EUROPEAN CENTRAL BANK

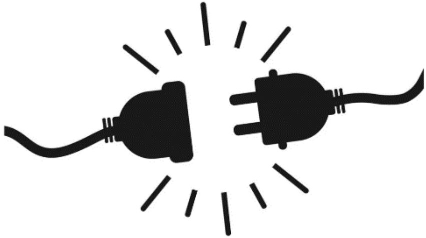
EUROSYSTEM

Ready to connect?

30/09/2021

Jean Clement
Adviser, ECB

Agenda



A Introduction

B Steps required to connect to TARGET Services

C Proofs of successful connectivity to TARGET Services

D Troubleshooting and support

Introduction

- With the start of **User Testing connectivity testing**, this presentation aims at providing market participants further information with regards to the **connectivity** to the **Eurosystem Single Market Infrastructure Gateway (ESMIG)**
- The ESMIG is a **single access point** to all TARGET Services (T2, T2S, TIPS and ECMS) for **Directly Connected Actors (DiCoAs)** (also called **TARGET Services Actors**. This access is provided by the Eurosystem **Network Service Providers (NSPs)** SIA-COLT and SWIFT
- The ESMIG supports both **U2A (User-to-Application)** and **A2A (Application-to-Application)** communication channels.

Steps required to connect to TARGET Services (1/2)

1 User Registration process

[Section 3: TARGET Services Connectivity Guide v1.0]

In order to register its users, a TARGET Service Actor is required to take the following actions:

1.1 Network Service Provider selection

- Select and sign a contract with a NSP, nominate their system administrators and register on the NSP website

1.2 Party setup

- Have its party set up by its relevant Central Bank (In case of T2, as Payment Bank or Ancillary System)*

1.3 Closed Group of User (CGU) subscription

- Request a subscription to a CGU (maintained by its NSP) through an electronic form authorised by the CB and the TARGET Service Operator

* And all users related configurations in CRDM e.g. create users, assign privileges, link Certificate DN to users

Steps required to connect to TARGET Services (2/2)

2 Request for Digital Certificates

[Section 4: TARGET Services Connectivity Guide v1.0]

The TARGET Service Actor needs to request a Digital Certificate(s) from its NSP(s).

The NSP Public Key Infrastructure (PKI) provides 2 types of digital certificates:

- For the U2A channel: certificates on a smart-card or USB token or remote Hardware Security Module (HSM);
- For the A2A channel: certificates on HSM for test and prod traffic

The same certificate can be used for all the TARGET Services. → if already requested for another TARGET Service using ESMIG, a new digital certificate is not needed.

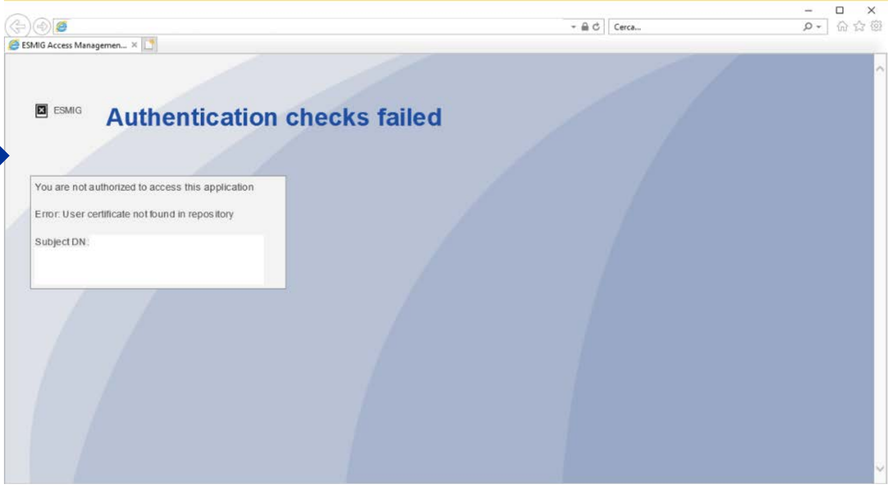
Proofs of successful connectivity to TARGET Services (1/3)

U2A Connectivity

Users can make sure of a successful U2A connectivity to T2 with one of the following outcomes (depending on their configuration at the time of the test):

1. Users not configured in UTEST

Users that were never configured in UTEST will get the error "You are not authorized to access this application" (see screenshot)



Authentication checks failed

You are not authorized to access this application

Error: User certificate not found in repository

Subject DN:

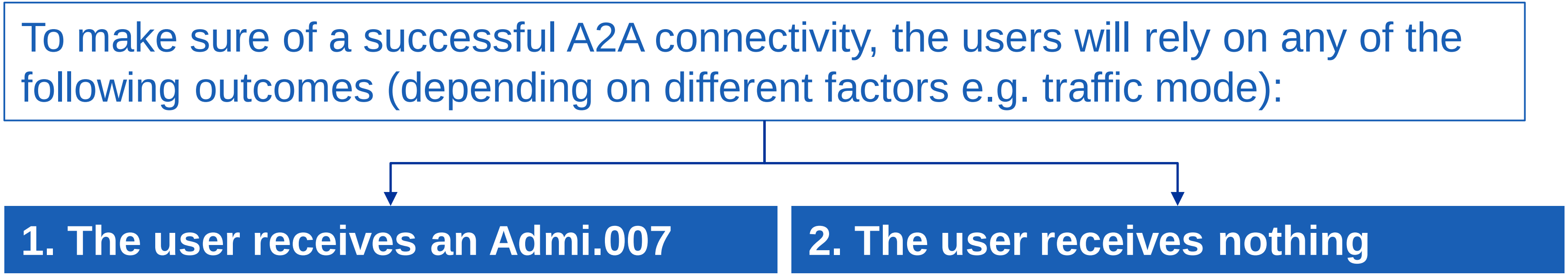
2. Users configured in UTEST

Users that were already configured in UTEST will see the ESMIG landing page. Depending on privileges already assigned to the user (e.g. CRDM_Access or TIPS_Access privilege), they will also be able to see the page where there is an option to select the applications.

