T2S Access Rights

January 2016

T2S Programme Office
European Central Bank

EUROPEAN CENTRAL BANK
EUROSYSTEM

Introductory Note

This presentation consists of two main parts:

1. an overview of the T2S Access Rights Management model.
The concepts presented in this section are detailed in the T2S documentation (UDFS and UHB) and were also presented in depth in the 2nd T2S Access Rights Workshop on 20 July 2012. The documentation workshop can be found at https://www.ecb.europa.eu/paym/t2s/governance/extmtg/html/mtg43.en.html

2. in-depth information on usage scenarios that are not described in the documentation.
These scenarios refer to specific behaviours that came up during testing.

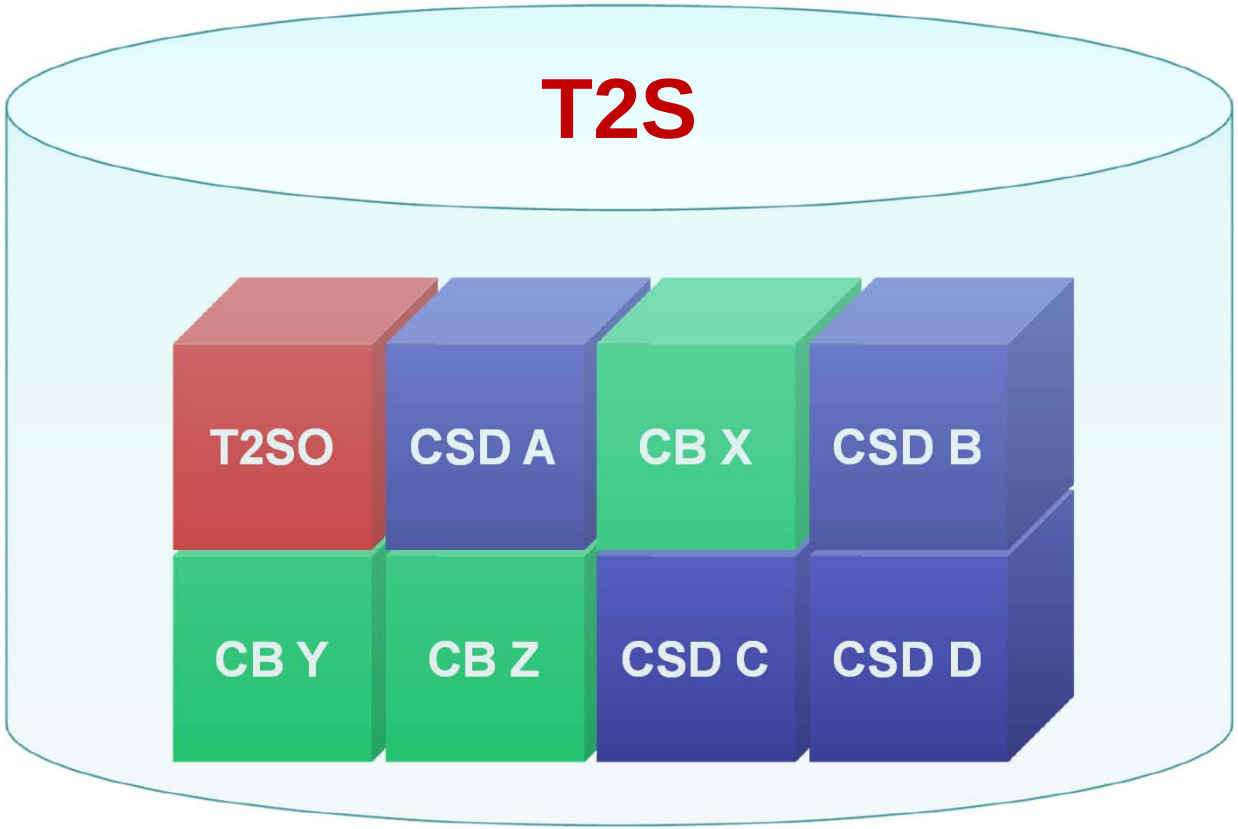
EUROPEAN CENTRAL BANK
EUROSYSTEM

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

System Entities

All data in T2S is partitioned and segregated by System Entity.
Each System Entity corresponds to the scope of a CSD or CB Party.
In addition, the T2S Operator has its own System Entity.

