TARGET Services Connectivity Guide

Author	4CB
Version	3.1
Date	07/10/2024
Status	Final
Classification	Public
Classified until	N/A

History of releases

RELEASE	DATE	ISSUES	STATUS
V1.0	06/08/2021	Approved by the (NE)CSG and the MIB	FINAL
V2.0	30/06/2022	Extension to the ECMS. Approved by the (NE)CSG and the MIB	FINAL
V2.1	08/02/2023	Enhancements of ECMS specifics	DRAFT
V2.2	06/03/2023	Enhancements of ECMS specifics – Incorporation of ECMS-WG comments (Intermediary version to be removed before the publication)	FINAL
V3.0	15/03/2024	Enhancements of ECMS specifics - Annual revision of the documentation	FINAL
V3.1	07/10/2024	Editorial updates to reflect the TIE test environment	

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.

The content of this Guide is valid for all TARGET Services, unless specified otherwise in the chapter specific to a given Service. This connectivity 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).

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 the user is an application or individual respectively.

2.2.1 A2A channel

2.2.1.1 A2A channel between TARGET Services and the NSP

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.

2.2.1.2 A2A channel between TARGET Service Actor and the NSP

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, except for the ECMS which uses only the store and forward mode in A2A:

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

[1] Only T2S allows to specify the compression settings.

2.2.2.2 Message size

The DEP is used to exchange data between the 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 and to the relevant TARGET

Service technical specifications. T2S Actors will refer 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 an 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. Where relevant, the party type Central Bank will also be designated as (National) Central Bank with the acronym (N)CB to cater for ECMS specifics. The ECMS scope defining documents refer to National Central Bank.

The relevant operator is responsible for setting up and maintaining party reference data for all (N)CBs, CSDs and TPAs relevant for TARGET Services. (N)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:

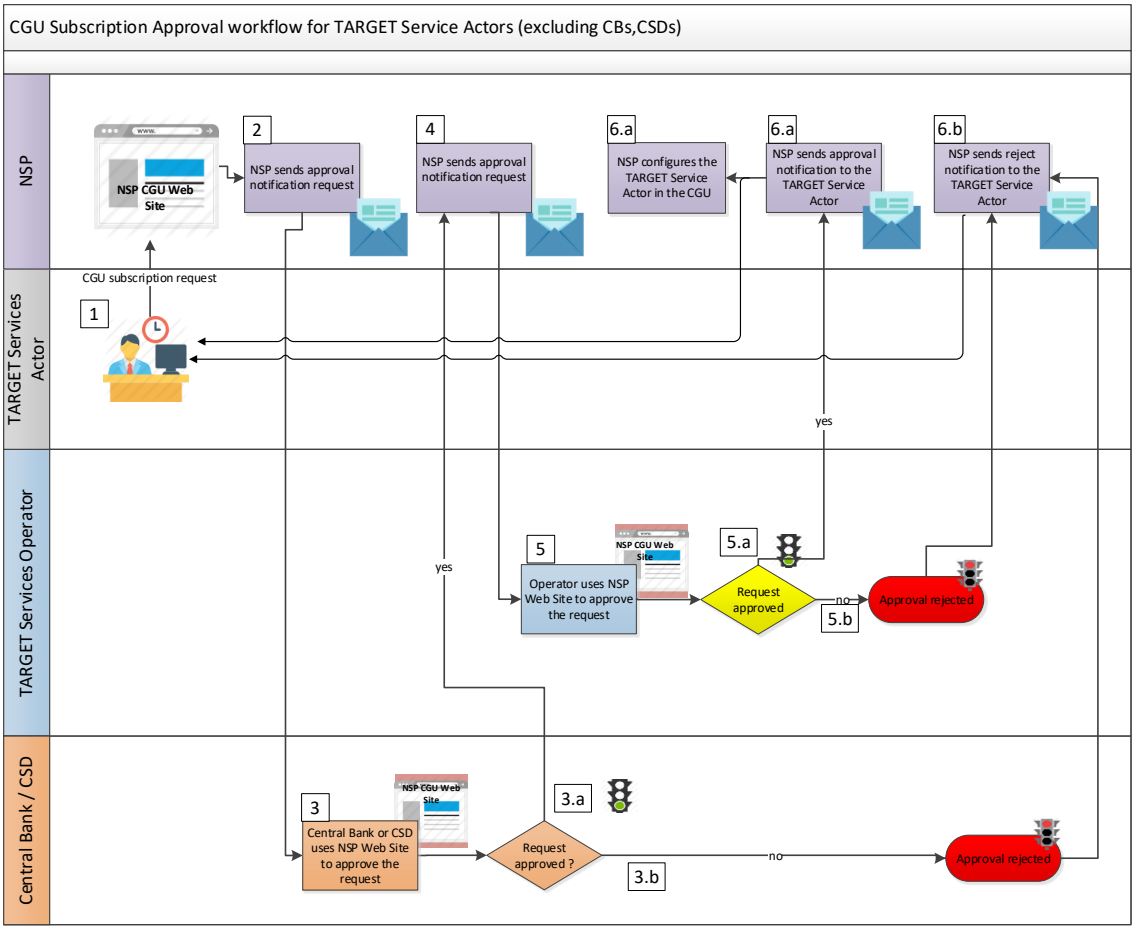
Reference Data Object	Responsible Actor	Mode
All TARGET Services (except ECMS)		
Party (CB, CSD)	Operator	A2A/U2A
Party (payment bank, CSD participant)	CB/CSD	A2A/U2A
Party (ancillary system)	CB	A2A/U2A
ECMS		
NCB	Operator	A2A/U2A
CSD/TPA	Operator	A2A
NCB's Counterparties	NCB	A2A/U2A

