T2S Connectivity Guide

Author	4CB
Version	1.0
Date	29/11/2013
Status	Final
Classification	Public
Classified until	N/A

TABLE OF CONTENTS

1. INTRODUCTION

The T2S Connectivity Guide describes in general terms the VAN connectivity and aims at guiding the T2S Actors between the different relevant documents.

2. GLOBAL CONNECTIVITY OVERVIEW

2.1. Global picture

All T2S Actors, including central banks managing connected RTGS and Collateral Management Systems, can choose their preferred connection type(s) and will be fully responsible for their choices.

The T2S Actors with a direct access to T2S are called **Directly Connected T2S Actors (DiCoA**). They are Central Security Depositories (CSD), CSD participants having a contractual relation with the CSD, Central Banks (CB), and members of a banking community having a contractual relation with the CB.

The technical platform consists of different environments. Each of them is logically separated from the others and has a specific role in the T2S application life cycle.

T2S environments can be grouped into two logical categories:

- "Production", for live operations (one environment only);
- "Test & Training": this category includes several environments (up to four) dedicated for testing and acceptance activities.

2.2. Connectivity

Reference document(s)	▪ UDFS, § 1.3 "Access to T2S"

The Single Shared Platform hosting T2S is built on four sites over two regions (Region 1 and Region 2) directly connected to the Network Service Providers (NSP).

Communication availability is ensured over these two regions in accordance with a highly demanding business continuity model.

Region 1 and Region 2 host the core business T2S applications, while other less critical applications (e.g. archiving, statistical information) are hosted in Region 3. The communication between the Regions is realized through the internal T2S network (4CB Network). Contracting DiCoAs can access the T2S platform through a **Value Added Network Service Provider (VA-NSP)**, which has to provide the following services**:**

- Network connectivity;
- Messaging services in U2A and A2A mode;
- Security services: PKI and closed group of user (CGU) management;
- Operational services like support and incident management.