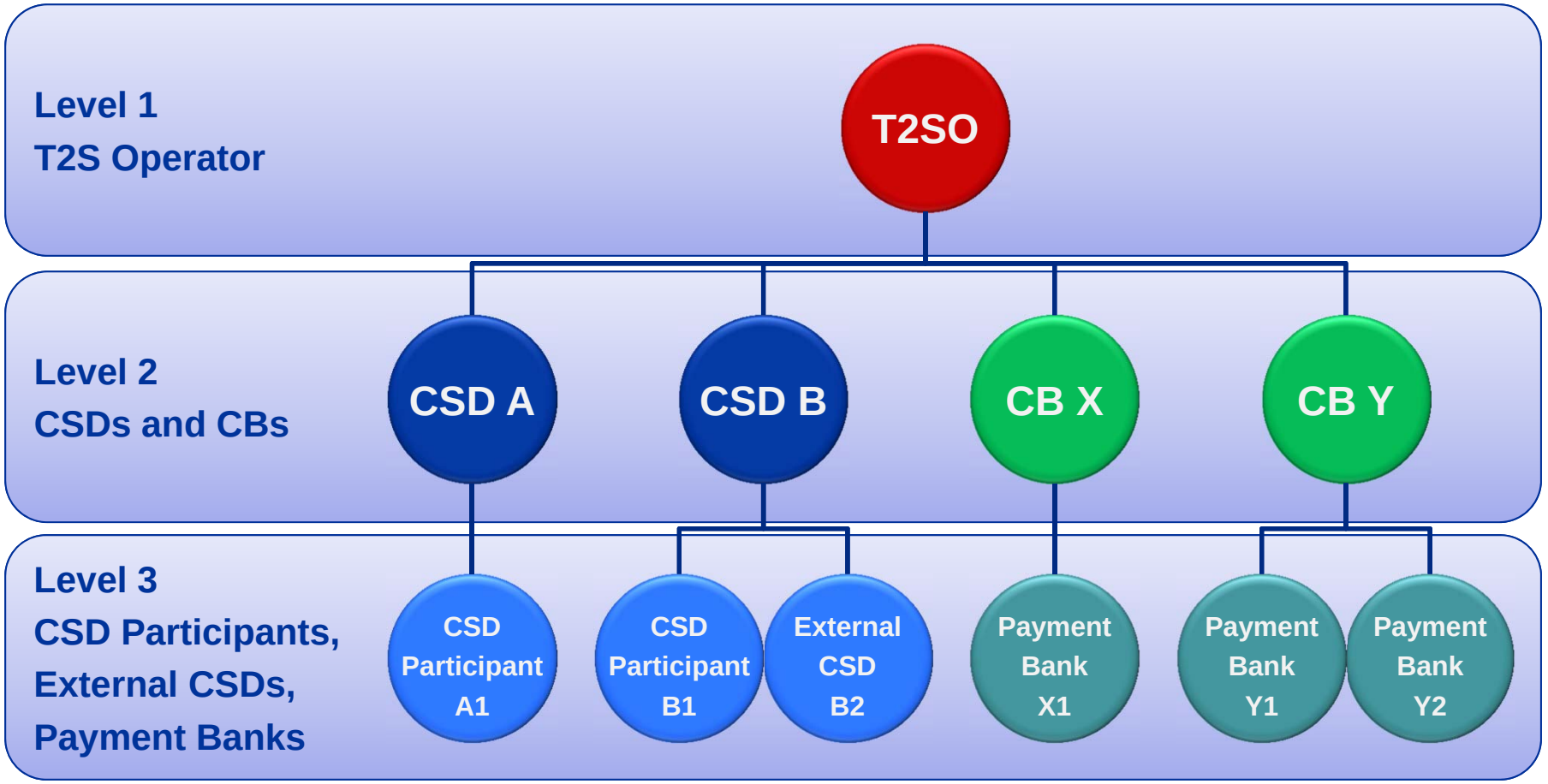


EUROPEAN CENTRAL BANK
EUROSYSTEM

Hierarchical Party Model

Refer to section 1.2.1.3 – Hierarchical party model in UDFS v2.1

T2S follows a three-level hierarchical Party structure.



