TARGET Services Connectivity Guide

Author	4CB
Version	1.0
Date	10/08/2021
Status	Final
Classification	Public
Classified until	N/A

Table of contents

History of releases

RELEASE	DATE	ISSUES	STATUS
V1.0	06/08/2021	Approved by the CSG/NECSG and the MIB	FINAL

Applicable documents

REFERENCE	OBJECT

Reference documents

REFERENCE	OBJECT

1. Introduction

The TARGET Services Connectivity Guide describes in general terms the connectivity to the Eurosystem Single Market Infrastructure Gateway (ESMIG). The ESMIG provides a single access point for Directly Connected Actors (DiCoAs) - henceforth called TARGET Services 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 is applicable for T2S, T2 and TIPS[1] and is valid for both production and test environments.

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

2. Global Connectivity Overview

2.1 Connectivity

The TARGET Services rely on the ESMIG for the communication with TARGET Services Actors. The ESMIG is the common entry point for all interactions with the Eurosystem Market Infrastructures and applications (T2, T2S, TIPS, ECMS and potential future services). It allows TARGET Services Actors to connect through one or multiple NSPs.

The ESMIG supports the connectivity of TARGET Services Actors as follows:

- A2A (Application-to-Application): it refers to the 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): it is the communication between ESMIG and the individual users of TARGET Services, via the online screen called Graphical User Interface (GUI).

[1] ECMS scope will be included at a later stage

2.2 The communication modes

Users - individuals or applications - can communicate with TARGET Services in two different modes: Application to Application (A2A) or User to Application (U2A) in case of the user is an application or individual respectively.

2.2.1 A2A channel

The A2A message and file exchange between TARGET Services and the NSP is based on a proprietary protocol named DEP (Data Exchange Protocol) except the TIPS instant payments which use the MEPT (Message Exchange Protocol for TIPS) protocol.

Both protocols rely 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 a TARGET Service Actor and an NSP is compliant with a protocol defined by the relevant NSP and it is managed by the network gateway provided by the NSP to the TARGET Service Actor and the network gateway of the NSP, supporting the interface to the TARGET Services.

The NSP offers connectivity Services and manages the bi-directional data exchange with TARGET Services Platform according to both DEP and MEPT.

For the A2A mode, the TARGET Services Platform communicates with the TARGET Services Actors using the following transfer modes:

- The "real-time" transfer mode 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 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 TIPS specific “instant messaging” message transfer using “stateless” messages. This implies that if the receiver is unavailable, no retry mechanism is in place. Any communication is in "push" mode.

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

2.2.2 DEP Protocol features

2.2.2.1 Message/File compression

For any types of outbound communication, the ESMIG compresses the data only if this is required by the compression settings specified by the TARGET Services Actor in the corresponding routing configuration. If the size of 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 TARGET Services Actor as well as for the ones sent out by the TARGET Services.

ESMIG does not process decompressed communication which size exceeds 99 MB. In this case, ESMIG will reject the message and send back a Negative Acknowledgement (NAN) message to the NSP.

2.2.2.2 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, shall be found in the ESMIG UDFS. However, T2S Actors shall continue to refer to the T2S UDFS, which will be the correct reference until November 2023. From that point on, the ESMIG UDFS will replace the relevant parts of the T2S UDFS and will therefore become the reference for all TARGET Services Actors.

2.2.2.3 Message/File signature

The Messages/Files exchanged between TARGET Services platform and TARGET Services 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 a NSP certificate.

  In incoming communication, the signature has to be performed by the TARGET Services Actors with a 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 certificate revocation status 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 or for T2S Actors, to the T2S UDFS until November 2023.

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).

2.2.2.4 Delivery Notification signature

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

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

2.2.2.5 Message Formats

The TARGET Services application uses messages in an ISO 20022 compliant format. For information on the message format, please refer to the ESMIG UDFS or for T2S Actors, to the T2S UDFS until November 2023.

