Eurosystem Collateral Management System

Connectivity Guide

Author 4CB

Version ECMS Connectivity Guide 1.0

Date 12/10/2020

History of releases

RELEASE	DATE	ISSUES	STATUS
V1.0	October 2020	Approved by MIB	

Reference documents

REFERENCE	OBJECT
AR.1.1 Technical Requirements and Compliance Check	ESMIG connectivity Technical Requirements and compliance check

1 Introduction

The Eurosystem Collateral Management System (ECMS) is a single collateral management system that is capable of managing the assets used as collateral in Eurosystem credit operations for all European jurisdictions. The ECMS will replace the individual collateral management systems currently in use by Eurosystem National Central Banks (NCBs). Moving to a single system is expected to increase efficiency in the mobilisation and management of collateral and further strengthen the level playing field among Eurosystem counterparties.

The aim of the Connectivity Guide is to provide the ECMS Actors with the relevant guidelines for establishing a technical connection to the ECMS testing and production environments. This document describes the different steps for establishing Value Added Network (VAN) connectivity for ECMS actors, including the technical sender in A2A.

The Connectivity guide is divided into chapters describing:

- The different communication modes that can be used by ECMS users,
- Detailed information on the steps needed to subscribe to the Value Added Network Service Provider's (VA-NSP) Services for ECMS (U2A – User-to-Application and/or A2A – Application-to-Application).

2 Scope of the document

The steps described in this Connectivity Guide for ECMS are applicable for the production environment and the testing environment.

The registration process must be carried out for both environments.

3 Global Connectivity Overview

3.1 Global picture

Reference document	"ESMIG connectivity Technical Requirements and compliance check" - Attachment 1.1 of the Concession Contract"

ECMS actors can choose their VA-NSP.

In compliance with the "ESMIG connectivity Technical Requirements and compliance check" (Attachment 1.1 of the Concession Contract), the VA-NSP shall provide in particular the following services:

- Network connectivity;
- Messaging services in U2A and/or A2A mode;
- Security services: Public Key Infrastructure (PKI) and Closed Group of Users (CGU) management;
- Operational services: Support and incident management.

3.2 Connectivity

The ECMS relies on the Eurosystem Single Market Infrastructure Gateway (ESMIG) for communication between the ECMS and the ECMS Actors. ESMIG is the common entry point for all interactions with the TARGET services (CLM, T2, T2S, TIPS, ECMS and potential future services). Based on common technical specifications, ESMIG is network agnostic, i.e. it does not rely on network specific features. It allows participants to connect via one or multiple service providers for both A2A and U2A interfaces, offering cost-effective and secure access to the various services, including the ECMS. Even though one certificate is used for all the Target Services, neither access to the ECMS in U2A nor the sending of A2A messages is possible without registration to the ECMS CGU.

The ECMS supports the connectivity of ECMS Actors as follows:

- A2A (Application-to-Application): Communication between software applications via XML messages or files using ISO 20022[1] messages or compliant with the ISO 20022 format (use of Business Application Header or Business File Header). A file contains one or several messages.
- U2A (User-to-Application): Online screen-based activities performed by ECMS Actors