EUROPEAN CENTRAL BANK
EUROSYSTEM

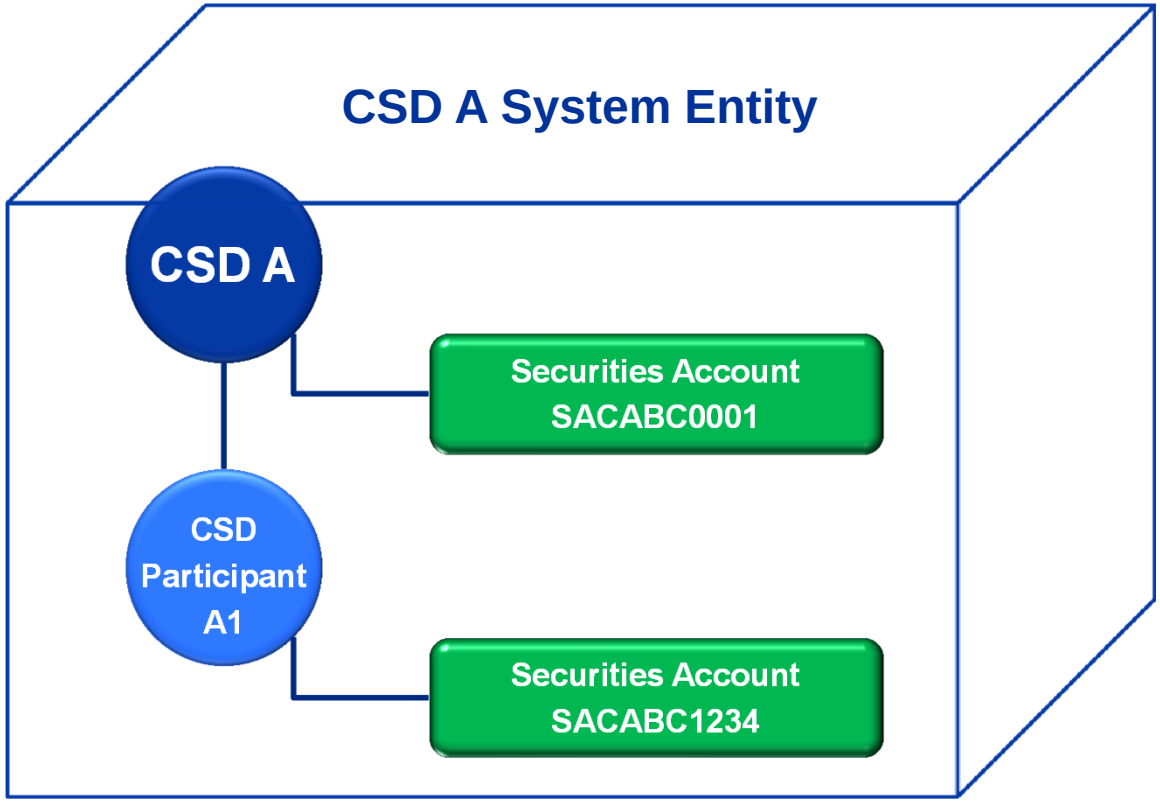
Object ownership

Every Static Data object belongs to a single System Entity.
In addition, certain objects have a direct relationship to a specific Party.

In this example, both Securities Accounts belong to the System Entity of CSD A.

In addition, they have different account holders:

- *For SACABC0001 it's CSD A;*
- *For SACABC1234 it's Party A1.*



EUROPEAN CENTRAL BANK
EUROSYSTEM

Privileges (I)

Refer to section 1.3.3.1.2 – Privilege in UDFS v2.1

T2S Privileges define the **functions** and **objects** that each grantee can access.

There are two types of privileges in T2S:

- **System privileges** can grant access to a specific T2S function. These privileges can only be granted **at system level**, i.e. with no reference to a specific T2S object. This allows the grantee to use that function on a predefined set of objects (normally, the ones within its default ownership)
- **Object privileges** can grant access to a specific T2S function and, optionally, to using that function on a specific object. These privileges can be granted at **system level** and at **object level**, i.e. with reference to a specific T2S object.