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 (TIE, EAC and UTEST), 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 (National) 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 and TPAs)

The CGU subscription includes a two steps approval workflow as described in the figure below: In the ECMS context, only NCBs and the ECMS Operator can approve the CGU subscription requests.



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 (N)CB/CSD.
3. The (N)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 (N)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.

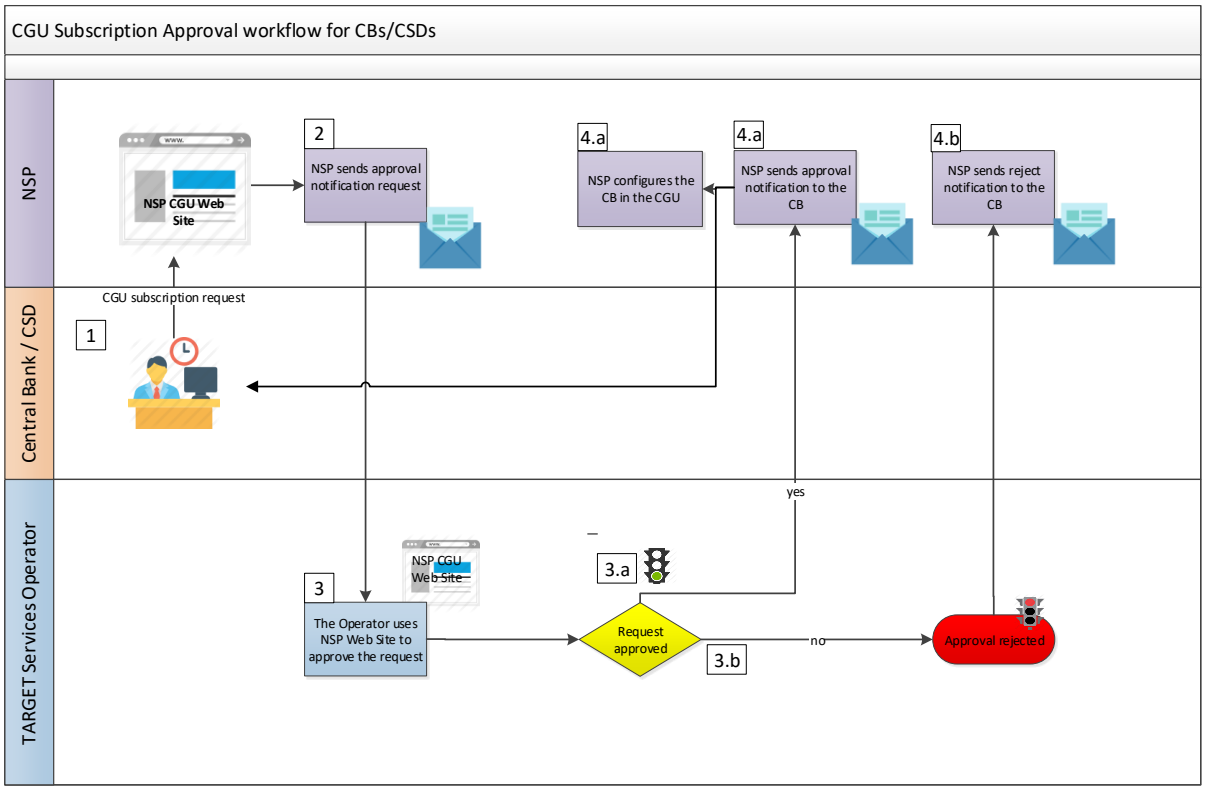
If there is a change of the CGU, the same approval flow is foreseen:

- Dual approval is requested for orders submitted by a TARGET Services Actor (other than a CB):
    - The responsible (N)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/TPAs

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



1. The (N)CB, CSD or TPA 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, CSD and TPA 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 (N)CB/CSD/TPA:
    - 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 (N)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 (N)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).