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

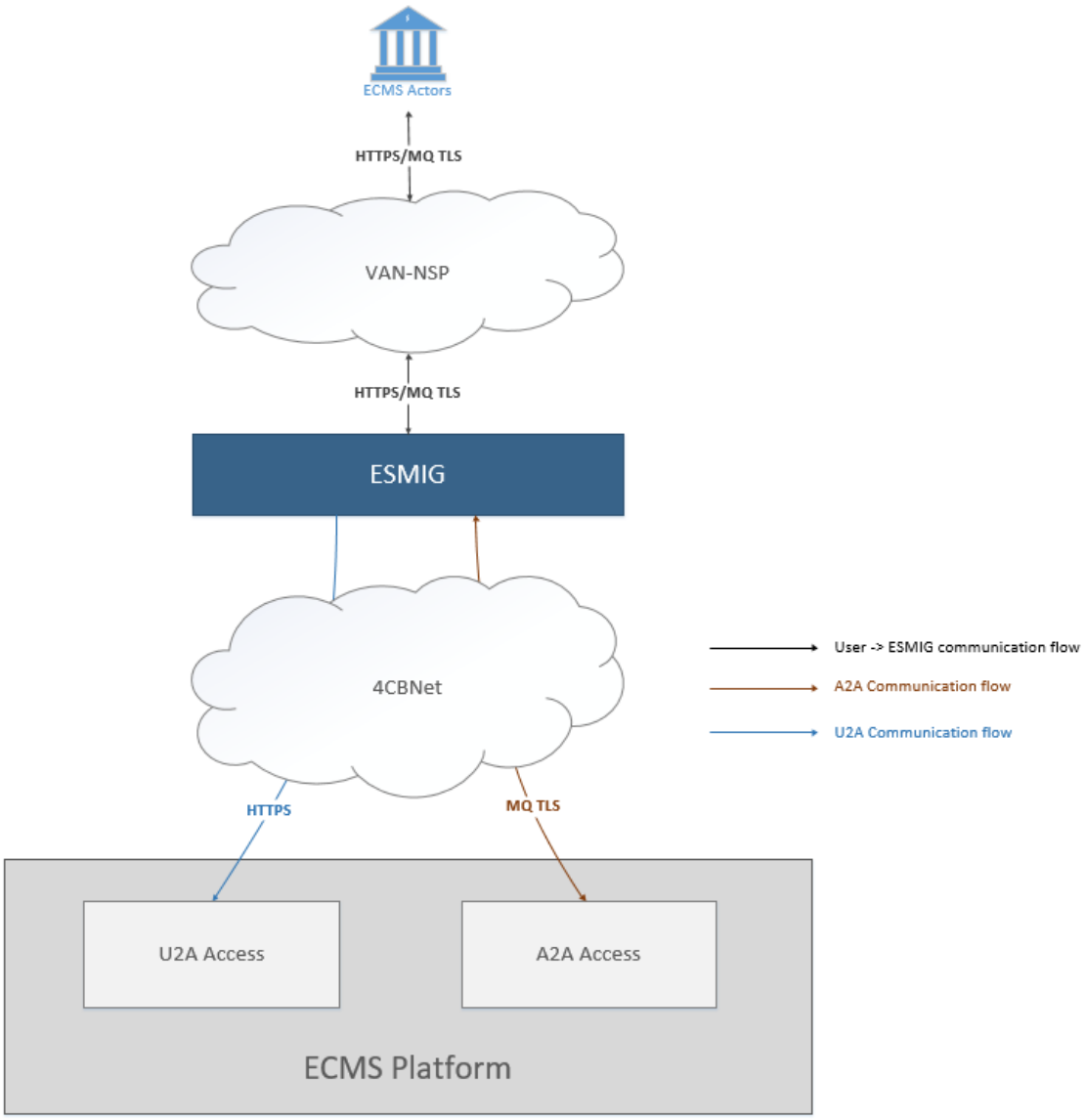

Figure 1 Technical overview of the connection via VA-NSP

1 http://www.iso20022.org/catalogue_of_messages.page

As illustrated above, ECMS Actors interact with the ECMS through ESMIG, which ensures secure access to the application. A2A and U2A interactions use different network protocols to operate. A2A interactions are made by means of the MQ (Message Queue) protocol for transmission of ISO 20022 messages. U2A access uses HTTPS (Hyper Text Transfer Protocol Secure), the standard web protocol. All data are encrypted using the TLS (Transport Layer Security) protocol to ensure confidentiality and integrity of communications.

For both U2A and A2A, ESMIG forwards requests and messages received from ECMS Actors to the ECMS application through 4CBNet.

3.3 The communication modes

Users can communicate with the ECMS in two different modes**: Application-to-Application (A2A)** or **User-to-Application (U2A).**

3.3.1 A2A channel

In A2A mode, the ECMS communicates with the ECMS Actors with one transfer mode: the "store-and-forward". Both messages and files can be exchanged with the "store-and-forward" mode. The file transfer in store-and-forward mode enables a sender to transmit messages or files even when a receiver is unavailable. If the receiver is temporarily unavailable, the VA-NSP stores the files for 14 calendar days and delivers them as soon as the receiver becomes available again.

3.3.2 U2A channel

The U2A interface between the ECMS and the VA-NSP is based on the standard HTTPS protocol; therefore, HTTPS traffic between the users' workstations and ESMIG must be enabled on the network devices on the Actor's side and on the ESMIG entry firewall. In this context, the VA-NSP has to provide connectivity, Closed Group of Users (CGU) and Public Key Infrastructure (PKI) services.

Actor identification and authentication is based on the same digital client certificate used to establish the HTTPS session with the ESMIG gateway. The certificates are provided by the VA-NSP and stored with the related private keys in a smart-card, USB token or remote HSM (Hardware Security Module) assigned to the relevant end-users.

4 VA-NSP documentation

The VA-NSP provides documentation regarding the access to A2A/U2A services which enables ECMS Actors to connect to the ECMS, including details on:

- ECMS relevant URLs (GUI, Trouble Management System…),
- ECMS GUI Operability Requirements – necessary hardware/software configuration to access the ECMS GUI,
- Access to the A2A services – addressing rules for Message/File exchange,
- PKI certificate procurement.

5 Subscription to the VA-NSP Services for ECMS (U2A and/or A2A)

Reference document	• "ESMIG connectivity Technical Requirements and compliance check" - Attachment 1.1 of the Concession Contract" • VA-NSPs own User documentation • VA-NSPs Registration process (VA-NSPs website)

5.1 ECMS users' registration process

ECMS Actors have to apply for a registration process in order to be able to use the ECMS services.

The ECMS user registration process is composed of three parts:

- The CGU subscription,
- The set-up of the ECMS Actors reference data and ECMS account configuration, which is performed either by the ECMS operator for NCB users, or by the NCB administrator for other ECMS users.
- The request for digital certificates by the VA-NSP PKI.

Please note that this process refers to the process of registration for connecting to the ECMS and must therefore be conducted in addition to any procedures and/or contractual requirements the NCB may establish regarding access to the functionalities provided via the

ECMS. All ECMS Actors are included in its data scope (e.g. access to monetary policy operations for counterparties).

For NCBs, the ECMS Operator will:

- Set-up the parties in the ECMS
- Create the NCB administrator(s)
- Input the U2A certificate(s) for the NCB administrator(s)
- Validate the comprehensiveness of the CGU form and the subscription to the CGU
- Inform the NCB of the performed activities

The management of the certificates will be conducted by the NCB administrator:

- for NCB U2A users, input of the nominative certificates in the ECMS (for the go-live, for new Users, and for the renewal of already registered Users)
- For NCBs' A2A applications, input of the A2A certificates in the ECMS and management of the renewal

For TPAs and CSDs, the ECMS operator will (on the basis of a Service Request coming from the domestic NCB):

- Receive the request from the domestic NCB (which is responsible for all communication and checks conducted with other NCBs)
- Input the A2A certificate(s) into the ECMS, in order to link the TPA/CSD IT system to the ECMS
- Validate the comprehensiveness of the CGU form and the subscription to the CGU (after 1st step approval by domestic NCB)
- Inform the domestic NCB of the performed activities
- Set up the parties in the ECMS according to the request sent by the domestic NCB
- Manage the renewal of A2A certificates and the updates in the ECMS

Assumption: Since there will be no U2A connection of TPA and CSDs, there will be no need for management of users certificates.