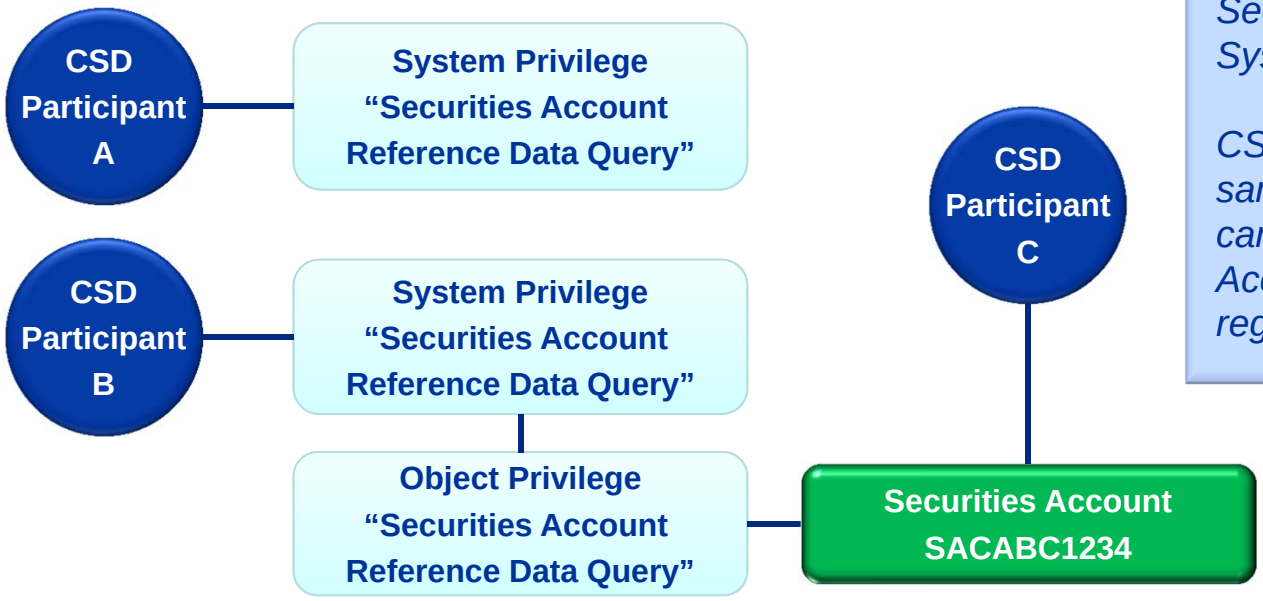
A grantee needs to have a privilege granted at **system level** before they can receive the same privilege at **object level**. In other words, it is necessary to have generic access to the function before it is possible to use that function to access a specific object outside one's ownership.

Privileges (II)

Refer to section 1.3.3.1.2 – Privilege in UDFS v2.1

Privileges granted at **system** level grant generic access to a specific T2S function.

Privileges granted at **object** level grant access to a specific T2S function (such as sending a Settlement Instruction or updating a Securities Account) on a specific object or group of objects.



CSDP A can query the Securities Accounts in its System Entity.

CSDP B can do the same, but in addition they can also query Securities Account SACABC1234, regardless of ownership.

EUROPEAN CENTRAL BANK
EUROSYSTEM

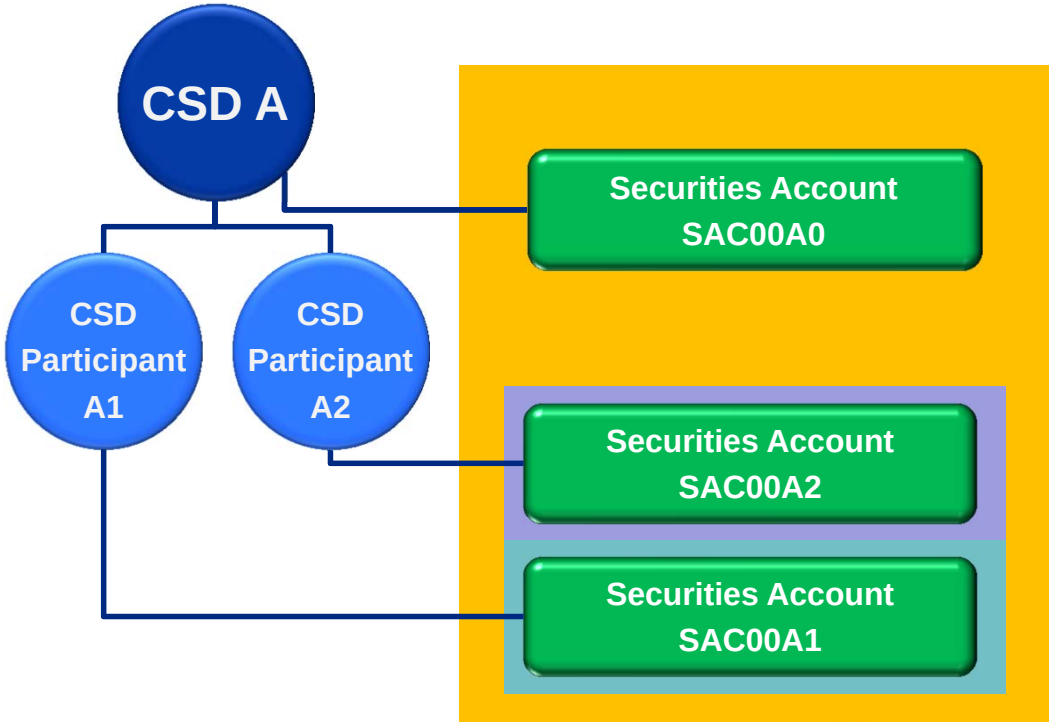
Privileges (III)

Privileges can be granted to Parties, Users and Roles.
Roles contain several privileges and can in turn be granted to Parties and Users.