(N)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 NSP. It should include the identification of the institution (name and/or BIC), the name and email address of the approvers
- . Based on the NSP selected the list can be communicated as follows:
    - SWIFT:
        - By sending an email to End-to-End.Ordering@swift.com
        - By opening a case in the Case Manager on SWIFT.COM
    - SIA
        - By sending an email to ESMIG-NSP@sia.eu

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 an NSP:

Step	Action	TARGET Service
1	Select the NSP of choice and select the related Services.	ALL
2	Ask the NSP's for an offer and order the related products.	ALL
3	Connectivity setup with the NSP.	ALL
4	Subscribe to the NSP's Services for TARGET Services (e.g. inclusion into the CGU).	ALL
5	Request for the NSP PKI certificates.	ALL
6	Create the Party in Reference Data in ECMS	ECMS
7	Create Party administrators in ECMS	ECMS
8	Create the users and the Distinguish Name in ECMS	ECMS
9	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 (e.g. admi.007[2], pacs.002, camt.025 and reda.xxx according to the service/component the message has been sent to) U2A • the user will be able to reach the ESMIG landing page	ALL

The steps 6 to 8 are also valid for other TARGET services but for those services, they are not prerequisites to connectivity test while they are for the ECMS. Step 9 has also some peculiarities in relation to the ECMS.

Further details on steps 6 to 9 are provided in the section 9.1 ECMS service, especially in sub-section 9.1.2 Connectivity check list – ECMS specifics and sub-section 9.1.4 Proof of effective A2A connectivity to ECMS.

[2] Admi.007 is returned as a result of business validation errors only for ECMS

7. Troubleshooting and support

For technical problems with 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, this Central Bank will contact the Operator of the related TARGET Service.

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 the Operator of the TARGET Service affected by the issue 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[3], 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.