For Foreign CBs, the ECMS Operator will:

- Set-up the parties in the ECMS

No A2A or U2A connection is expected (no registration process, no management of users' certificates).

5.1.1 CGU subscription

The VA-NSP shall allow the creation and removal of logically segregated groups of ECMS Actors. In particular, the VA-NSP shall create and manage groups of ECMS Actors for both the production and the testing environment, i.e. one group for each environment.

The subscription to a group of users, and any subsequent modification to such a subscription, shall be arranged through an electronic workflow on the Internet. All electronic forms from the VAN provider shall be authorised by the relevant NCB and the ECMS Operator.

The activation date for subscriptions shall be set at the latest within two weeks after the form's approval by the ECMS Operator. Upon request from the ECMS Operator, the VA-NSP shall remove an ECMS Actor from the CGU within one hour.

5.1.1.1 CGU subscription for NCBs

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

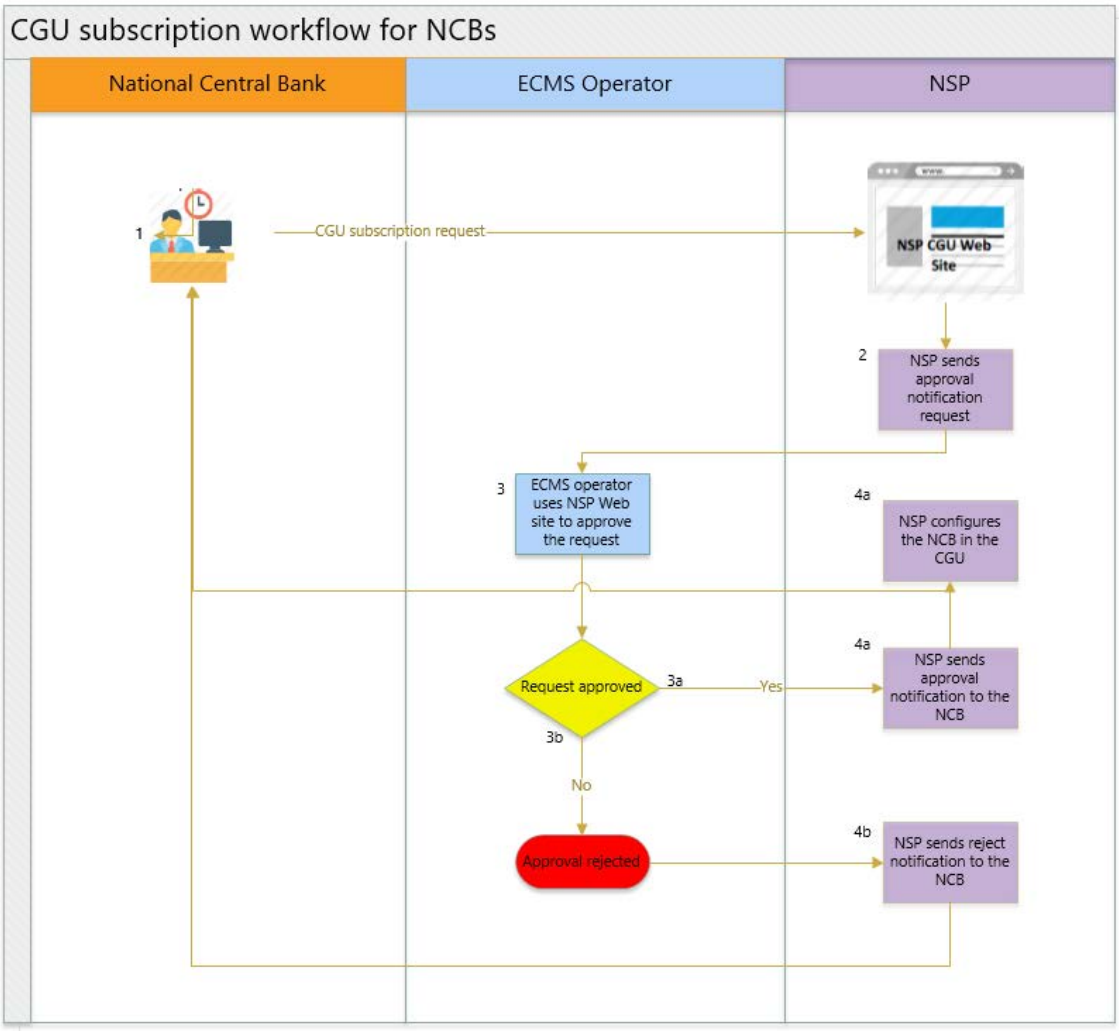

Figure 2 - CGU Subscription workflow for NCBs

1. The NCB submits the subscription request through the VA-NSP website.
2. The VA-NSP verifies the correctness of the request and sends the approval notification request to the ECMS Operator.
3. The ECMS Operator checks[2] the subscription request in the VA-NSP website.
   a. The request is approved
   b. The request is rejected
4. The VA-NSP sends the approval or reject notification

[2] list of criteria to be checked by the ECMS operator for the subscription request is detailed in the Annex

a. The request is approved. The VA-NSP configures the NCB in the CGU.
b. The request is rejected

In case of modification, the NCB 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 whether 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 NCB:
    - The approval is done by the ECMS 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.

