	T2 Connectivity Guide	Page 1 of 16



T2 Connectivity Guide

Author	4CB
Version	1.0
Date	31/03/2021
Status	Final
Classification	Public
Classified until	N/A

Table of contents

Table of contents.....	2
1. Introduction.....	4
2. Global Connectivity Overview	4
2.1 Connectivity	4
2.2 The communication modes.....	4
2.2.1 A2A channel.....	5
2.2.1.1 <i>Message/File compression</i>	5
2.2.1.2 <i>Message size</i>	6
2.2.1.3 <i>Message/File signature</i>	6
2.2.1.4 <i>Delivery Notification signature</i>	7
2.2.1.5 <i>Message Formats</i>	7
2.2.2 U2A channel.....	8
3. User Registration process	8
3.1 Set-up of parties.....	8
3.2 CGU subscription	8
3.2.1 CGU subscription for T2 Actors (excluding CBs)	9
3.2.2 CGU subscription for CBs.....	10
3.2.3 CB Authorised Approvers	12
4. Request for Digital Certificates by the NSP PKI	12
4.1 Setting up security.....	12
5. NSP documentation.....	13
6. Connectivity checklist	13
7. Troubleshooting and support.....	13
8. Availability.....	14
9. Acronyms	14
10. Appendix	15
10.1List of criteria for CGU subscription	15

History of releases


RELEASE	DATE	ISSUES	STATUS
V1.0	25/03/2021	Approved by MIB	FINAL

Applicable documents

REFERENCE	OBJECT

Reference documents

REFERENCE	OBJECT
CLM User Detailed Functional Specifications v2.1	CLM UDFS 2.1
ESMIG User Detailed Functional Specifications v2.1	ESMIG UDFS 2.1
RTGS User Detailed Functional Specifications v2.1	RTGS UDFS 2.1

	T2 Connectivity Guide	Page 4 of 16

1. Introduction

The T2 Connectivity Guide describes in general terms the connectivity of T2 Actors to the Eurosystem Single Market Infrastructure Gateway (ESMIG). The ESMIG provides a single access point for directly connected actors to access TARGET services.

Access to the ESMIG is provided by the two Network Service Providers (NSP) selected by Banca d'Italia on behalf of the Eurosystem, which are SIA-COLT and SWIFT.

This connectivity guide only is not sufficient to achieve the connectivity to ESMIG. All NSPs specific steps and technical details (e.g. settings, tokens, etc) to achieve the connectivity to T2, are described in the relevant NSP (SWIFT or SIA-COLT) related documentation.

2. Global Connectivity Overview

2.1 Connectivity

Reference document	RTGS UDFS v2.1 "Access to RTGS"
--------------------	---------------------------------


The T2 service relies on the ESMIG for the communication with T2 Actors. The ESMIG is the common entry point for all interactions with the Eurosystem Market Infrastructures and back-office applications (T2, T2S, TIPS, ECMS and potential future services). It allows relevant Actors to connect through one or multiple NSPs for both A2A and U2A interfaces.

The ESMIG supports the connectivity of T2 Actors as follows:

- A2A (Application-to-Application): Communication between software applications via Extensible Markup Language (XML) messages or files using ISO 20022 messages or compliant with the ISO 20022 format. A file contains one or several messages.
- U2A (User-to-Application): Communication between ESMIG and users (such as T2 Actors) via an online screen, the Graphical User Interface (GUI).

2.2 The communication modes

Users can communicate with T2 in two different modes: Application to Application (A2A) or User to Application (U2A).

	T2 Connectivity Guide	Page 5 of 16

2.2.1 A2A channel

For the A2A mode, T2 communicates with the T2 Actors with two transfer modes: the "real-time" and the "store-and-forward". Both messages and files can be exchanged with the "real-time" and the "store-and-forward" modes.

The "real-time" message and file transfer requires that both parties, a sender and a receiver, are available at the same time to exchange messages or files. In the case of unavailability of the receiver, no retry mechanism is foreseen. The communication is based on a request-response pattern; this means that for each request the client submits to the server, a response is expected to be sent from the server to the client. The "real-time" mode is used for query/response message flow; the response will use the same transfer mode (i.e. real-time) of the request.

The "store-and-forward" message or file transfer enables a sender to transmit messages or files even when a receiver is unavailable. In the case of temporary unavailability of the receiver, the NSP stores messages and files for up to 14 calendar days and delivers them as soon as the receiver becomes available again.