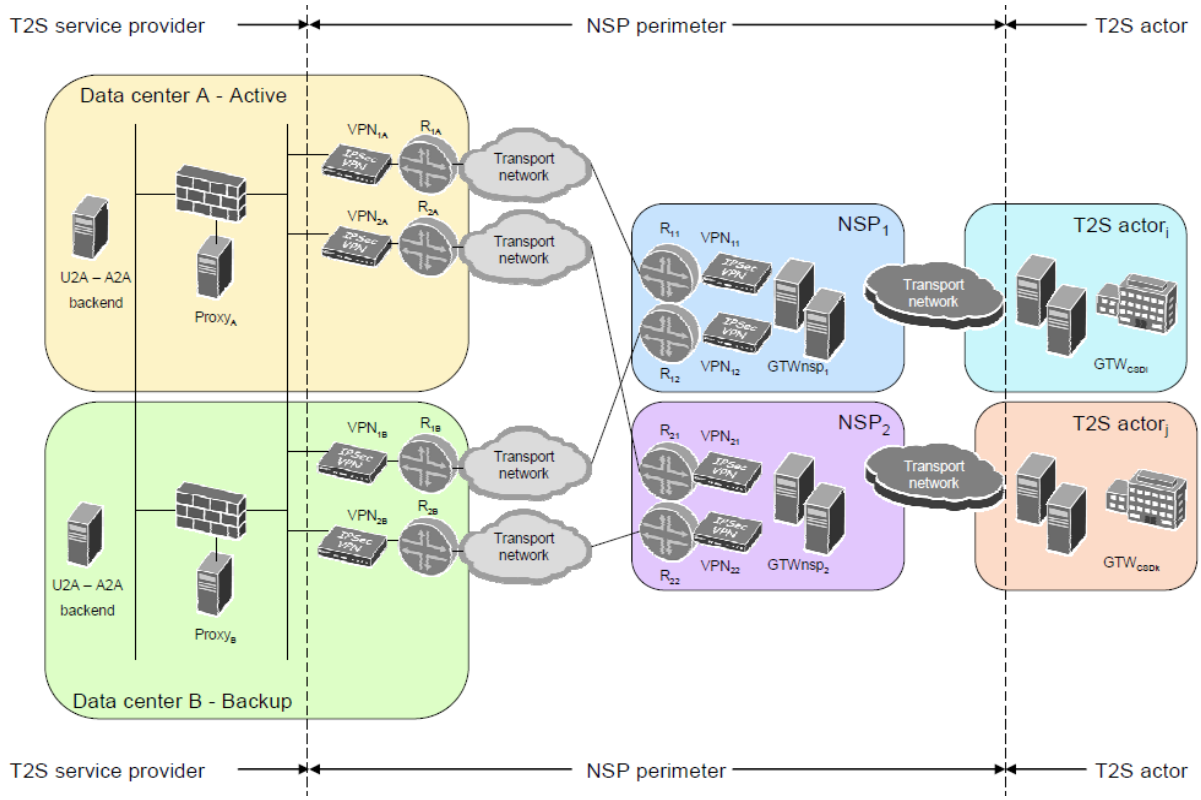

Figure 1 – Connection via VA-NSP (Technical Overview)

The picture above shows the DiCoAs' access to the T2S Platform using a Network Service Provider offering Value Added Services (VA-NSP): the NSP de-couples the

interface from the T2S Platform and from the DiCoAs and offers all services required to the T2S Platform and to the DiCoAs.

The licensed VA-NSPs connected to T2S are SWIFT and SIA/Colt.

2.3. The communication modes

Reference document(s)	▪ T2S External Networks. Technical Requirements (Attachment 1 to the Licence Agreement)[1] ▪ UDFS, § 1.7 “Limitations of the system”, § 3.2.2 Communication infrastructure, § 4.7 Digital signature on business layer

The DiCoAs’ applications and the end-users can communicate with T2S with two different modes: Application to Application (A2A) or User to Application (U2A).

2.3.1. A2A channel

For the A2A mode, the T2S Platform communicates with the DiCoAs 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" mode[2].

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 messaging service 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

[1] Documents related to T2S Connectivity Licenses are available at the following URL: http://www.ecb.europa.eu/paym/t2s/pdf/20120102_licence.zip?6fac78aa1040634a5a616eebe531bd9d

[2] Currently the possibility to exchange files in real time mode is not used by the T2S application.

unavailability of the receiver, the NSP stores messages and files for 14 calendar days and delivers them as soon as the receiver becomes available again.

All communication is in "push" mode, both from T2S to the DiCoAs and from the DiCoAs to T2S. The "push" mode refers to the originator of a message or file pushing it to the final receiver.

The A2A message and file exchange between T2S and the VA-NSP is based on a T2S protocol named DEP (Data Exchange Protocol). The protocol relies on XML messages, transported over an MQ connection and containing all the relevant information to address and describe messages and files.

The data exchange between the DiCoA and the VA-NSP is compliant with a protocol defined by the relevant VA-NSP and it is managed by the gateway of the DiCoA (i.e. the original sender) and the gateway of the VA-NSP. The VA-NSP offers connectivity services and manages the bi-directional data exchange with T2S Platform according to the DEP.