5.1.1.2 CGU subscription for Counterparties, CSDs and TPAs

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

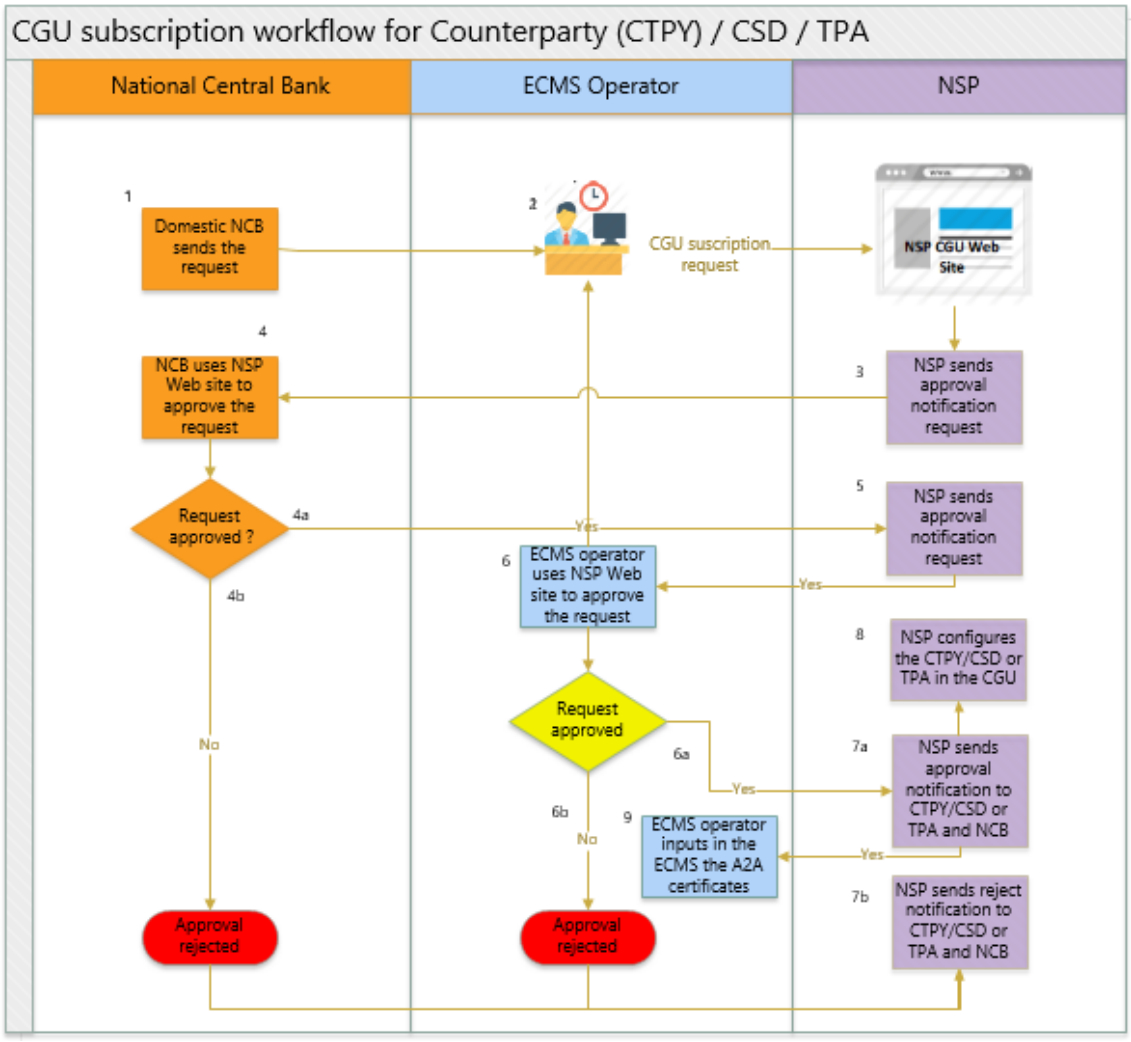

Figure 3 - CGU Subscription workflow for Counterparties, CSDs and TPAs

1. The domestic NCB sends the request to the ECMS Service Desk (the domestic NCB is responsible for all communication and checks conducted with other NCBs)
2. The ECMS operator submits the subscription request through the VA-NSP website.
3. The VA-NSP verifies the correctness of the request and sends the approval notification request to the NCB.
4. The NCB checks the subscription request in the VA-NSP website.
   a. The request is approved.
   b. The request is rejected.

5. In case the subscription request is approved by the NCB, the VA-NSP sends the approval notification request to the ECMS Operator.
6. The ECMS Operator checks[3] the subscription request in the VA-NSP website
   a. The request is approved
   b. The request is rejected
7. The VA-NSP sends the Approval or Reject notification to the counterparty/CSD/TPA and NCB part of its jurisdiction.
   a. The request is approved. The VA-NSP configures the counterparty or CSD or TPA in the CGU.
   b. The request is rejected.
8. The VA-NSP configures the counterparty/CSD/TPA in the CGU.
9. The ECMS operator inputs in the ECMS the A2A certificate(s) to link the TPA/CSD IT system to the ECMS

In case of modification, the ECMS operator (following the domestic NCB request) 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 same approval flow is foreseen:

- Dual approval is requested for orders submitted by the ECMS operator following the request of the domestic NCB:
  - The first approval is done by the domestic NCB;
  - The second approval is done by the ECMS 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.