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

9. TARGET Services Specific Information

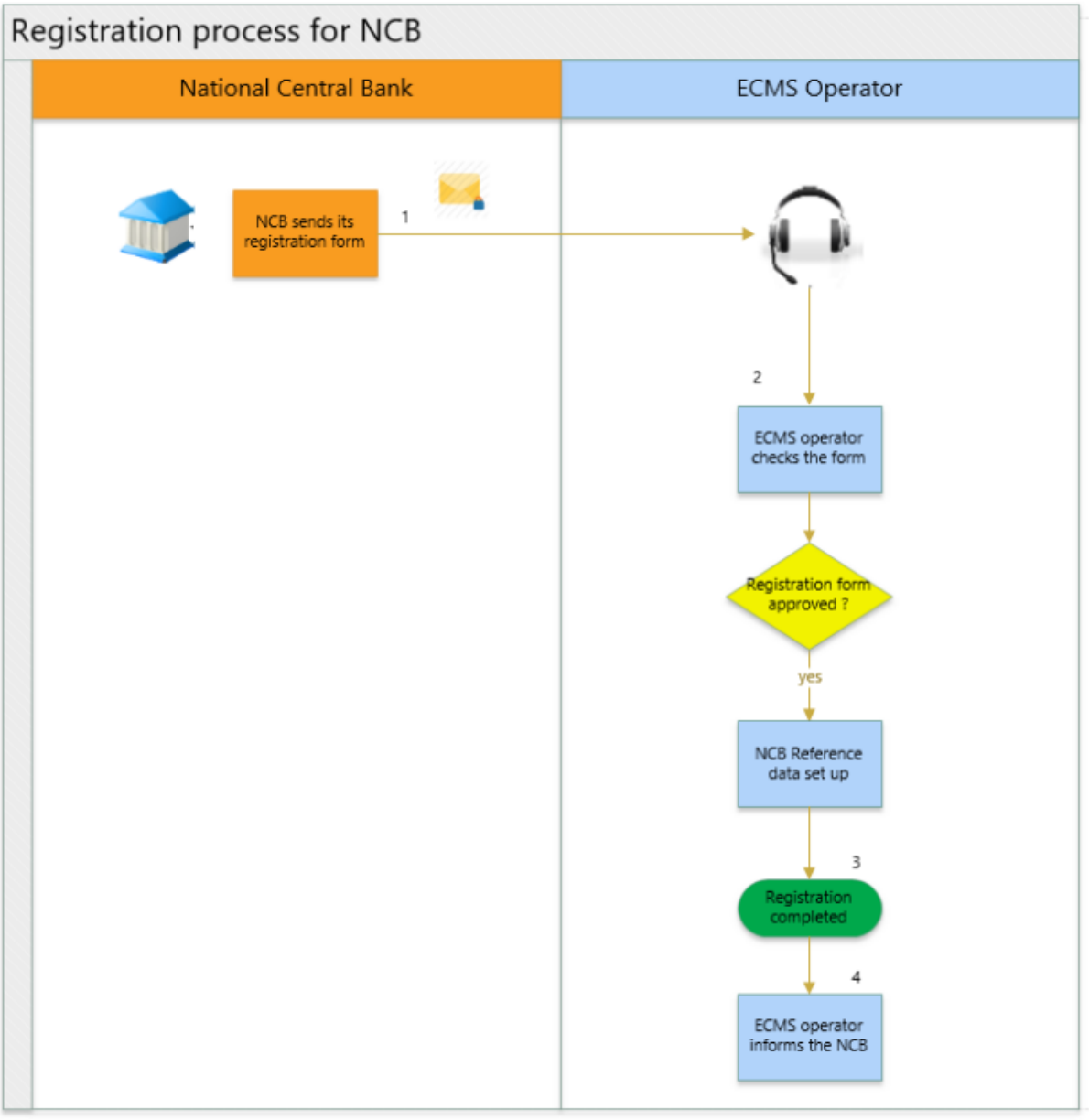
9.1 ECMS service

This section describes additional information particularly relevant for the ECMS.

9.1.1 Registration process and reference data setup

To complement the section 3.3 related to the CGU subscription, the following section describes the workflow for the set-up of ECMS reference data.