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

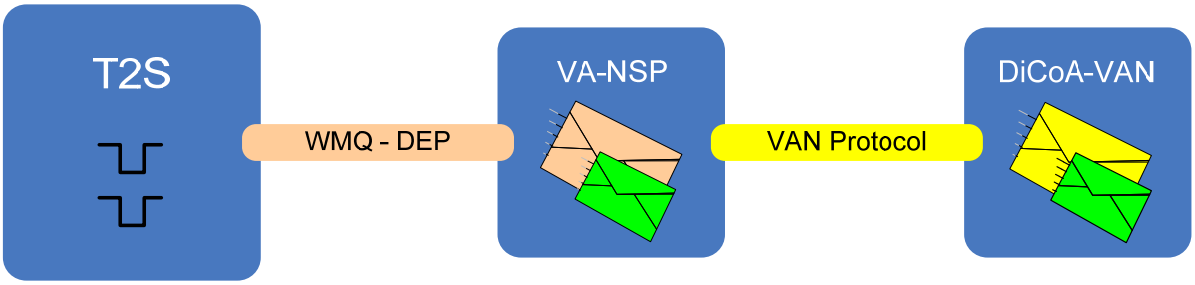

Figure 2 – Message/File Exchange Protocol

2.3.1.1. Message/File compression

For any types of outbound communication, T2S compresses the data only if this is required by the compression setting specified by the T2S Actor in the corresponding routing configuration. However, two exceptions are foreseen:

- if the outbound communication is smaller than 2KB, then T2S does not compress the data regardless of the setting;
- if the outbound communication is a report, then T2S compresses the data regardless of the setting.

All the XML business data has to be compressed including BAH or BFH. After compression, the compressed data has to be converted in BASE64 (i.e. ZIP deflate and the BASE64 RFC 2045) to be properly conveyed in the Business Envelope field of the DEP message. Data belonging to the network protocol (DEP ExchangeHeader) is not compressed. That is valid for messages sent by a T2S Actor as well as for the ones sent out by T2S.

The compression algorithm supported by T2S is the ZIP algorithm.

2.3.1.2. Message size

The Data Exchange Protocol (DEP) is used to exchange data between the T2S platform and the VA-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 T2S 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, T2S 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.

Technical solutions are available on T2S Platform in case the maximum size of 32 MB is exceeded by a T2S outbound communication flow. Further details about these functionalities can be found in the UDFS.

2.3.1.3. Message/File signature

The Messages/Files exchanged between T2S and DiCoAs are in general provided with two digital signatures:

- the Technical Envelope signature;
- the Business Layer signature (BAH signature for message and BFH signature for file).

The Technical Envelope signature

These signatures are performed by T2S and by the VA-NSP by means of digital certificates issued by the VA-NSP PKI.

The Business Layer signature

As described in the UDFS, 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 business application header (BAH) in case of individual messages or in the file header (BFH) in case of a file.

In outgoing communication, the signature is performed by T2S through a VA-NSP certificate.

In incoming communication, the signature has to be performed by the DiCoA with a VA-NSP certificate.

The VA-NSP will provide the necessary APIs to manage activities related to the signature, e.g. signing, verification of signature, check against directory services (such as CRL and/or CSL).

In addition, the VA-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 T2S User Detailed Functional Specifications available on the ECB website.

The certificates used are issued by the VA-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.

2.3.1.4. Delivery Notification signature

For incoming Store-and-Forward traffic, the VA-NSP sends a Delivery Notification upon reception by T2S of a Message/File to inform the DiCoAs who have chosen the option. The Delivery Notification is built by the VA-NSP using the Technical Acknowledgment from T2S and it carries the following pieces of information:

- the timestamp set by T2S when the Message/File was received;
- the digital signature generated by T2S of the received Message/File, included in the Technical Envelope signature.

2.3.1.5. Message Formats

The T2S application uses messages in ISO 20022 format. For information on the message format, please refer to the T2S User Detailed Functional Specifications available on the ECB website.

2.3.2. U2A channel

The U2A interface between T2S and the NSP is based on the standard HTTPs protocol; therefore HTTPs traffic between the users' workstations and the T2S platform must be enabled on the network devices at the DiCoA's side and at the T2S entry firewall. In this context the NSP has to provide mainly connectivity, CGU and PKI services.

DiCoA identification and authentication is based on digital client certificate. Certificates are provided by the VA-NSP and assigned to the end-users, stored with the related private keys in a smart-card or USB token.