[3] list of criteria to be checked by the ECMS operator for the subscription request is detailed in the Annex

5.1.2 ECMS reference data set up

National Central Banks registration process

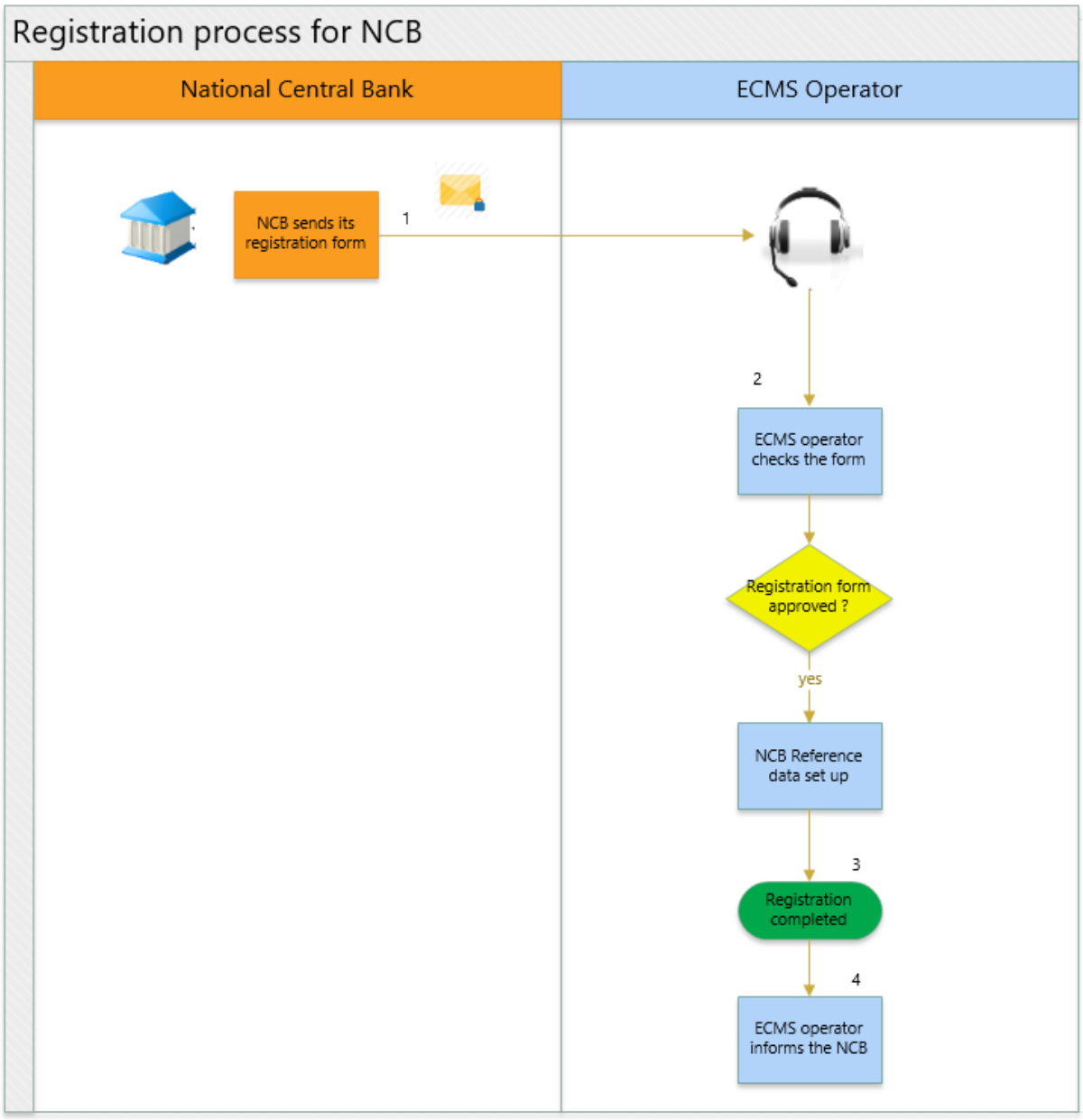

Figure 4 - Registration process for NCB

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

1. The NCBs send 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

Counterparty registration process

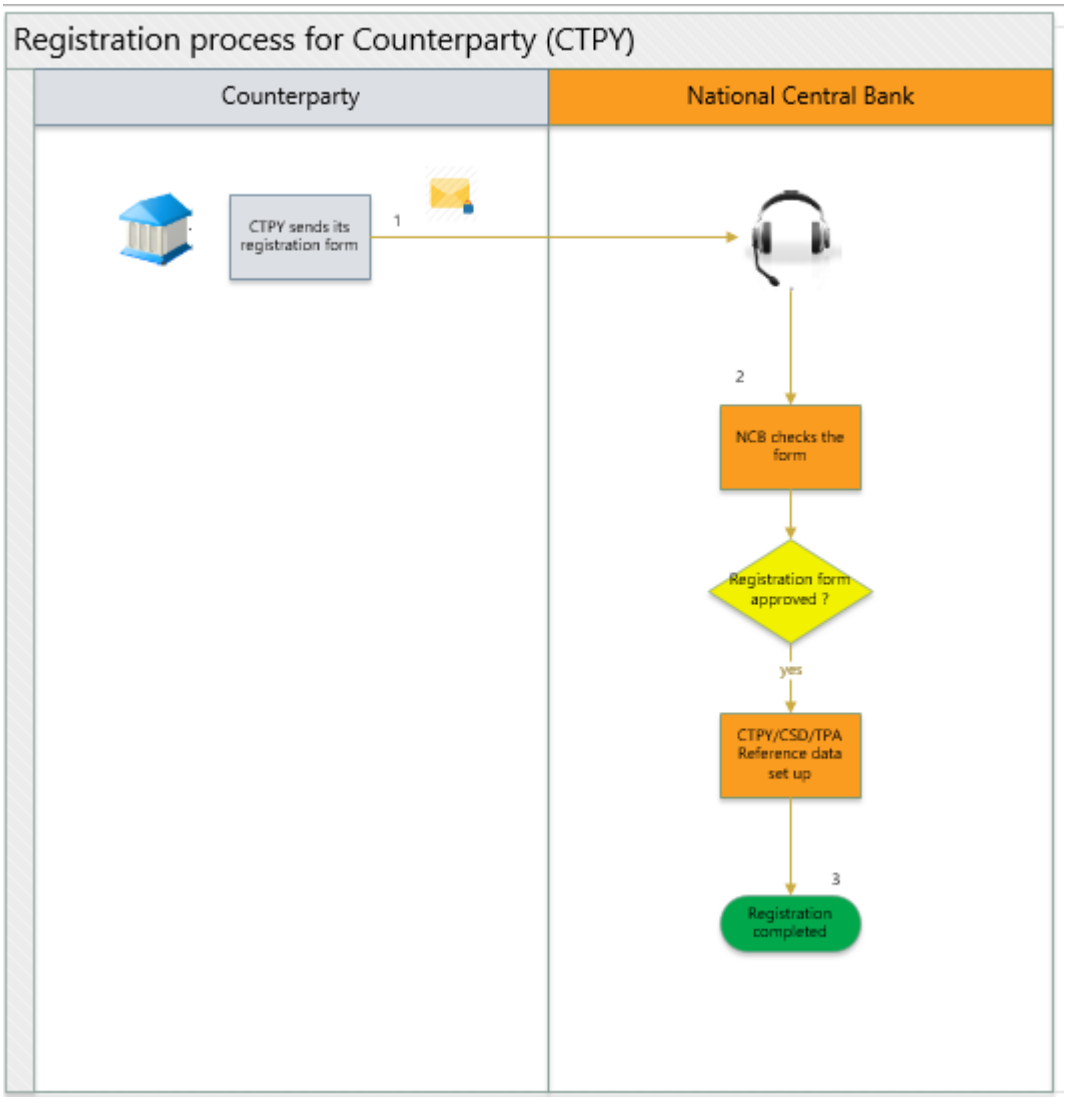