- **Registration process and reference data setup for National Central Banks**

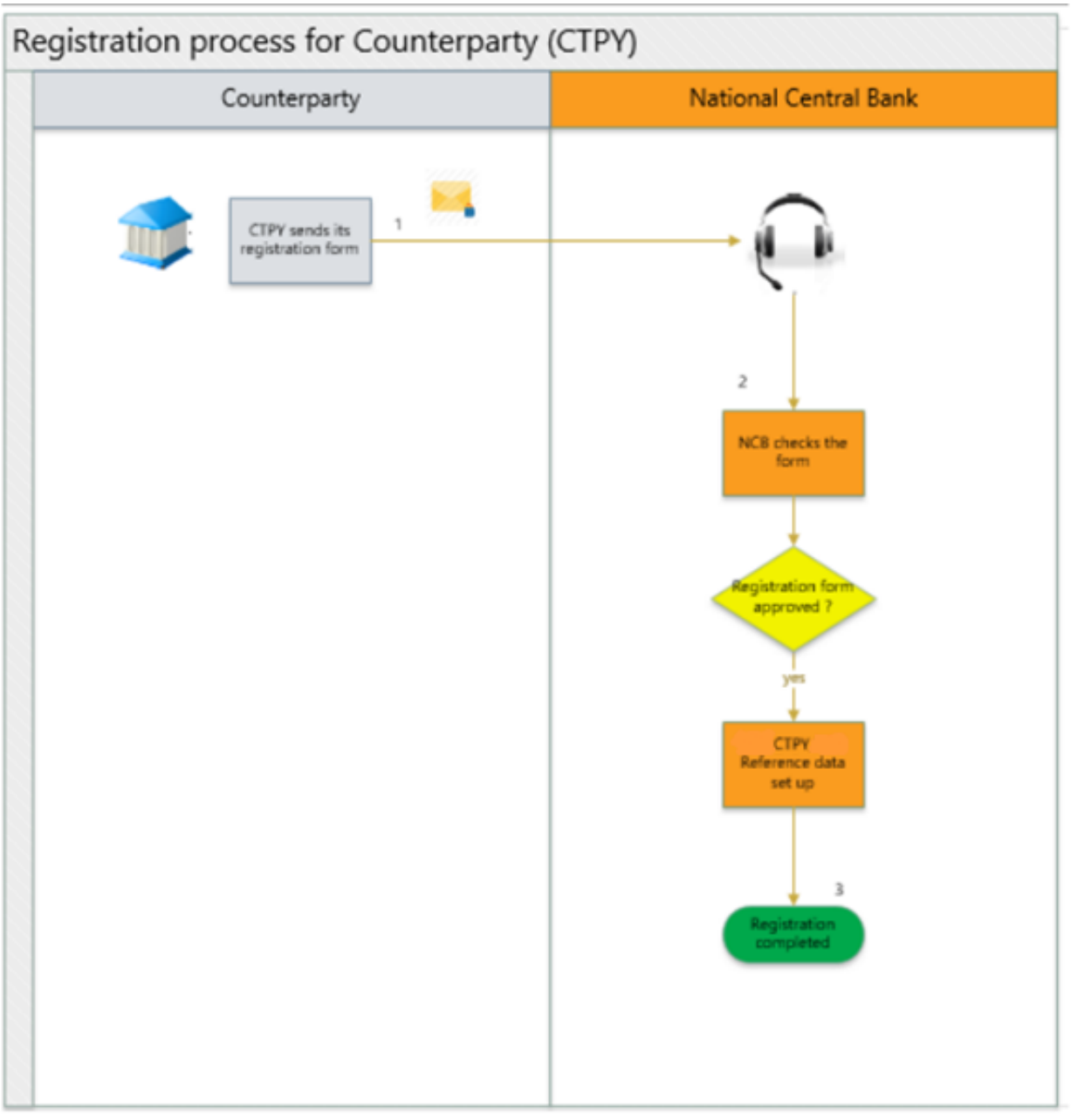


The ECMS Operator is responsible for setting up the reference data for NCBs:

1. The NCBs send the service request including the registration forms to the ECMS Operator.
2. The ECMS Operator checks the completeness and correctness of the forms.
    a. If a form is correct, the ECMS Operator proceeds with reference data set-up in the ECMS.
    b. If a form is not correct, the ECMS Operator asks the NCB to review and resubmit the form.
3. Registration completed.
4. The ECMS Operator informs the NCB

- **Registration process and reference data setup for counterparties**

The below figure describes the registration process and party reference data for counterparties.



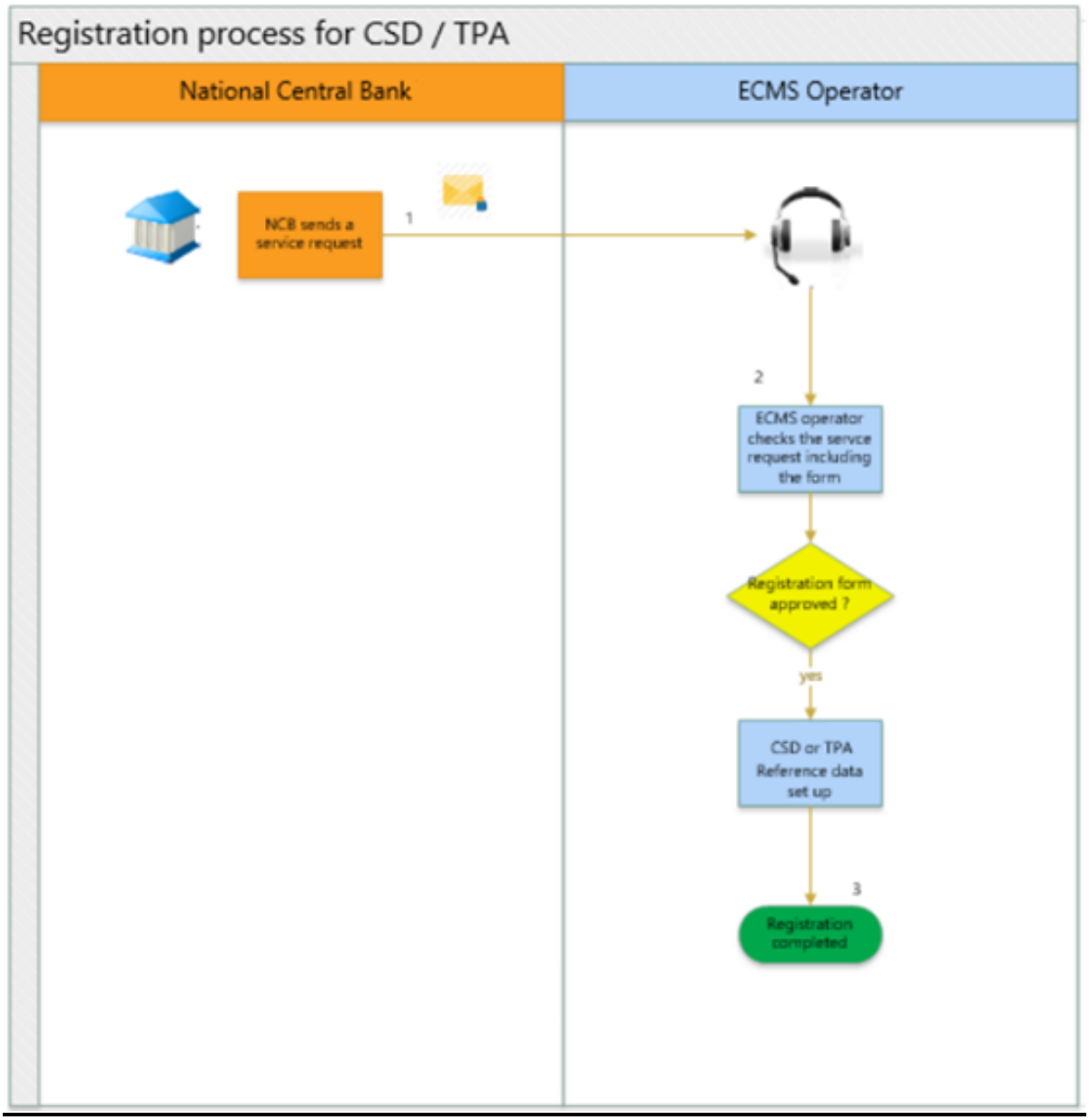
1. The counterparty sends the registration form to their NCB.
2. The NCB checks the completeness and correctness of the form as described in its internal procedure.
    a. If the form is approved, the NCB proceeds with the capturing of the reference data in the ECMS.