3. NSP DOCUMENTATION

Reference document(s)	▪ VA-NSPs own User documentation

As per the Licence Agreement, Attachment 2 "Business requirements for T2S Network Service Providers", each NSP "ensure[s] the availability of comprehensive and clear documentation, as well as a support structure, that allows the DiCoA to implement the T2S connectivity services in a timely, cost-effective and resilient way".
The documentation shows:

- which technical solutions are available for different types of DiCoAs, and which options are available for DiCoAs to influence or deviate from those solutions;
- what documentation and support structure is available to potential DiCoAs, and which procedures have to be followed, in order to allow them to make an informed decision about the viability and cost-effectiveness of the DiCoA's T2S connectivity solutions;
- what documentation and support structure is available to actual DiCoAs and which procedures have to be followed, in order to allow them to implement their preferred T2S connectivity solution;
- what the different implementation stages are on the DiCoA's side, the mandatory and/or optional validation points, and which testing opportunities (and support) are available at these points.

4. USING THE CONNECTIVITY OPTIONS

Reference document(s)	▪ VA-NSPs own User documentation ▪ VA-NSPs Registration process (VAN-NSPs website)

4.1. Registration process

In order to become DiCoAs, potential T2S Actors need to complete the registration process defined by the VA-NSP of choice specifying the connectivity services and communication channels.

In any case, access to the T2S GUI (i.e. to the U2A channel) is mandatory for CSDs and CBs, since some functions are available only through this channel.

VA-NSPs restrict access to their Connectivity Services only to identified end-users, creating logically segregated groups of T2S DiCoAs called Closed Group of Users (CGU).

The CGUs are: (a) U2A only, (b) U2A + A2A, and separate CGUs are available for the Production environment and the Test & Training ones. Therefore on the NSP website two registration scenarios are available:

T2S Actor	CGU	Environment
CSD/CB/DCP	U2A only	Test & Training
		Production
	U2A + A2A	Test & Training
		Production

The registration process must be carried out for both Test&Training and Production.

The subscription to a group of users, and any subsequent modification to such subscription, is arranged through an electronic workflow on the relevant VA-NSP's website.

4.1.1. Registration process for a DCP

The forms contain at least the following information:

- Customer Information:
  - Legal name
  - BIC
  - User Name of the person submitting the form
- CSD/CB 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

The subscription of a DCP has to be approved by the relevant CSD or CB and then by the T2S operator according to the following sequence:

1. Subscription request on NSP website
2. NSP Validation
3. CSD/CB Approval
4. T2S Operator Approval

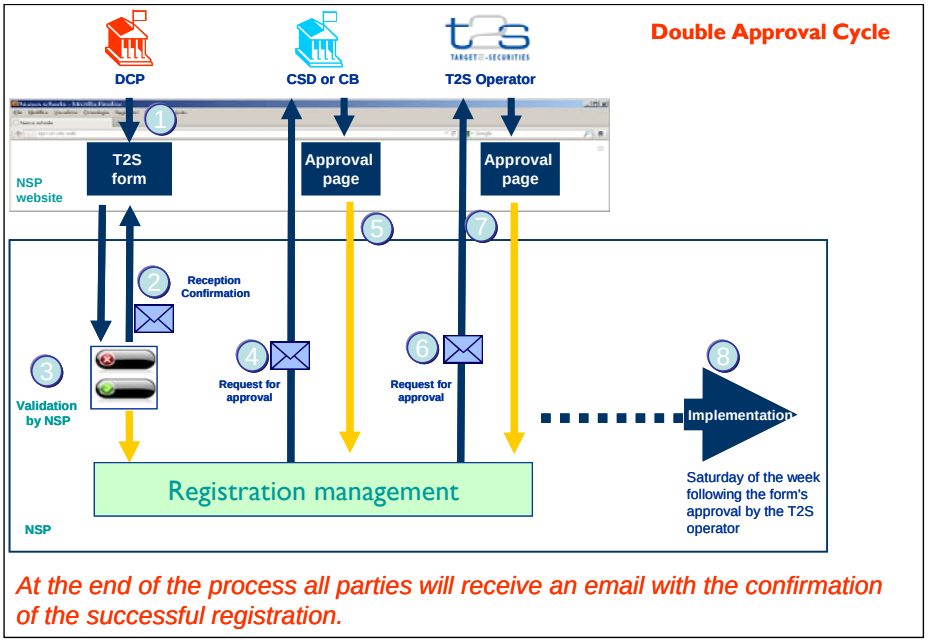

Figure 3 – Approval Cycle for DCP Registration

At the end of the process all parties receive an email with the confirmation of the successful registration.