The A2A message and file exchange between T2 and the NSP is based on a proprietary protocol named DEP (Data Exchange Protocol). The protocol relies on XML messages, transported over a Message Queue (MQ) connection and containing all the relevant information to address and describe messages and files.

The data exchange between the T2 Actor and the NSP is compliant with a protocol defined by the relevant NSP and it is managed by the gateway of the Actor (i.e. the original sender) and the gateway of the NSP. The NSP offers connectivity services and manages the bi-directional data exchange with ESMIG according to the DEP.

The NSP offers several functionalities: Technical Sender Authentication, CGU, non-repudiation, encryption, NSP protocol transformation into and from DEP protocol.

2.2.1.1 *Message/File compression*

For any types of outbound communication, the ESMIG compresses the data only if this is required by the compression settings. However, an exception is foreseen:

- if the outbound communication is smaller than 2KB, then the ESMIG does not compress the data regardless of the setting;

All the XML business data has to be compressed including Business Application Header (BAH) or Business File Header (BFH).

The compression algorithm supported by ESMIG is the ZIP algorithm (i.e. ZIP deflate and the BASE64 RFC 2045).

After compression, the compressed data has to be conveyed in the Business Envelope field of the DEP message. Data belonging to the network protocol (DEP Exchange Header) is not compressed.

That is valid for messages sent by a T2 Actor as well as for the ones sent out by T2.

ESMIG does not process decompressed communication which size exceeds 99 MB.

2.2.1.2 Message size

The DEP is used to exchange data between ESMIG and the NSP.

In the DEP, data can be exchanged as a message or a file. From a DEP point of view, the distinction between a file and a message is based on the size of the transported Business Envelope.

The channel through which data is exchanged, both for messages and files, defines the maximum size of the Business Envelope part of the DEP message (size is calculated without considering the *BusinessEnvelope* tags).





	Maximum Length
Message channel	32 KB (KB=2 ¹⁰)
File channel	32 MB (MB=2 ²⁰)

For the ESMIG outbound traffic, the size limitation of 32 KB could lead to messages not being transmitted as their content unavoidably exceeds the maximum size. This is particularly the case for query responses and reports where a considerable amount of information referring to the same business case needs to be transported.

When the size of an outbound message exceeds the aforementioned size of 32 KB, the ESMIG automatically switches from a message-based network service to a file-based network service allowing for a maximum file size transmission of 32 MB. By doing so, it can be avoided to split the message into different messages below the 32 KB maximum limit.

Further details about this functionality, named oversize management, can be found in the ESMIG UDFS.

2.2.1.3 Message/File signature

 BANCA D'ITALIA EUROSISTEMA	 BANCODE ESPAÑA Eurosisistema	T2 Connectivity Guide	Page 7 of 16
 BANQUE DE FRANCE EUROSYSTEME	 DEUTSCHE BUNDESBANK EUROSYSTEM		

The Messages/Files exchanged between T2 and T2 Actors are provided with two digital signatures:

- **the Technical Envelope signature;**

This signature is performed by the ESMIG and by the NSP by means of digital certificates issued by the NSP PKI.

- **the Business Layer signature**

The purpose of the Business Layer signature is to authenticate the business sender and guarantee the integrity of the business payload.

The signature is stored in the BAH in case of individual messages or in the file BFH in case of a file.

In outgoing communication, the signature is performed by the ESMIG through an NSP certificate.

In incoming communication, the signature has to be performed by the T2 Actors with an NSP certificate.

The NSP will provide the necessary Application Programming Interface (API) to manage activities related to the signature, e.g. signing, verification of signature and check against directory services. In addition, the NSP may optionally provide additional services to further help preparing the data to be signed/verified.

For information on the Business Layer signature format, please refer to the ESMIG UDFS.

The certificates used are issued by the NSP PKI in both outgoing and incoming cases and belong to a specific certificate class with a strong level of authentication and non-repudiation. The validity period of these certificates is 24 months (users shall start renewal process in due time).

2.2.1.4 Delivery Notification signature

For incoming Store-and-Forward traffic, the NSP sends a Delivery Notification upon reception by T2 of a Message/File to inform the T2 Actors who have chosen the option. The Delivery Notification is built by the NSP using the Technical Acknowledgment from T2 and it carries the following pieces of information:

- The timestamp set by T2 when the Message/File was received;
- The digital signature generated by T2 of the received Message/File, included in the Technical Envelope signature.