b. If the form is not approved, the NCB asks the counterparty to review and resubmit the form.

3. Registration completed.
4. NCB informs the counterparty

- **<u>Registration process and party reference data setup for CSD / TPA</u>**

The below figure describes the registration process and party reference data for CSDs and TPAs.



1. The domestic NCB or the responsible CB sends the Service Request (including the registration form) to the ECMS Operator.
2. The ECMS Operator checks the completeness and correctness of the form.
    a. If the form is approved, the ECMS Operator proceeds with the capturing of the reference data in the ECMS.
    b. If the form is not approved, the ECMS Operator asks the domestic NCB or the responsible CB (that should ask the CSD or TPA or non-euro Foreign CB) to review and resubmit the form.
3. Registration completed.
4. The ECMS Operator informs the domestic NCB.

9.1.2 Connectivity check list – ECMS specifics

This section provides ECMS specifics additional details in relation to the section 6 and in particular, to the steps 6 to 9 of the table of the connectivity checklist.

The steps for the connectivity testing should follow the below sequence:

Activity	Actor
1. Creation of NCB/CSD/TPA party	ECMS Operator
2a. Creation of NCB user(s) with the role 'NCB Admin' 2b. Creation of CSD/TPA A2A user with the corresponding role	ECMS Operator
As from 2b. CSD/TPA A2A connectivity testing can be done	CSD/TPA A2A user
3. Connection to the ECMS GUI landing page (and the user can access menu corresponding to his role)	NCB Admin
4a. Creation of NCB A2A user with the corresponding role 4b. Creation of NCB User(s) with the role 'NCB – U2A General Reference Data Execution' (as from that moment the NCB user can access the menu corresponding to his role)	NCB Admin
As from 4a. NCB A2A connectivity testing can be done	NCB A2A user
5. Creation of the CPTY party	NCB User in U2A (cf. step 4b)
6. Creation of the CPTY user(s) with the role 'CTPY Admin'	NCB Admin
7. Connection to the ECMS GUI landing page (and the user can access menu corresponding to his role)	CTPY Admin
8. Creation of CTPY A2A user with the corresponding role	CTPY Admin
As from 8. CTPY A2A connectivity testing can be done	CTPY A2A user

No other creation or modification of data apart for those described above should be done in ECMS during the Connectivity Testing period.

9.1.3 DN configuration in ECMS

9.1.3.1 Introduction

This chapter describes the format required by ECMS for the three reference data (A2A Certificate DN, U2A Certificate DN and Party Technical Address) that follow the Distinguished Name standard[4]. The ECMS allows many-to-many relationship between users and DNs.

The format integrates the constraints stemming from both the NSPs and CRDM. The latter is involved because the DNs captured in the ECMS reference data module are propagated to CRDM for authorisation and authentication purpose. When ESMIG checks a user access via U2A, it performs its authentication against the DN stored in CRDM (not against the one in ECMS).

9.1.3.2 Required format

Please refer to the next section for examples of DN following the DN format rules detailed here below.