2.2.3 U2A channel

The U2A interface between TARGET Services and the NSP is based on the standard Hyper Text Transfer Protocol secure (HTTPs) protocol; therefore, HTTPs traffic between the users' workstations and TARGET Services must be properly configured on the customer device and at the ESMIG entry firewall. In this context, the NSP must provide mainly connectivity, CGU (Closed Group of Users) and PKI Services. TARGET Services 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 or 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)	▪ NSPs own User documentation ▪ NSPs Registration process (NSPs website)

3.1 Network Service Provider selection

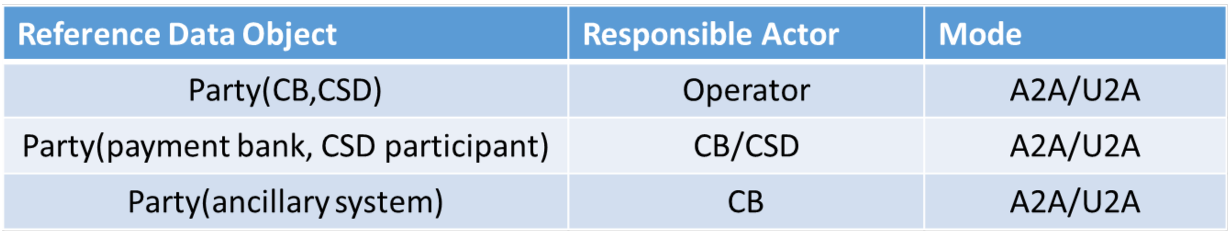
TARGET Services Actors registration is mainly supported by the establishment of a contractual relationship between them and the NSP. Once a TARGET Services Actor has established the contractual relationship with NSP and nominated their representatives (admin) then they are also registered in the NSP Website.

3.2 Set-up of parties

A party is defined as a legal entity or an organization interacting with TARGET Services.

The relevant operator is responsible for setting up and maintaining party reference data for all CBs and CSDs relevant for TARGET Services. CBs and CSDs 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 TARGET Services and specifies the required communication mode:



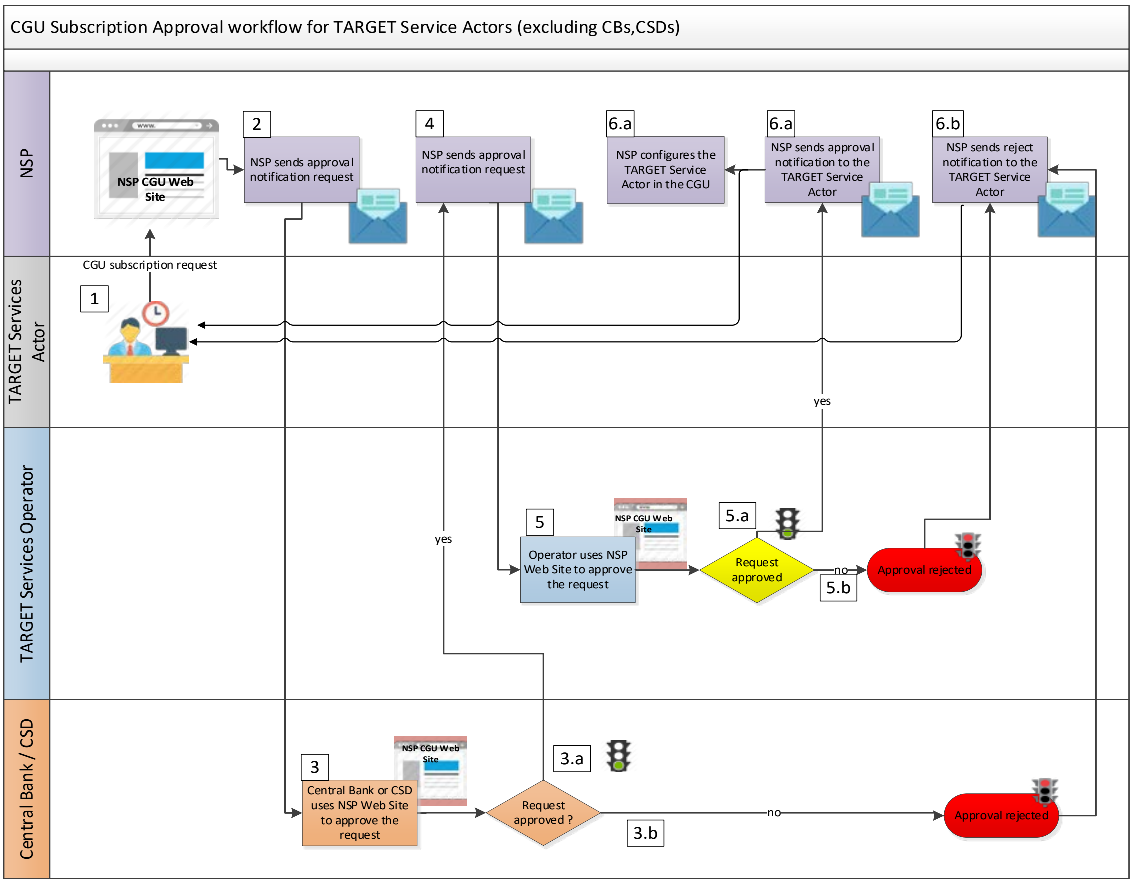
Reference Data Object	Responsible Actor	Mode
Party(CB,CSD)	Operator	A2A/U2A
Party(payment bank, CSD participant)	CB/CSD	A2A/U2A
Party(ancillary system)	CB	A2A/U2A

