EUROPEAN CENTRAL BANK

EUROSYSTEM

target services | T2S

ECB-PUBLIC
19 October 2021

T2S COMMUNITY READINESS TO ESMIG

INFORMATION TO "DIRECTLY CONNECTED ACTORS IN T2S"

1. Preamble

The Eurosystem Single Market Infrastructure Gateway (ESMIG) was developed in the context of the Market Infrastructure Services' Consolidation project. It will provide a single access point for external inbound and outbound communication to all TARGET Services, the market infrastructure common components and applications. Additional information on the reasons why ESMIG was developed and on its impact on T2S can be found in the related change request CR-701-SYS: https://www.ecb.europa.eu/paym/target/t2s/governance/pdf/crg/ecb.targetseccrg190228_T2S-0701-SYS.en.pdf?ad56759016493581 51d865152d38fa2c

In order to successfully connect to ESMIG for T2S, the migrating actors will have to execute a series of activities detailed in both the TARGET Services Connectivity Guide and the respective Network Services Providers (NSPs) documentation.

The testing of the connectivity to ESMIG for T2S in UTEST will be open from 1 December 2021 until 8 April 2022. The production environment for the connectivity to ESMIG for T2S in PROD environment will be open as from 1 March 2022. The latest date to connect has been set to 5 May 2022.

Given the importance of a successful connectivity to ESMIG, a specific monitoring of the readiness and the connectivity test execution is introduced with all directly connected actors.

2. Connectivity guide

The TARGET Services Connectivity Guide (Common Connectivity Guide "CCG") describes in general terms the connectivity to the ESMIG. The ESMIG provides a single access point for directly connected actors to access TARGET Services.

The current TARGET Services Connectivity Guide is applicable for T2S, T2 and TIPS and is valid for both production and test environments.

The TARGET Services Connectivity Guide provides information on communication modes (A2A/U2A), Messages (CCG Ch. 2 – Global Overview), User Registration process (CCG Ch. 3 – User Registration Process and exchange of certificates (CCG Ch. 4 – Request for Digital Certificates by the NSP PKI). A dedicated section provides information on how troubleshooting must be addressed and how generic support is organized (CCG Ch. 7 - Troubleshooting and support).

The actions to be performed are also summarised in a checklist (CCG Ch. 6 – Connectivity Checklist).

The TARGET Services Connectivity Guide (CCG) is available on the Eurosystem website at the following address: https://www.ecb.europa.eu/paym/target/consolidation/profuse/shared/pdf/2021-08-10_target_services_connectivity_guide_v1-0.pdf

3. ESMIG U2A Qualified Configurations

The ESMIG U2A Qualified Configurations describes the general configuration that ESMIG users shall be complaint with in order to access TIPS, ECMS, RTGS, CLM and CRDM GUI via the ESMIG web portal. A specific section is devoted to describe the technical framework needed to fully implement the non-repudiation of origin functionality (NRO). The NRO solution, based on the Ascertia Go>Sign Desktop application, will be the unique U2A NRO solution to be adopted for TARGET services, therefore only one version of the Go>Sign Desktop client will be used and distributed across the different services. There will be two available ESMIG browsers from T2S Release 6.0, Google Chrome 88.0+ and Firefox 78.0+.

The ESCMIG U2A Qualified Configurations is available on the Eurosystem website at the following address:
https://www.ecb.europa.eu/paym/target/tips/profuse/shared/pdf/ESMIG_U2A_Qualified_Configurations_v1_3_1.pdf

4. Network Service Providers (NSPs)

Two network service providers (NSPs), SIA-COLT and SWIFT, have been selected, based on the result of the public awarding procedure, to provide connectivity services for ESMIG:

- SIA-Colt Technology Services;
- SWIFT.

All NSPs specific steps and technical details (e.g. e-ordering, User Registration, Certificates, etc) to achieve the connectivity to TARGET Services, are described in the relevant NSP (SWIFT or SIA-COLT) related documentation.

5. Monitoring

The Central Securities Depositories (CSDs) and National Central Banks (NCBs) are responsible for the readiness monitoring of their communities. In that context, they will contact your institutions prior the start of the testing phase (readiness monitoring) and during the testing phases (testing execution monitoring).

The readiness monitoring aims at evaluating the respective preparedness to connect to the environments. The monitoring during the testing execution aims at validating the actual capability to connect to the environments.

The objective of this monitoring is to ensure that any potential delay or issue is identified as soon as possible to allow effective mitigating action and successful migration by all actors.

In specific cases where a DCP has contractual relationships with both the CSD and the NCB, the DCP shall report on its readiness status to both the CSD and the NCB. In case of technical issues, the DCPs can contact directly the T2S Service Desk (CCG Ch. 7 - Troubleshooting and support).