A2A Certificate DN configuration

a) Qualifier in uppercase
b) No whitespace (blank) before and after "="
c) Attribute value
   - Not all special characters are accepted (unlike other TARGET Services) – see list in the table below
   - Swift: lowercase and without whitespaces (blank)
   - SIAnet: case sensitive
d) Comma "," separator between two RDN attributes (RDN - Relative Distinguished Name)
e) No whitespace (blank) before and after the comma "," separator between two RDNs

U2A Certificate DN configuration

a) Qualifier in uppercase
b) No whitespace (blank) before and after the "="
c) Attribute value:
   - Not all special characters are accepted (unlike other TARGET Services) – see list in the table below

[4] These reference data are provided by the ECMS actors via the Registration Forms.

- Swift: lowercase and without whitespaces (blank)
- SIAnet: case sensitive

d) Comma "," as separator between two attributes (RDN - Relative Distinguished Name)

e) A whitespace (blank) must be present after the comma and before the following attribute type

Party Technical Address DN configuration

a) Qualifier in lowercase

b) No whitespace (blank) before and after "="

c) Attribute value

- Not all special characters are accepted (unlike other TARGET Services) – see list in the table below
- Swift: lowercase and without whitespaces (blank)
- SIAnet: lowercase

d) Comma "," separator between two attributes (RDN - Relative Distinguished Name)

e) No whitespace (blank) before and after the comma "," separator between two RDNs

List of not accepted/not recommended characters

Description	List of characters[5]
The following characters are not permitted at all from the ECMS reference data perspective for a DN.	O \ O "
The following characters permitted from the ECMS reference data perspective for a DN. However, they cannot be transmitted correctly to CRDM.	O á O ä O ´ O ¨ O Ç O Â O ª O º O ¬ O ¡ O ¿ O Ñ

[5] "O" are separators

9.1.3.3 Examples

Note: the tables below show the difference between SWIFT and SIA interfaces notations versus the ECMS one.

9.1.3.3.1 Examples for access to ECMS via SWIFT

For SWIFT, only the notation for DN for (PTA) matches the one in ECMS.

	Notation in Swift interface software (SAG/SNL/SAA/ Alliance Cloud)	**Notation in ECMS**
DN for (A2A)	Example 1: cn=p23,ou=a2a,ou=t2,ou=prod,o=ecbfdeff,o=swift Example 2: cn=t2prod,o=ecbfdeff,o=swift	Example 1: CN=p23,OU=a2a,OU=t2,OU=prod,O=ecbfdeff,O=swift Example 2: CN=t2prod,O=ecbfdeff,O=swift
DN for (U2A)	cn=john-smith,ou=t2prd,o=ecbfdeff,o=swift	CN=john-smith, OU=t2prd, O=ecbfdeff, O=swift
DN for (PTA)	cn=xts3,ou=t2,o=ecbfdeff,o=swift	cn=xts3,ou=t2,o=ecbfdeff,o=swift

9.1.3.3.2 Examples for access to ECMS via SIAnet (Nexi-Colt)

For SIA, all the DN notations match the one in ECMS.

	Notation in SIAnet	**Notation in ECMS**
DN for (A2A)	CN=bls,OU=A2A,O=12431,DC=sianet,DC=sia,DC=eu	CN=bls,OU=A2A,O=12431,DC=sianet,DC=sia,DC=eu

DN for (U2A)	CN=John Smith, OU=U2A, O=12431, DC=sianet, DC=sia, DC=eu	CN=John Smith, OU=U2A, O=12431, DC=sianet, DC=sia, DC=eu
DN for (PTA)	cn=application,ou=prod,o=12431,dc=sianet,dc=sia,dc=eu	cn=application,ou=prod,o=12431,dc=sianet,dc=sia,dc=eu

9.1.3.4 Root cause of the different notations

The digital certificate itself does not contain the qualifier[6] nor the complete SubjectDN[7] as a string.

Within the digital certificate, the SubjectDN is not represented as a string but as a list of pairs of attribute qualifier/attribute value instead, and the qualifiers must follow a common international standard (for example, they must all be uppercase):

CN=john-smith

OU=t2

O=bank0001

O=certificateprovider

Therefore, the SubjectDN as a string is built up by the software implementation used to access the digital certificate, and it's this SubjectDN that will be used for comparison with the SubjectDN in the reference data (for example with the SubjectDN stored in CRDM). Each software provider may implement a slightly different way of building such string, while the DN inside the certificate remains the same.