Figure 5 - Registration process for CTPY

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

CSD / TPA and non-euro Foreign CB registration process

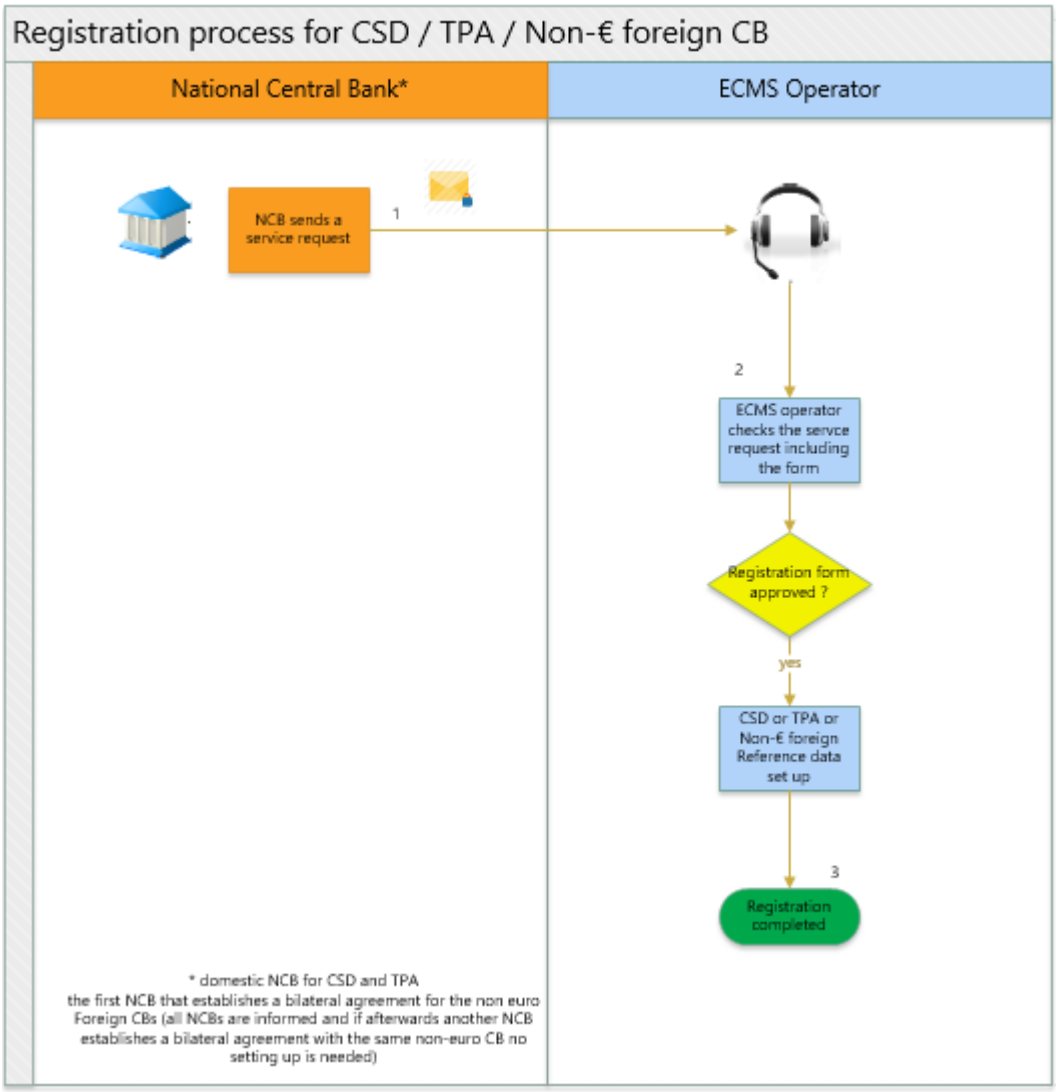

Figure 6 - Registration process for CSD / TPA / non-euro Foreign CB

1. The domestic NCB or the responsible CB sends the service request (including the registration form) to the ECMS service Desk.
2. The ECMS operator checks the completeness and correctness of the form.