2.2.1.5 Message Formats

The T2 application uses messages in an ISO 20022 compliant format. For information on the message format, please refer to the T2 CLM or RTGS UDFS.

2.2.2 U2A channel

The U2A interface between T2 and the NSP is based on the standard Hyper Text Transfer Protocol secure (HTTPS) protocol; therefore, HTTPS traffic between the users' workstations and T2 must be properly configured on the customer device, in order to enable as default security protocol the ESMIG entry firewall. In this context, the NSP must provide mainly connectivity, CGU and PKI services. T2 Actor identification and authentication are based on digital client certificates. Certificates are provided by the NSP and assigned to the end-users, stored with the related private keys in a smart-card, USB token or remote HSM (Hardware Security Module).

Low volume users may opt for a connectivity option provided by an NSP using U2A only.

3. User Registration process

Reference document(s)	<ul style="list-style-type: none"> ▪ NSPs own User documentation ▪ NSPs Registration process (NSPs website)
------------------------------	---

3.1 Set-up of parties

A party is defined as a legal entity or an organization interacting with T2 Service.

The operator is responsible for setting up and maintaining party reference data for all CBs relevant for T2. CBs are responsible for setting up and maintaining party reference data for the parties of their community.

The following table summarizes the configuration responsibilities for each reference data object related to parties in T2 and specifies the required communication mode:

Reference data object	Responsible actor	Mode
Party (CB)	Operator	A2A/U2A
Party (payment bank)	CB	A2A/U2A
Party (ancillary system)	CB	A2A/U2A