Since a DCP can be linked to more than one CSD/CB, it has the possibility to select the BIC of the Approver directly in the form. Moreover, if the DCP needs to change something in the registration due to the link to another CSD, it may select the BIC of the second CSD as Approver in the form for change, if envisaged. As far as the VA-NSP is concerned, approval from the first relevant CSD/CB remains valid regardless of any additional relationship with other CSD/CBs.

In the picture below is an example of a DCP linked to more than one CSD: the two CSDs migrate in two different waves.

The T2S Service Desk contacts the Approver CSD if conflicting information is provided in the change form.

The DCP's CSD or CB have access to the forms of all the DCPs that have selected them as Approver (both for Registration and Change forms), while the T2S Operator can see all the forms. This helps supporting the DCP in any connectivity issue (e.g. inconsistency in the Static Data setup).

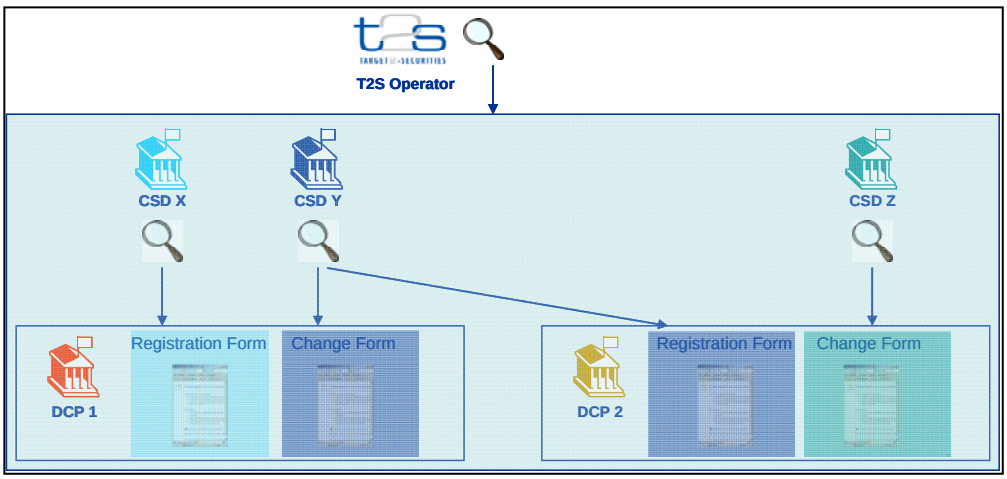

Figure 4 – Visibility of the different Actors on the Registration Process

CSD/CB Authorized Approvers

Each CSD/CB supporting the T2S activities for a DCP designates up to three people who are allowed to approve or reject T2S NSP orders related to the DCP. The list has to be sent to the T2S Service Desk provided with BIC, name, email, telephone and address.

The T2S Service Desk sends the list to the NSP. Upon reception of the list, VA-NSP registers the people referenced in the list and subsequently activates the CSD/CB BIC on the NSP web pages as approver for the registration.

Procedures for maintaining the Authorized Approvers' list are further detailed in the VA-NSP documentation.

Test&Training

The DCP subscription to Test&Training automatically implies the provisioning on all the test environments.

The Eurosystem will make the different test environments available according to the schedule depicted in the image below.

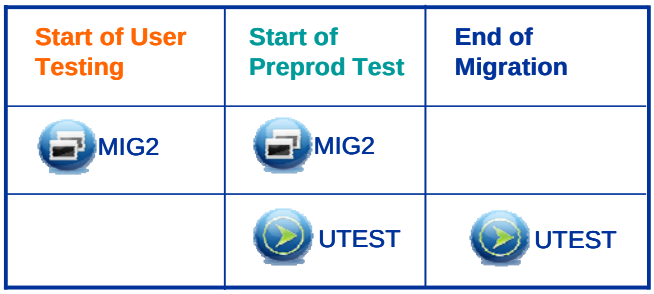

Figure 5 – Provisioning of the Test environments for DCPs

The UTEST test environment will remain in place after the go-live of the final migration wave in T2S.