3.3 CGU subscription

The NSP shall create and manage CGUs (Closed Group of Users) containing the relevant TARGET Services Actors for both the Production environment (PROD) and the Test environment (UTEST and EAC), one CGU for each environment and for each Eurosystem Market Infrastructure (T2, T2S, TIPS, ECMS and potential future services). 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 or CSD, where applicable, and the relevant TARGET Services Operator. After the form's approval by the TARGET Services Operator, the NSP and the TARGET Services Actor agree the activation date for the subscriptions; the activation date should be 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 TARGET Services Operator, the NSP shall withdraw from the CGU a TARGET Services Actor within one hour.

3.3.1 CGU subscription for TARGET Services Actors (excluding CBs, CSDs)

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


CGU Subscription Approval workflow for TARGET Service Actors (excluding CBs,CSDs)
NSP
TARGET Services Actor
TARGET Services Operator
Central Bank / CSD
NSP CGU Web Site
CGU subscription request
1
2
NSP sends approval notification request
4
NSP sends approval notification request
6.a
NSP configures the TARGET Service Actor in the CGU
6.a
NSP sends approval notification to the TARGET Service Actor
6.b
NSP sends reject notification to the TARGET Service Actor
yes
5
NSP CGU Web Site
Operator uses NSP Web Site to approve the request
5.a
Request approved
no
5.b
Approval rejected
yes
3
NSP CGU Web Site
Central Bank or CSD uses NSP Web Site to approve the request
Request approved ?
3.a
3.b
no
Approval rejected

1. The TARGET Services Actor submits the subscription request through the NSP website.
2. The NSP validates technically the request and sends the approval notification request to the CB/CSD.
3. The CB/CSD checks the subscription request in the NSP website.
   a. The request is approved
   b. The request is rejected
4. In case the subscription request is approved by the CB/CSD, the NSP sends the approval notification request to the relevant TARGET Services Operator.
5. The relevant TARGET Services 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 TARGET Services Actor in the CGU.
   b. The request is rejected

In case of a modification request, the TARGET Services 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.