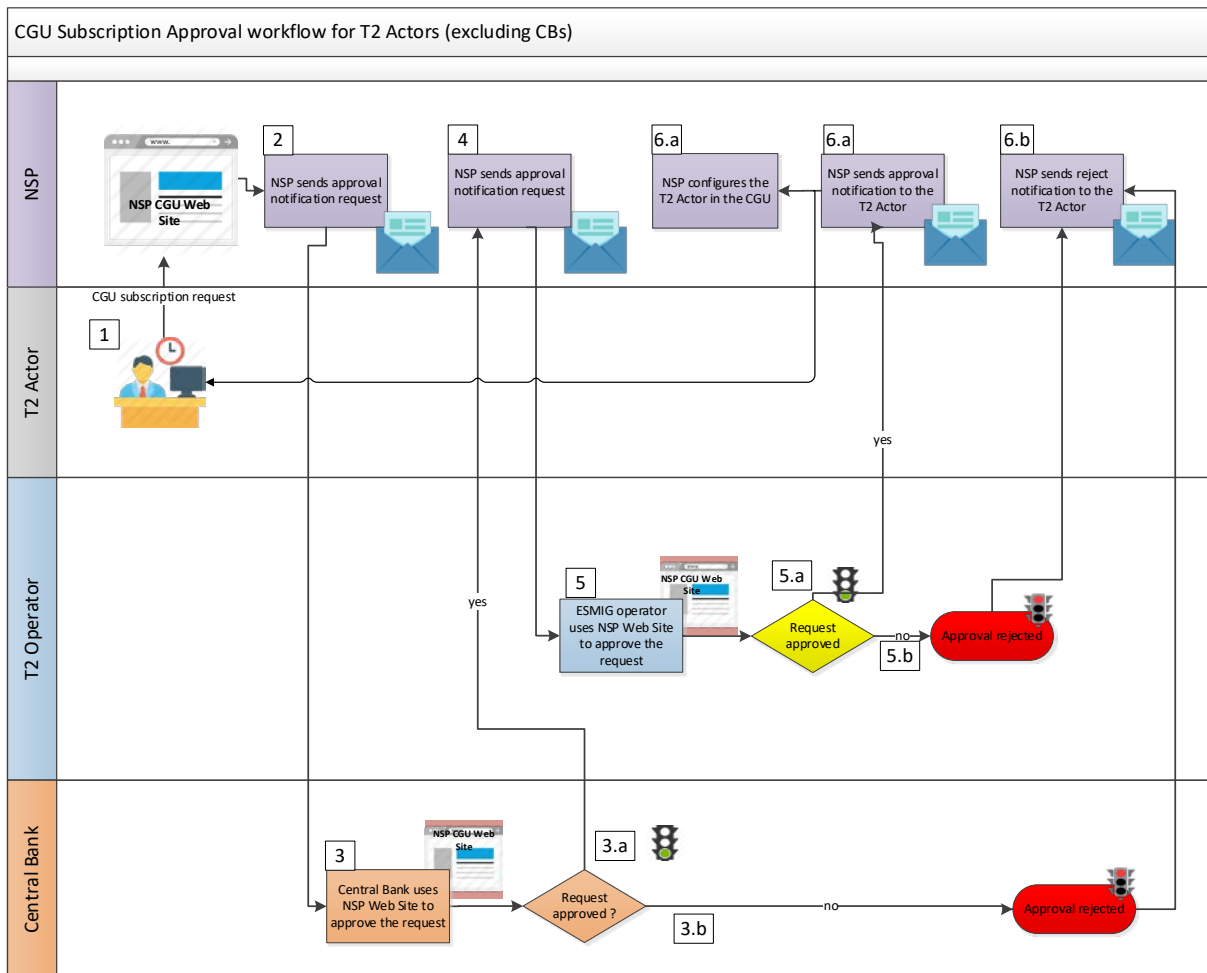
3.2 CGU subscription

The NSP shall create and manage CGUs (Closed Group of Users) containing the relevant T2 Actors for both the Production environment (PROD) and the Test & Training environment (UTEST and


EAC), one CGU for each environment. The subscription to a CGU, and any subsequent modification to such subscription, shall be arranged through an electronic workflow on the Internet. All the electronic forms shall be authorised by the relevant Central Bank and the T2 Operator. The T2 Operator shall set the activation date for the subscriptions at the latest within two weeks after the form's approval; the new subscription shall be scheduled and activated ensuring the availability of the service. Upon request from the T2 Operator, the NSP shall withdraw from the CGU a T2 Actor within one hour.

3.2.1 CGU subscription for T2 Actors (excluding CBs)

The CGU subscription includes a two steps approval workflow as described in the figure below:



1. The T2 Actor submits the subscription request through the NSP website.
2. The NSP validates the request and sends the approval notification request to the CB.
3. The CB checks the subscription request in the NSP website.
 - a. The request is approved

	T2 Connectivity Guide	Page 10 of 16

- b. The request is rejected
4. In case the subscription request is approved by the CB, the NSP sends the approval notification request to the T2 Operator.
5. The T2 Operator checks the subscription request in the NSP website
 - a. The request is approved
 - b. The request is rejected
6. The NSP sends the Approval or Reject notification
 - a. The request is approved. The NSP configures the T2 Actor in the CGU.
 - b. The request is rejected

In case of a modification request, the T2 Actor undergoes the change process as defined by the NSP, who receives the request and performs the standard validation against the information provided. If the validation is successful, the NSP evaluates if the order contains a change of the CGU.

If there is a change of the CGU, the same approval flow is foreseen:

- Dual approval is requested for orders submitted by a T2 Actor (other than a CB):
 - The responsible CB performs the first approval;
 - The T2 Operator performs the second approval.

For all other types of changes (e.g. the technical parameters), no external approval is required and the technical implementation can be executed by the NSP autonomously.

3.2.2 CGU subscription for CBs

The CGU subscription consists of a single approval workflow as described in the figure below:

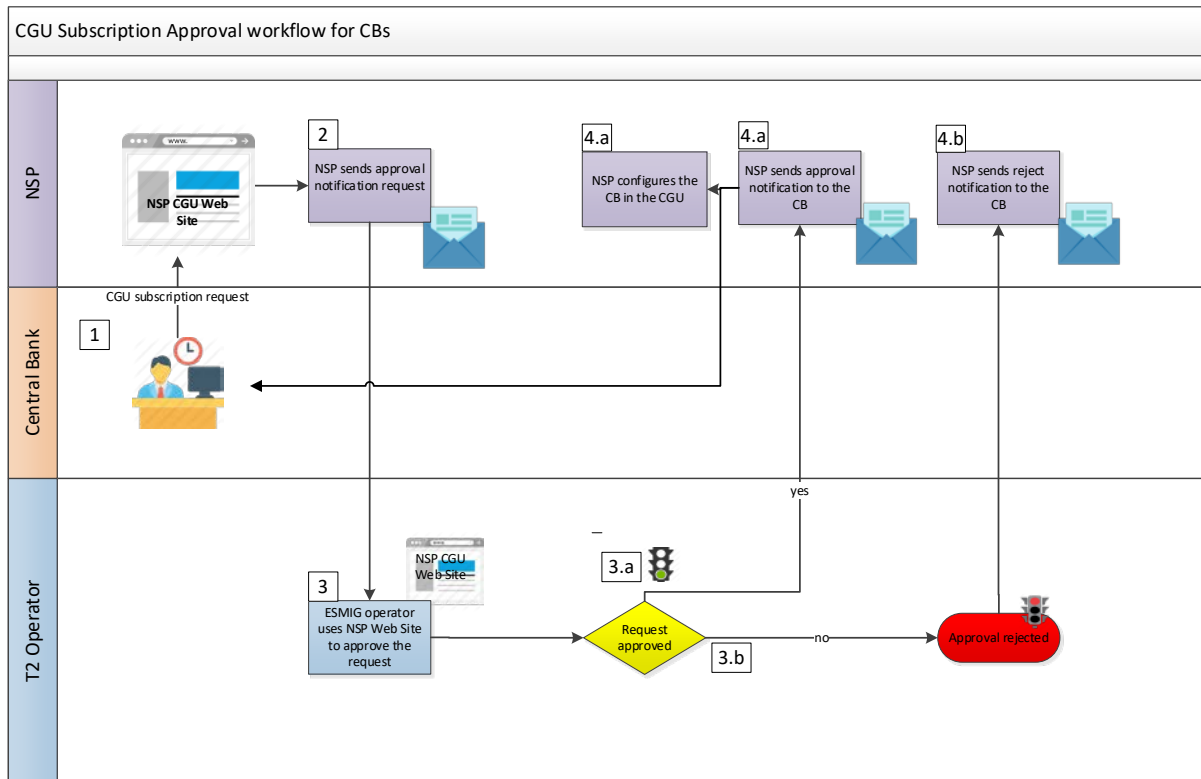



FIGURE 1 – CGU SUBSCRIPTION WORKFLOW FOR CBs

1. The CB submits the subscription request through the NSP website.
2. The NSP verifies the correctness of the request and sends the approval notification request to the T2 Operator.
3. The T2 Operator checks the subscription request in the NSP website.
 - a. The request is approved
 - b. The request is rejected
4. The NSP sends the Approval or Reject notification
 - a. The request is approved. The NSP configures the CB in the CGU.
 - b. The request is rejected

In case of modification, the CB undergoes the change process as defined by the NSP, that receives the request and performs the standard validation against the information provided. If the validation is successful, the NSP evaluates if the order contains a change of the CGU. If there is a change of the CGU, the same approval flow is foreseen:

- Single approval is requested for orders submitted by a CB:
 - The T2 Operator does the approval.

	T2 Connectivity Guide	Page 12 of 16

For all other types of changes (e.g. the technical parameters), no external approval is required and the technical implementation can be executed by the NSP autonomously.

3.2.3 CB Authorised Approvers

Each CB supporting the T2 activities designates up to three people allowing them to approve or reject T2 NSP orders related to their participants. CB authorised users in the NSP specific web site section can manage the list of approvers independently. Alternatively, the following process which consists of the below steps can be used:

- The list of approvers has to be sent to the T2 Operator. It should include the BIC of the institution, the name, email address, telephone number and postal address of the approvers
- The T2 Operator sends the list to the NSP. Upon reception of the list, NSP registers the people referenced in the list and subsequently activates the CB BIC on the NSP web pages as approver for the registration. Procedures for maintaining the Authorised Approvers' list are further detailed in the NSP documentation.

4. Request for Digital Certificates by the NSP PKI

The NSP Public Key Infrastructure (PKI) provides digital certificates of the following kind:

- For the U2A channel: certificates on a smart-card, USB token or remote HSM;
- For the A2A channel: certificates on HSM for live traffic.

The procedure to procure the certificates is described in the NSPs User documentation.

4.1 Setting up security

Reference document(s)	<ul style="list-style-type: none"> ▪ NSPs own User documentation
------------------------------	---

The NSPs are responsible for providing a secure connection to and from T2 for those clients

subscribing to their services. The implementation of the security measures is managed by the NSP. Regarding the T2 Actors network interfaces, the NSPs provide the necessary support for the security setup.

For more information on the security aspects, see the NSPs documentation.

5. NSP documentation

Reference document	NSPs own User documentation
---------------------------	-----------------------------

The NSP shall provide all the necessary documentation regarding the access to A2A/U2A services so that the T2 Actors can connect to T2, including details on:

- T2 relevant URLs (GUI, Trouble Management System, CLM, RTGS, ...),
- T2 GUI Operability Requirements – needed hardware/software configuration to access T2 GUI,
- Access to the A2A services – addressing rules for Message/File exchange,
- PKI certificates procurement.