4.1.2. Registration process for a CSD/CB

The forms contain at least the following information:

- Customer Information:
  - Legal name
  - BIC
  - User Name of the person submitting the form
  - Technical Identifiers for U2A/A2A (e.g. network addresses, IP, DN pattern,…) if requested by the NSP

The subscription of CSDs/NCBs can be approved by the T2S Operator only, according to the following sequence:

1. Subscription request on the NSP website
2. NSP Validation
3. T2S Operator Approval

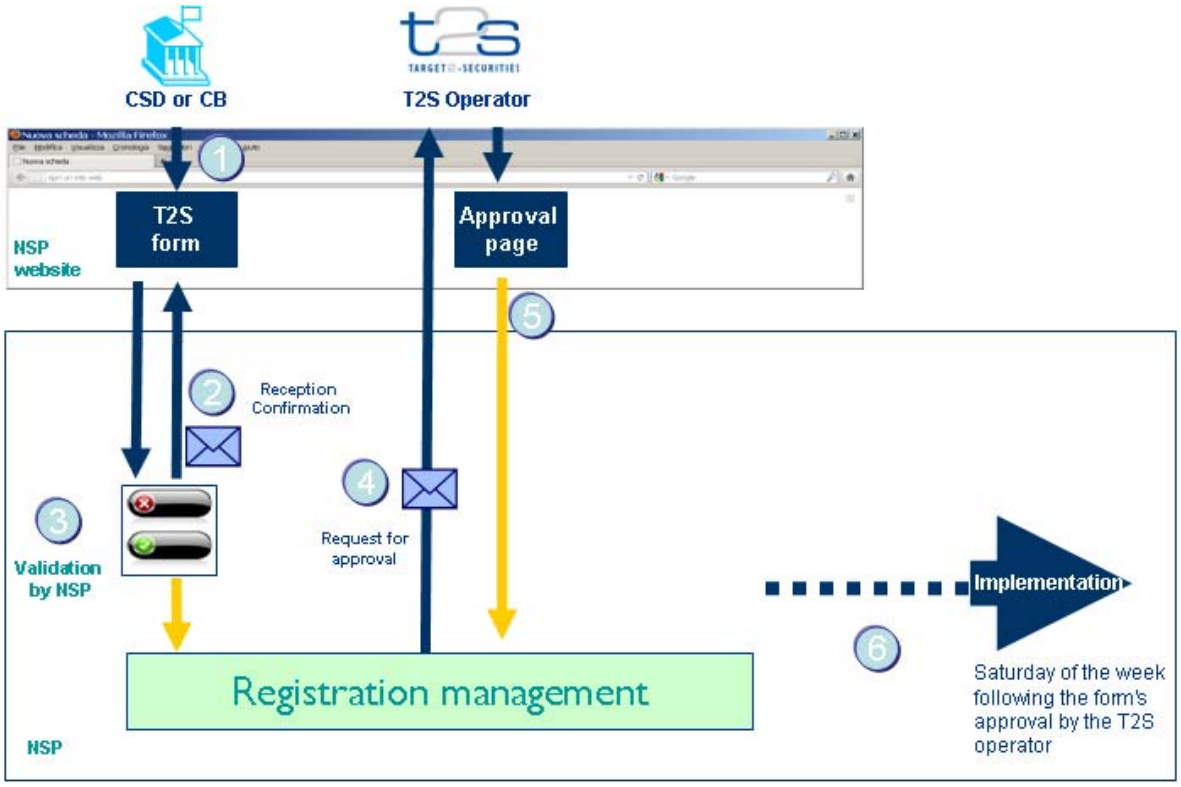

Figure 6 – Approval Cycle for CSD/CB Registration

At the end of the process all parties receive an email with the confirmation of the successful registration.