Assuming that the sample above is related to a U2A Certificate DN, it will be displayed as follows by the Swift interface:

cn=john-smith,ou=t2,o=bank0001,o=certificateprovider

But will be interpreted as follows by ESMIG:

CN=john-smith, OU=t2, O=bank0001, O=certificateprovider

[6] Qualifier stands for "attribute qualifier"

[7] SubjectDN of a U2A or A2A certificate refers to the U2A or A2A Certificate DN

9.1.3.5 Impact of a wrong DN

For both U2A and A2A certificates, the impact of a wrong DN lies mainly in the ESMIG (for U2A certificates) and ECMS (for A2A certificates) components due to checks performed by these modules on the SubjectDN of the certificate (the check by ESMIG is done on the U2A DN propagated in CRDM from ECMS). So, both incorrect U2A and A2A certificates will be positively transferred over the network of the NSP regardless of the configuration in CRDM or ECMS until the detection of the misconfiguration by either ESMIG or ECMS.

For PTA DN, which is written directly as a string in the message (not like in the A2A or U2A digital certificate), using a wrong DN will cause a failure at the network level due to missing configuration, since the mentioned PTA is not configured in the network.

9.1.4 Proof of effective A2A connectivity to ECMS

9.1.4.1 Principle

After sending a message (e.g., admi.005, sese,023, etc.) to ECMS, any message received back by the sender on top of the ACK message from the NSP proves that ESMIG and possibly ECMS have been reached. Details are provided later in this section.

Admi.007 messages are sent back by ESMIG or by the ECMS in case of rejection (for technical or business reason) or in case of error in a report request.

In case the inbound message is processed, ECMS sends functional answers when relevant (details can be found in ECMS UDFS).

In the context of the connectivity testing, no inbound message shall be processed, and an admi.007 is to be expected by any user.

The Reason Code reported by the admi.007 allows to differentiate the admi.007 messages sent by ESMIG from those sent by ECMS. If the reason code relates to a check done by ESMIG, it means that ECMS has **not** been reached. Any other reason code means that ECMS has been reached.

9.1.4.2 Reason Codes related to checks done by ESMIG

The table below[8] provides the list of Reason Codes that could be reported in an admi.007 sent by ESMIG.

If the user is reported any of those codes, it means that **ECMS is not reached.**

If the user received an admi.007 listing a Reason Code different from those codes or received another message type, this means that **ECMS is reached.**

BR NAME	DESCRIPTION	INBOUND MESSAGE	REPLY MESSAGE	REASON CODE	ERROR TEXT
ICSA010	The digital signature has to be valid.	head.001	admi.007	I071	Digital signature is not valid.
ICSA010	The digital signature has to be valid.	head.002	admi.007	I071	Digital signature is not valid.
ICAA001	The invoked TARGET service responds to the query request within the timeout limit. Message based or file based store and forward network service will be used.	any query message	admi.007	I074	TARGET service cannot respond to the query request within the timeout limit. Store and forward network service will be used.
ICAA002	The invoked TARGET service responds to the query request via file store and forward network service as the query response exceeds the real time message based network service size (oversize handling).	any query message	admi.007	I076	TARGET service cannot respond via message based network service due to size restriction. File store and forward network service will be used.
ICAA003	The invoked TARGET service responds to the query request as the query response exceeds the file store and forward network service size limit.	any query message	admi.007	I077	The invoked TARGET service cannot respond to the query due to size restriction.

[8] The table is extracted from section 2.2 of the ESMIG UDFS 3.0. The most recent version of the ESMIG UDFS should be used.

10. Acronyms

Acronym	Full Text
A2A	Application to Application
BAH	Business Application Header
BFH	Business File Header
(N)CB	(National) Central Bank
CGU	Closed Group of Users
CRL	Certificate Revocation List
CSL	Certificate Suspension List
DEP	Data Exchange Protocol
DICOAs	Directly Connected Actors
ECMS	Eurosystem Collateral Management System
ESMIG	Eurosystem Market Infrastructure Gateway
HTTPs	Hyper Text Transfer Protocol secure
MEPT	Message Exchange Processing for TIPS
NSP	Network Service Provider
PKI	Public Key Infrastructure
TPA	Triparty Agent
U2A	User to Application
WMQ	WebSphere Message Queue
XML	Extensible Markup Language

11. Appendix

11.1 List of criteria for CGU subscription

Regarding the TEST environment (TIE, 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 TIE, 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 must perform the three steps described above for the TEST environment (TIE, 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 user's 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. For the ECMS community testing, the test cases are up to each NCB;

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, if applicable, described in the Manual of Operational Procedures (MOP) of the relevant TARGET Service, for (National) Central Banks and CSDs/TPAs, 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.