EUROPEAN CENTRAL BANK

EUROSYSTEM

**ECB**
DG-MIP
T2/T2S Consolidation Project Team

# T2/T2S Consolidation

## User access rights

Task Force on Future RTGS Services

4th TF meeting, 27 March 2017

# Overview

## Background and objective

During the last TF, a request was expressed to have an overview of the user access rights concept in the T2/T2S consolidation

- T2S includes a flexible and complex concept for access rights, which is not intended to be discussed
- For the future RTGS services, it was already agreed in the TF to stick to pre-defined roles, i.e. to have a restricted use of a potentially consolidated model
- The changes brought by the migration to ISO20022 (the move from Y-copy to V-shape) and ESMIG (network agnostic approach) impacts the current way of working

# Role and Privilege concepts

Any user

- Is granted with a list of roles
- Each role enables him with a list of privileges
- Each privilege relates to one business function, either in 2-eye or 4-eye

In the future RTGS services, a fixed list of roles is pre-defined (there is no need to allow user administrators to define ad-hoc roles)

# Data scope concept

- Any user
  - Has access to the data of its entity
  - Can be granted access to several entities
- In U2A, the user chooses its entity (so-called “Work as”)
- In the future RTGS services, this data scope is fixed
  - There is no need to extend or restrict this default data scope by entity
- CB users of the service desks are granted access to “act on behalf” of all their participants

## GUI access in T2

- Today, the users are managed by SWIFT (RBAC)
- They identify themselves in the SAG through their DN, and the list of roles and entities is passed by SWIFT to the ICM, allowing to show only the list of allowed screens
- Datascopes are checked by each module

# GUI access in the Future RTGS services

Tomorrow, users connect to the ESMIG, which checks

- Authentication (users are registered with the Common Reference Data)
- That the user is allowed to the requested service (single sign on for all services)

It is up to each service GUI to check that the user is allowed to each business function through its list of roles and privileges. Each module checks the data scope