A2A interactions on the available interfaces by using simulators and/or with the collaboration of the CSDs.

The tests will be performed by the 4CB, on behalf of the Eurosystem. T2S actors will be involved in the preparation of the test scenarios and are invited as observers to the global system test. The results of such test will be communicated to the T2S stakeholders.

The test plan will follow a gradual approach to verify, in sequence, that:

- All infrastructure components and services are properly sized to handle the defined peak workload of settlements;
- The T2S application is able to satisfy the defined performance requirements **{URD v4.2 – section 17.1.1}**.

### 6.4.3. Business continuity Tests

The main objective of the Business continuity tests is to verify the ability of T2S to guarantee the continuity of business services in case of local component failure, regional disaster event or planned maintenance. These tests will be performed on the T2S production environment only, both before go-live and, after go-live, on a regular basis.

The test plan will include a comprehensive list of test cases including:

- **Fault tolerance** (i.e. resiliency of single component);
- **Intra Region Recovery**;
- **Inter Region Recovery (only Regions 1 and 2)**.

In addition, tests will be performed to validate the rotation between Region 1 and Region 2 strongly linked to the disaster recovery test in terms of organisation and operational procedures.

The tests will be performed by the 4CB, on behalf of the Eurosystem. T2S actors will be involved in the preparation of test scenarios and are invited as observers to the main tests. The results will be communicated to the T2S stakeholders.

The test plan will cover local and regional recovery and will verify that the recovery objectives are fulfilled **{T2S.18.1220}**.

### 6.4.4. Security Tests

The main objective of the security tests is to verify the ability of T2S to guarantee the security requirements, in terms of integrity and confidentiality of information, as well as authentication and non-repudiation of messages. These tests will be performed on the T2S production environment only, both before go-live and, after go-live, on a regular basis.

The test plan will include a comprehensive list of activitiexs including:

- **Vulnerability assessment**
- **Configuration analysis**;
- **Penetration tests**.

The tests will be performed by the 4CB, on behalf of the Eurosystem, possibly assisted by external IT security experts. T2S actors will be involved in the preparation of test scenarios and will be informed of the test results.