c. If the form is approved, the ECMS operator proceeds with the capturing of the reference data in the ECMS.
d. If the form is not approved, the ECMS operator asks 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.

5.1.3 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 or remote HSM;
- for the A2A channel: certificates on HSM for live traffic.

The procedure to procure the certificates is described in the VA-NSPs User documentation. If an ECMS actor has already received a certificate to access another TARGET service (e.g. T2/T2S), the request of another certificate for the ECMS is not needed.
ECMS Actors assign certificates to their users (interacting with the ECMS in U2A mode) and applications (interacting with ECMS in A2A mode). If an ECMS Party uses multiple connectivity providers to connect to the ECMS, then it has to assign one certificate to each of its users and applications for each VA-NSP. This information is used by ESMIG and stored in the Common Reference Data Management (CRDM).

5.2 Setting up security

Reference document	• VA-NSPs own User documentation

The VA-NSPs are responsible for providing a secure connection to and from ESMIG for clients subscribing to their services. The implementation of the security measures is managed by the VA-NSP. Regarding the ECMS actors' interfaces, the VA-NSPs provide the necessary support for the security setup.
For more information on the security aspects, see the VA-NSPs documentation.

5.3 Set-up of parties in the ECMS

The set-up of Parties in the ECMS includes the configuration of reference data for parties.

The ECMS Operator is responsible for setting up and maintaining reference data in the ECMS for NCBs, non-euro area CBs and CSDs/TPAs.

Similarly, NCBs are responsible for setting up and maintaining party reference data for their counterparties including their business roles. The following table summarises, for each reference data object related to the set-up of Parties in the ECMS, the ECMS Party responsible for its configuration and which mode can be used for configuration.

Data Object	Responsible ECMS Party	Mode[4]
NCB	ECMS Operator	U2A
Non-euro area CB	ECMS Operator	U2A
CSD/TPA	ECMS Operator	U2A
NCB's Counterparties, cash correspondent	National Central Bank	U2A
Entity Business Roles	National Central Bank	U2A

Table 1- Setup of Parties in the ECMS[5]

6 Troubleshooting and support

NCBs should address any issues related to the connection between the NCB network and the VA-NSP directly with the VA-NSP, for support or to investigate potential issues related to the NCB / VA-NSP connectivity (e.g. certificate management or software configuration of users' workstations).

In case of a connection issue between VA-NSP and ESMIG,

- 1st level of contact: the National Service Desk with the VA-NSP; this should address the technical issues that are specific to one NCB. Otherwise (if the VA-NSP confirms

[4] U2A covers both U2A data entry by the responsible actor and for the migration purposes, the use of DTT download functionalities described in the DTT requirements.

it is a general connection issue with the ESMIG), the National Service Desk should escalate the issue.

- Escalation level via the ECMS Service Desk: in that case, the ECMS service desk shall take charge of the issue liaising with the ESMIG operational team (OT).
-

Further details on the VA-NSP's commitments are presented in the VA-NSP's documentation.

7 Check list

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

Step	**Action**
1	Selection of the Network Service Provider
2	Subscription to the VA-NSP's Services for ECMS (U2A and/or A2A)
3	Request for the VA-NSP digital certificates
4	Connectivity set-up with VA-NSP
5	Create the Distinguished Name (DN) in ECMS
6	Create the Party in Reference Data in ECMS
7	Link the Party to the Network Service of choice in Reference Data in ECMS
8	Create Party administrators in ECMS
9	Create the users and link it with the Distinguish Name in ECMS
10	Assign groups/roles to them according to their functions in ECMS
11	Connectivity test with ECMS

8 Glossary

Item	Description
Application-to-Application (A2A)	A technical mode of communication that permits the exchange of information between different software applications without a graphical user interface.
Central Securities Depository (CSD)	An entity that: 1) enables securities transactions to be processed and settled by book entry; 2) provides custodial services (e.g. the administration of corporate actions and redemptions); and 3) plays an active role in ensuring the integrity of securities issues. Securities can be held in a physical (but immobilised) form or in a dematerialised form (whereby they exist only as electronic records).
Closed Group of Users (CGU)	Closed Group of Users is a logically segregated group of users. The Network Service Providers allow creation, management and removal of logically segregated groups of ECMS actors. The VA-NSP must have different CGUs for the production environment and for the test environments.
Common Reference Data Management (CRDM)	The Common Reference Data Management (CRDM) handles in a single point the data that is shared by different Eurosystem Common Components.
Counterparty (CPTY)	Institution with which a Eurosystem CB has a business/contractual relationship for purposes of monetary policy operations and intraday credit or other collateral management activities in the scope of the ECMS.
Distinguished Name (DN)	A name that uniquely identifies an entry in a directory or network. Usually it is a sequence of attribute-value assertions (e.g. "cn=smith") separated by commas, e.g. <cn=smith,ou=t2s-ops, o=bnkacctt,o=nsp-1>.
ECMS actors	Any legal entity or organisation interacting with the ECMS for the purpose of collateral management. ECMS Actors are: Counterparties, Central Security Depositories (CSD), Triparty Agents (TPA), NCBs, non-euro Central Banks, Cash Correspondent
ECMS user	Human user or an application that interacts with ECMS. The ECMS user can communicate with ECMS via U2A mode (User To Application) using the ECMS GUI or via A2A mode (Application