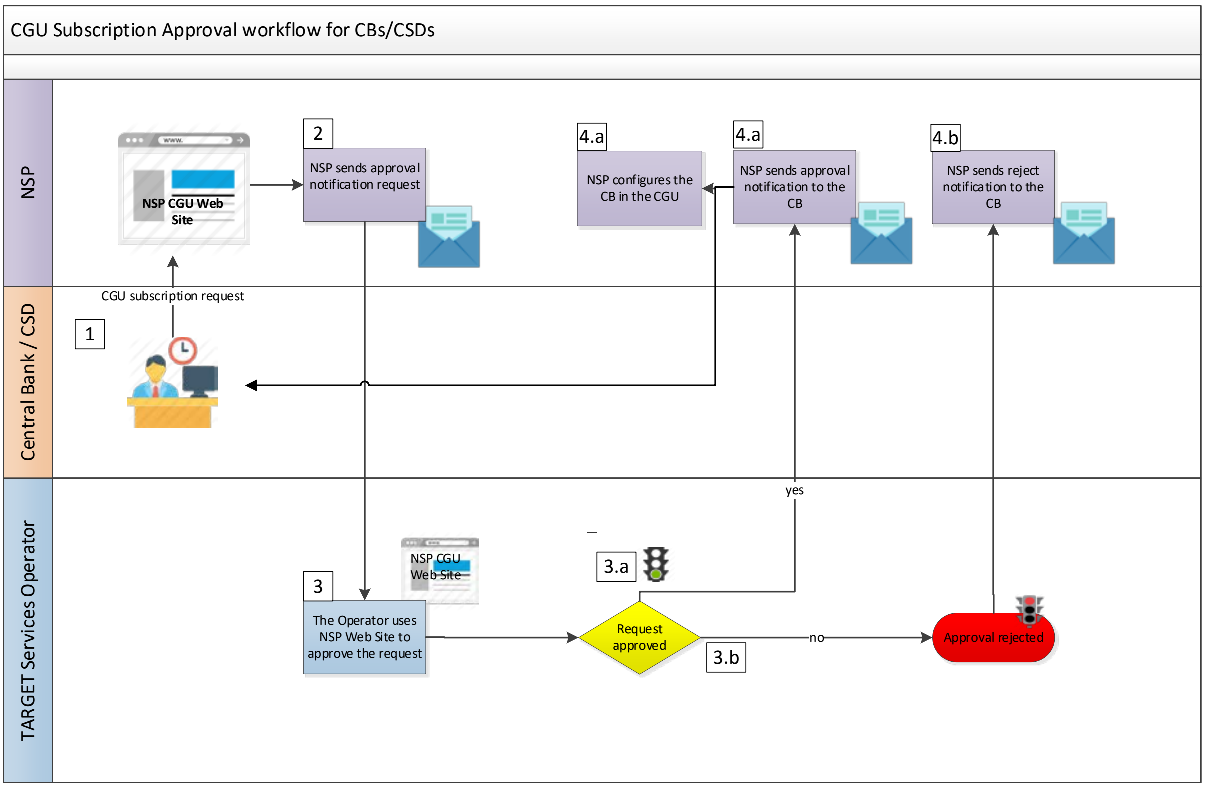
If there is a change of the CGU, the same approval flow is foreseen:

- Dual approval is requested for orders submitted by a TARGET Services Actor (other than a CB):
  - The responsible CB/CSD performs the first approval;
  - The relevant TARGET Services 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.

3.3.2 CGU subscription for CBs/CSDs

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


CGU Subscription Approval workflow for CBs/CSDs
NSP
Central Bank / CSD
TARGET Services Operator
NSP CGU Web Site
CGU subscription request
1
2
NSP sends approval notification request
4.a
NSP configures the CB in the CGU
4.a
NSP sends approval notification to the CB
4.b
NSP sends reject notification to the CB
3
The Operator uses NSP Web Site to approve the request
NSP CGU Web Site
3.a
Request approved
yes
no
3.b
Approval rejected

1. The CB or CSD 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 responsible TARGET Services Operator.
3. The TARGET Services 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 or CSD in the CGU.
    b. The request is rejected

In case of modification, the CB or CSD 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/CSD:
  - o The relevant TARGET Services Operator does the 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.