6. Connectivity checklist

The table below shows a quick summary of the steps to be taken in order to connect to T2 through a NSP:

Step	Action
1	Select the NSP of choice and select the related services.
2	Ask the NSP's for an offer and order the related products.
3	Subscribe to the NSP's Services for T2 (e.g. inclusion into the CGU).
4	Request for the NSP PKI certificates.
5	Connectivity setup with the NSP.
6	Connectivity test with T2 (during the connectivity test phase before entering relevant data in CRDM, in case of A2A connection the user will receive an admi.007 message reporting a validation error related to the configuration of the certificate, technical user, or both. In U2A mode the user will be able to reach the ESMIG landing page)

7. Troubleshooting and support

For technical problems in regards to the NSP connectivity, depending on the nature of the issue, the first level of support can be provided either by the NSP of T2 Actor or by the National Service Desk

of the Central Bank. In case of doubt, the T2 Operator should be contacted.

In case of need, the NSP's support and the T2 Operator can cooperate by means of a joint teleconference with the Central Banks.

T2 Actors can contact the NSP support teams 24 hours a day, seven days a week, all year round.


The NSP shall inform T2 Operator in advance of known problems and any corrective measures to be taken. Further details on the NSP's commitments are presented in the NSP's documentation.

8. Availability

The Connectivity Services provided by the NSP are available 24 hours per day, seven days per week, excluding a fixed maintenance window that should be defined within the documentation of each NSP. Whenever an additional maintenance window is required, both the T2 Operator and National Service Desk of the Central Bank should communicate in advance to the T2 Actors with a reasonable timeframe and if possible during the previous business day

9. Acronyms

Acronym	Full Text
A2A	Application to Application
BAH	Business Application Header
BFH	Business File Header
CB	Central Bank
CGU	Closed Group of Users
CRL	Certificate Revocation List
CSL	Certificate Suspension List
DEP	Data Exchange Protocol
HTTPs	Hyper Text Transfer Protocol secure
NSP	Network Service Provider
PKI	Public Key Infrastructure
U2A	User to Application
WMQ	WebSphere Message Queue
XML	Extensible Markup Language

	T2 Connectivity Guide	Page 15 of 16

10. Appendix

10.1 List of criteria for CGU subscription


Regarding the TEST environment (EAC and UTEST), the T2 Actors should have successfully performed the following steps to confirm their readiness to be registered within the T2 EAC and UTEST CGU:

- 1- Finalisation of the procurement of the NSP provider
- 2- Nomination of the NCB administrator and counterparty administrator and the organizational procedures related to the CGU management
- 3- The registration form should contain at least the following information:
 - ✓ Customer Information:
 - Legal name
 - BIC
 - User Name of the person submitting the form
 - ✓ Counterparty/NCB Approver BIC

Technical Identifiers for U2A/A2A (e.g. network addresses, IP, DN pattern,...) may also be included in the form if requested by the NSP

Regarding the PROD environment, the T2 Actors should perform the three steps described above for the TEST environment (EAC and UTEST) and in addition the following ones:

- 4- Successful realization of the following tests:
 - (i) **Connectivity testing** that enables to verify the communication between the users systems, the network and the platform in both U2A and A2A modes. It is validated through the correct sending and receiving of messages.
 - (ii) **Functional testing** with in particular the following objectives:
 - a. to verify the entire system and the interfaces between the various components work end-to-end and are compliant with the functional user requirements
 - b. the T2 Actors to ensure that their local systems are properly connected with the new services; and
 - c. the T2 Actors to execute test cases to ensure that they are technically, functionally and operationally ready to join the services.
 - (iii) **Community and business day:** Users, all together, shall
 - a. execute joint test cases defined together by the users to check the correct behaviour of the services;

	T2 Connectivity Guide	Page 16 of 16

b. execute their own test cases.

- (iv) **Operational tests:** Users, all together, shall check that the system-related parts of the operational procedures operate as expected and fulfil their needs in terms of operations as well in terms of overall process. Such procedures are described in the TARGET Manual of Operational Procedures (MOP), for Central Banks, and in the Information Guide for the participants;
- (v) **Migration:** Users, all together, are able to rehearse migration, check the correct behaviour of migration tools and correct migration of their data.