Item	Description
	To Application) using messages
Eurosystem Single Market Infrastructure Gateway (ESMIG)	The ESMIG provides the single access point for the external communication to all market infrastructure services (ECMS, T2S, TIPS, etc.). The ESMIG ensures a network agnostic communication with the users, where network agnostic means multiple network providers are allowed.
Graphical User Interface (GUI)	The interface that allows a user to interact with a software application through the use of graphical elements (e.g. windows, menus, buttons and icons) on a computer screen, using the keyboard and mouse.
Hardware Security Module (HSM)	Hardware-based security device that generates, stores, and protects cryptographic keys.
Hyper Text Transfer Protocol Secure (HTTPS)	HTTPS (HyperText Transfer Protocol Secure) is an encrypted version of the HTTP protocol. It uses SSL or TLS to encrypt all communication between a client and a server. This secure connection allows clients to safely exchange sensitive data with a server.
Message Queue (MQ) protocol	MQ is an IBM standard for program-to-program messaging across multiple platforms.
National Central Bank (NCB)	A Central Bank that provides collateral services to Participants.
NCB User	Human user who has interactive access to the ECMS online functions or an application that requests services from the ECMS. They interact with the ECMS, belong to one NCB and act on behalf of this NCB or its community.
Public Key Infrastructure (PKI)	A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
Technical sender	The technical sender is the ECMS Actor submitting an A2A message to the ECMS. Each technical sender is identified by

Item	Description
	means of a certificate issued by the connectivity provider. The network infrastructure of the connectivity provider authenticates the technical sender on the basis of its certificate, both in A2A mode and in U2A mode. The certificate DN of the technical sender represents the technical address used by the technical sender to connect to the ECMS.
Transport Layer Security (TLS)	Formerly known as Secure Sockets Layer (SSL), is a protocol used by applications to communicate securely across a network, preventing tampering with and eavesdropping on email, web browsing, messaging, and other protocols. Both SSL and TLS are client / server protocols that ensure communication privacy by using cryptographic protocols to provide security over a network. When a server and client communicate using TLS, it ensures that no third party can eavesdrop or tamper with any message.
Triparty Agent (TPA)	The triparty service provider (referred to as “triparty agent” or “TPA”) responsible for the processing of instructions on behalf of both collateral giver and the collateral taker.
User-to-Application (U2A)	A mode of technical communication that permits the exchange of information between software applications of the ECMS and the ECMS system user through a Web graphical user interface.
Value Added – Network Service Provider (VA-NSP)	The ECMS Actors can choose their preferred NSP, which fulfils the ECMS Connectivity Requirements and passes the relevant compliance checks. The NSP provides the ECMS Actors the means to access the ECMS, in addition to providing network connectivity, messaging services (U2A and A2A), security services, and operational services.
Extensible Markup Language (XML)	Extensible Markup Language (XML) is used to describe data. The XML standard is a flexible way to create information formats and electronically share structured data via the public Internet, as well as via corporate networks. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

9 Appendix

9.1 Preparatory activities and list of criteria for CGU subscription for ECMS actors

9.1.1 For TEST environments

Regarding the TEST environments, the connectivity set-up includes specific preparatory activities needed to start the connectivity tests:

- Reference data set-up includes the configuration of a minimum set of business data that will allow the connectivity tests to begin. The minimum set of business data comprises reference data, network services and related technical addresses, user and roles.
- ECMS Operator will ensure the coherence of the reference data with the parameters used in the connectivity set-up (e.g. the certificate associated with a technical address).
- The value-added network service provider provides the PKI with a VAN connection.
- Prior to the start of the connectivity set-up, the actors must have finalised their negotiations with NSP(s).

Then the actors verify that they can connect to the ECMS (TEST):

- A2A actors can communicate at technical and application level.
- Actors with their respective VAN provider can test the value-added services (out of ECMS scope).
- U2A users reach the welcome page of ESMIG and perform the login to the ECMS.

9.1.2 For PROD environment

The following steps must be completed prior to joining the ECMS PROD CGU:

- Connectivity set-up for PROD
- Successful completion of testing executed on the user test environments including functional, community/business day, operational and migration testing.

In addition to the above, the following prerequisites must be fulfilled:

Nomination of at least one administrator and formalisation of organisational procedures related to the CGU registration process (person in charge of sending the registration to the NSP and that would be the contact point for the NSP and the ECMS operator). As for the setup of reference data, it is also important that the NCB ensures the nomination at least of one administrator for the NCB reference data set up. As for counterparty, in case the NCB is taking this responsibility, at least one NCB party administrator should be indicated in the registration form of the counterparty. The registration form should contain at least the following information:

- ✓ Customer Information:
  - ✓ Legal name
  - ✓ BIC
  - ✓ RIAD code
  - ✓ User Name of the person submitting the form
- ✓ Counterparty or CSD or TPA / NCB Approver BIC
- ✓ Counterparty or CSD or TPA / NCB administrator name

Please note the VA-NSP may request that the form includes additional information such as technical Identifiers for U2A/A2A (e.g. network addresses, IP, DN pattern).