Test & Training

The CSD/CB subscription to Test&Training automatically implies the provisioning on all the test environments

The Eurosystem will make the different test environments available according to the schedule depicted in the image below.

Start of Pilot testing	Start of User Testing	Start of Preprod Test	End of Migration
EAC	EAC	EAC	EAC
	MIG1	MIG1	
	MIG2	MIG2	
		UTEST	UTEST

Figure 7 – Provisioning of the Test environments for CSDs/CBs

The EAC and UTEST test environments will remain in place after the go-live of the final migration wave into T2S.

4.1.3. Change process

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

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

- Dual approval is requested for orders submitted by DCP:
  - First approval is done by the responsible CSD/CB;
  - Second approval is done by the T2S Operator.
- Single approval is requested for orders submitted by CSD/CB:
  - Approval is done by the T2S Operator.

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 VA-NSP autonomously.

4.1.4. Request for Digital Certificates by the VA-NSP PKI

The VA-NSP PKI provides digital certificates of the following kind:

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

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

4.2. Setting up security

Reference document(s)	▪ VA-NSPs own User documentation

The VA-NSPs are responsible for providing a secure connection to and from T2S for those clients subscribing to their services. The implementation of the security measures is managed by the VA-NSP. Regarding the DiCoAs network interfaces, the VA-NSPs provide the necessary support for the security setup.

For more information on the security aspects for DiCoA-VANs, see the VA-NSPs documentation.

4.3. Setting up parties and users

Reference document(s)	▪ UDFS, § 1.2 “Configuration of Parties, Securities and Accounts” ▪ UDFS, § 1.3 “Access to T2S” ▪ User Handbook, § 3.8 “Party Management“ ▪ User Handbook, § 3.2 “Access Rights”

The T2S Operator is responsible for setting up and maintaining party Static Data for all CSDs and NCBs in T2S. Similarly, CSDs are responsible for setting up and maintaining party Static Data for their CSD participants and for other CSDs that are external to T2S, whereas NCBs have the same responsibility assigned for setting up their Payment Banks.

The following table summarises, for each Static Data object related to the setup of parties in T2S, the responsible T2S Actor for its configuration and it specifies which mode the T2S Actor can use for the configuration.

Party Type	Responsible T2S Actor	Mode
CSD	T2S Operator	U2A
NCB	T2S Operator	U2A
CSD Participant	CSD	A2A/U2A
Payment Bank	NCB	A2A/U2A
External CSD	CSD	A2A/U2A

For each Party in T2S, at least one Technical Address has to be set up at the moment of the Party's creation (further Technical Address can be set up afterwards). The Technical Address then has to be connected to one of the available Network Services through a Technical Address Network Service Link.

Further steps in order to make the message exchange between T2S and the T2S Actor properly functioning are:

- set up the default and conditional routing configurations (in order to specify the technical elements T2S uses to send outgoing messages to the relevant T2S Actor);
- configure the message subscription (the specific set of messages, or copies of messages, they want to receive from T2S).

Users are likewise defined in Static Data. Users belonging to CSDs and NCBs can create users for their own Parties or for their CSD Participants or Payment Banks respectively. Users belonging to a CSD Participant, External CSD, or Payment Bank can only create users for their own party.

It is a responsibility of the parties to ensure consistency between the Static Data and the information provided in their registration to the Closed Group of Users.

5. ACCESS TO THE U2A SERVICES

5.1. T2S GUI URLs

In the user documentation provided by the VA-NSP of choice the URLs for the access to the T2S GUI, the Trouble Management System and the Long-Term Statistical Module are reported.

5.2. T2S GUI Operability Requirements

For the T2S GUI Operability Requirements, please refer to the VA-NSPs User documentation.

6. ACCESS TO THE A2A SERVICES

The Message/File exchange is performed as per the addressing rules defined by the VA-NSP of choice and outlined in the VA-NSP's documentation.