3.3.3 CB/CSD Authorised Approvers

Each CB or CSD supporting the TARGET Services activities designates a limited list of people allowing them to approve or reject TARGET Services NSP tickets for CGU subscription related to their participants. Two processes are defined in order to have CB or CSD “authorized approver” users registered in the NSP web portal to manage CGU subscription tickets and it is up to the NSP to decide which one to implement (or both) .

CB or CSD is registered in the NSP web portal and their admin users authorise users in the NSP specific web site section to 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 responsible TARGET Services Operator. It should include the identification of the institution (name and/or BIC), the name and email address of the approvers
- The TARGET Services Operator in charge sends the list to the NSP. Upon reception of the list, NSP registers the people referenced in the list and subsequently activates the CB/CSD 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 or USB token or remote HSM;
- For the A2A channel: certificates on HSM for test and prod traffic.

The same certificate can be used for all the TARGET Services.

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

4.1 Setting up security

Reference document(s)	▪ NSPs own User documentation

The NSPs are responsible for providing a secure connection to and from TARGET Services for those clients subscribing to their Services. The implementation of the security measures is managed by the NSP. Regarding the TARGET Services 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 TARGET Services Actors can connect to TARGET Services, including details on:

- ESMIG Portal URL
- TARGET Services GUI Operability Requirements – needed hardware/software configuration to access TARGET Services 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 TARGET Services 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	Connectivity setup with the NSP.
4	Subscribe to the NSP's Services for TARGET Services (e.g. inclusion into the CGU).
5	Request for the NSP PKI certificates.
6	Connectivity test with TARGET Services A2A • in case of schema validation error, the user will receive an admi.007 message • business validation errors will trigger the relevant business response message (eg. Pacs.002, camt.025 and reda.xxxaccording to the service/component the message has been sent to) U2A • 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 TARGET Services Actor or by the National Service Desk of the Central Bank. In case of doubt, the relevant TARGET Services Operator should be contacted.

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

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

The NSP shall inform TARGET Services 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, applicable only for TARGET Services using the DEP interface[2], that should be defined within the documentation of each NSP. Whenever an additional maintenance window is required, the responsible TARGET Services Operator, National Service Desk of the Central Bank and Central Securities Depositories (CSDs) should communicate in advance to the TARGET Services Actors with a reasonable timeframe and if possible during the previous business day.

9. TARGET Services Specific Information

This is placeholder to be used for information relevant for specific TARGET Services (e.g. ECMS).

10. 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
MEPT	Message Exchange Processing for TIPS
NSP	Network Service Provider
PKI	Public Key Infrastructure
U2A	User to Application
WMQ	WebSphere Message Queue
XML	Extensible Markup Language

[2] All TARGET Services except TIPS which does not use the DEP

11. Appendix

11.1 List of criteria for CGU subscription

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

1- Finalisation of the procurement of the NSP provider

2- Nomination of the NCB/CSD administrator or participant administrator depending on the TARGET Service Actor, and the organizational procedures related to the CGU management

3- The NSP registration form should contain at least the following information:

- ✓ Customer Information:

  Legal name

  BIC (optional)

  User Name of the person submitting the form

- ✓ CB/CSD Approver BIC or Institution Name

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

These registration forms shall be filled within the NSP website.

Regarding the PROD environment, the TARGET Services 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 TARGET Services Actors to ensure that their local systems are properly connected with the new Services; and

c. the TARGET Services 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 to check the correct behaviour of the Services;

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 Manual of Operational Procedures (MOP) of the relevant TARGET Service, for Central Banks and CSDs, and in the relevant Information Guide, if applicable, 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.