Proofs of successful connectivity to TARGET Services (2/3)

A2A Connectivity

Considering that the backend modules will be deployed in UTEST by 26 Nov 2021. Until then, a subset of messages can be exchanged with T2 over ESMIG.



To make sure of a successful A2A connectivity, the users will rely on any of the following outcomes (depending on different factors e.g. traffic mode):

1. The user receives an Admi.007

2. The user receives nothing

Proofs of successful connectivity to TARGET Services (3/3)

A2A Connectivity

1. The user receives an Admi.007

The Admi.007 will be sent out in the following case:

- 40 seconds after a Real Time message is sent to T2 (to inform the user about the triggering of the timeout management process)

2. The user receives nothing

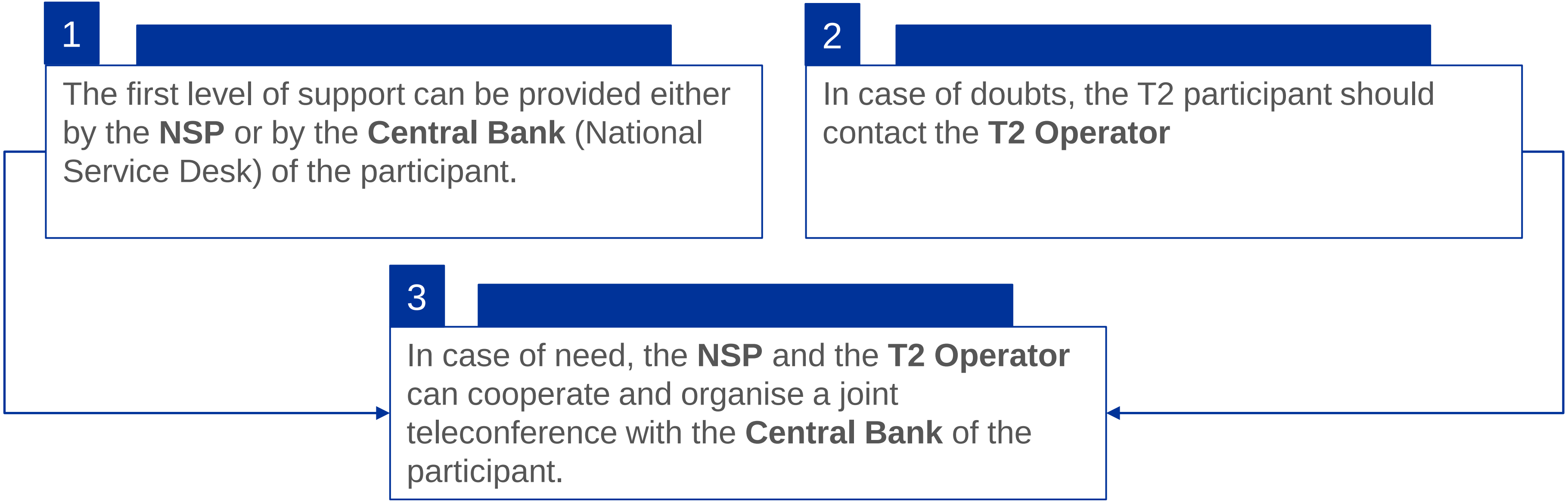
In case of a Store and Forward message successfully received by the platform.

For users that have opted for it, the NSP will send a Delivery Notification to inform the TARGET Service Actor that a message or file has been received by the platform. [Section 3: TARGET Services Connectivity Guide v1.0]

The TARGET Service Desk can be contacted to get the evidences of messages/files received by the platform.

Troubleshooting and support

For technical problems with regards to the NSP connectivity, depending on the nature of the issue, the TARGET Services Actors can count on the following support: [Section 7: TARGET Services Connectivity Guide v1.0]



1

The first level of support can be provided either by the **NSP** or by the **Central Bank** (National Service Desk) of the participant.

2

In case of doubts, the T2 participant should contact the **T2 Operator**

3

In case of need, the **NSP** and the **T2 Operator** can cooperate and organise a joint teleconference with the **Central Bank** of the participant.

Annex 1: Useful links

For further details on the connectivity to TARGET Services (especially in the case of T2), please refer to the following documents:

- Relevant NSP documentation
- TARGET Services Connectivity Guide v1.0 (europa.eu)
- ESMIG U2A Qualified Configurations v1_3 (europa.eu)
- Terms of reference for user testing (europa.eu)
- T2 User Detailed Functional Specifications v2.2 - Eurosystem Single Market Infrastructure Gateway (ESMIG) (europa.eu)

Thank you for the attention!

www.ecb.europa.eu/paym

@TARGET_ECB

ECB: market infrastructure and payments