7. BUSINESS CONTINUITY

Reference document(s)	▪ T2S External Networks. Technical Requirements (Attachment 1 to the Licence Agreement)

The VA-NSPs support the T2S Business Continuity imperceptibly to the DiCoAs, i.e. without any necessary intervention or impact on their technical configuration.
In the case of a T2S intra-region recovery (between primary and secondary Site in the same region), the NSP shall switch the traffic between the sites in less than 15 minutes.
In the case of a T2S inter-region recovery (between two Regions), the NSP shall switch the traffic between the Regions in less than 30 minutes.

On periodic rotation occurrences (almost every six months), the NSP shall switch the traffic between the Regions during a week-end in less than 30 minutes (planned operation).

The NSP shall manage its own disaster recovery solution, which affects the T2S Connectivity Services, with the following objectives:

- In the case of a NSP intra-region recovery, the NSP shall switch the traffic to its back-up site in less than 15 minutes. The T2S active site will not switch over to the T2S back-up site.
- In the case of a NSP regional disaster, the T2S active Region will not switch to the second Region. The Directly Connected T2S Actors served by the NSP will lose access to T2S until the NSP restores the Connectivity Services. The procedures supporting the VA-NSP disaster recovery are defined by the VA-NSP of choice and outlined in the VA-NSP's documentation.

8. PRICING

Reference document(s)	▪ List of maximum prices (Attachment 4 to the Licence Agreement)

The maximum prices applied by the VA-NSP shall cover all activities and components that allow a DiCoA to make use of the Connectivity Services.~~,~~

The NSP shall be obliged to supply, and charge accordingly, the services included in the Attachment 4 to the Licence Agreement, which are necessary for a DiCoA to make use of the Connectivity Services efficiently and securely. Should a DiCoA require higher service levels for certain services than the ones specified in the Licence Agreement and its Attachments as the basis for the maximum prices, the NSP shall not be bound by the maximum price specified for these services.

9. CHECKLIST

The table below shows a quick summary of the steps to be taken in order to connect to T2S through a VA-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 T2S (e.g. inclusion into the CGU).
4	Request for the VA-NSP PKI certificates.
5	Connectivity setup with the NSP.
6	Create the Party in T2S Static Data according to the T2S registration procedure: ▪ if the Party to be created is a CSD or NCB, the T2S Operator is responsible for this step; ▪ if the Party is a CSD Participant, External CSD, or Payment Bank, the relevant CSD or NCB is responsible.
7	Link the Party to the Network Service of choice in Static Data.
8	Create the users, set up the related Certificate-DN links, and assign role/privileges to them according to their functions.
9	Set up statements and reports in Static Data.
10	Connectivity test with T2S.

10. TROUBLESHOOTING AND SUPPORT

For technical problems in regards to the VA-NSP connectivity, depending on the nature of the issue, the first level of support can be provided either by the NSP of choice or by the T2S Service Desk. In case of doubt, the T2S Service Desk should be contacted.

In case of need, the VA-NSP's support and the T2S Service Desk can cooperate by means of a joint teleconference with the DiCoA.

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

The NSP shall inform T2S in advance of known problems and any corrective measures to be taken. Further details on the NSP's commitments are presented in the VA-NSP's documentation.

11. AVAILABILITY

The Connectivity Services are available 24 hours per day, seven days per week, excluding a maintenance window during the weekend from 17:00 CET on Saturday to 08:00 CET on Sunday.

12. 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
CSD	Central Securities Depositories
CSL	Certificate Suspension List
DCP	Directed Connected Party
DEP	Data Exchange Protocol
DiCoA	Directly Connected Actor
HTTPs	Hyper Text Transfer Protocol secure
NSP	Network Service Provider
PKI	Public Key Infrastructure
U2A	User to Application
VAN	Value Added Network
VA-NSP	Value Added Network Service Provider
WMQ	WebSphere Message Queue
EAC	Interoperability
MIG1	Migration
MIG2	Community

UTEST	Pre-production