Data scope (I)

Refer to section 1.3.3.1.8 – Data Scope and Tables 36-47 in UDFS v2.1

The “data scope” is the set of objects on which a grantee can use a certain function. It always refers to a grantee-privilege combination.
Without object privileges, a grantee’s data scope coincides with its **default data scope** for a given privilege. The default data scope is always based on fixed rules.



For privilege ‘Update Securities Account’, the default data scope corresponds to…

- *All Securities Accounts within the grantee’s System Entity (if grantee is a CSD)*
- *All Securities Accounts owned directly by the grantee’s Party (if grantee is a CSD Participant)*

Default data scope of CSD A

Default data scope of CSDP A1

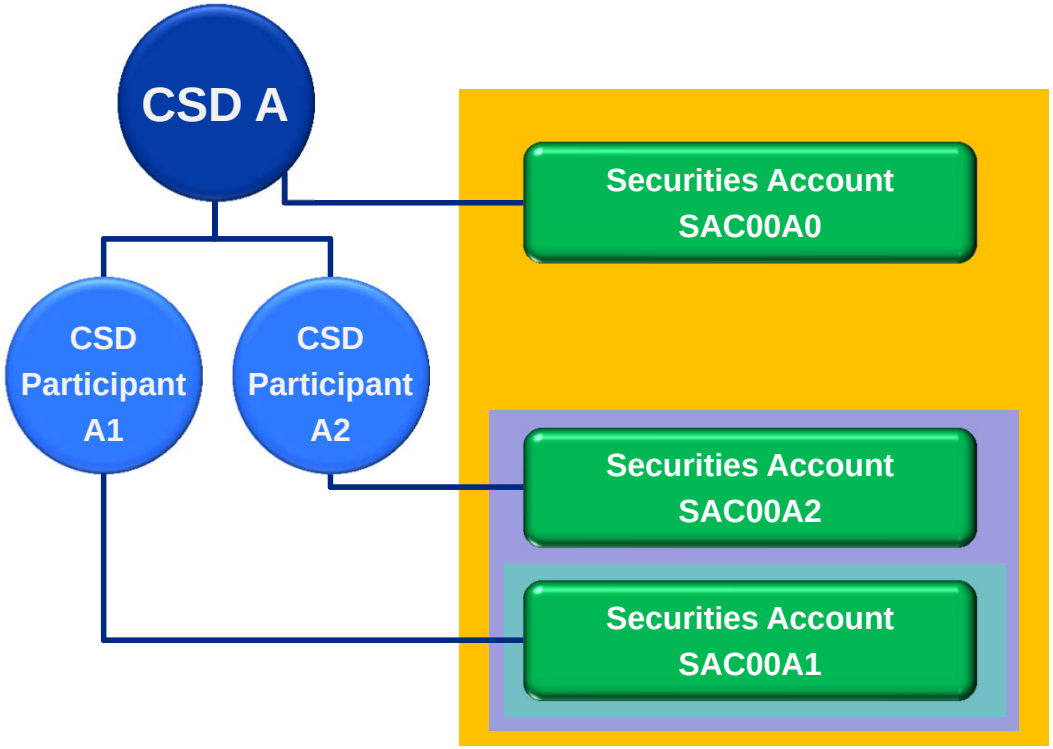
Default data scope of CSDP A2

EUROPEAN CENTRAL BANK
EUROSYSTEM

Data scope (II)

Refer to section 1.3.3.1.8 – Data Scope and Tables 36-47 in UDFS v2.1

The data scope can be extended or reduced by means of object privileges. In that case it no longer corresponds to the default data scope.



If CSD Participant A2 receives an object privilege 'Update Securities Account' with object = SAC00A1, its data scope will be extended to include this object as well.

Data scope of CSD A

Data scope of CSDP A1

Data scope of CSDP A2

EUROPEAN CENTRAL BANK
EUROSYSTEM

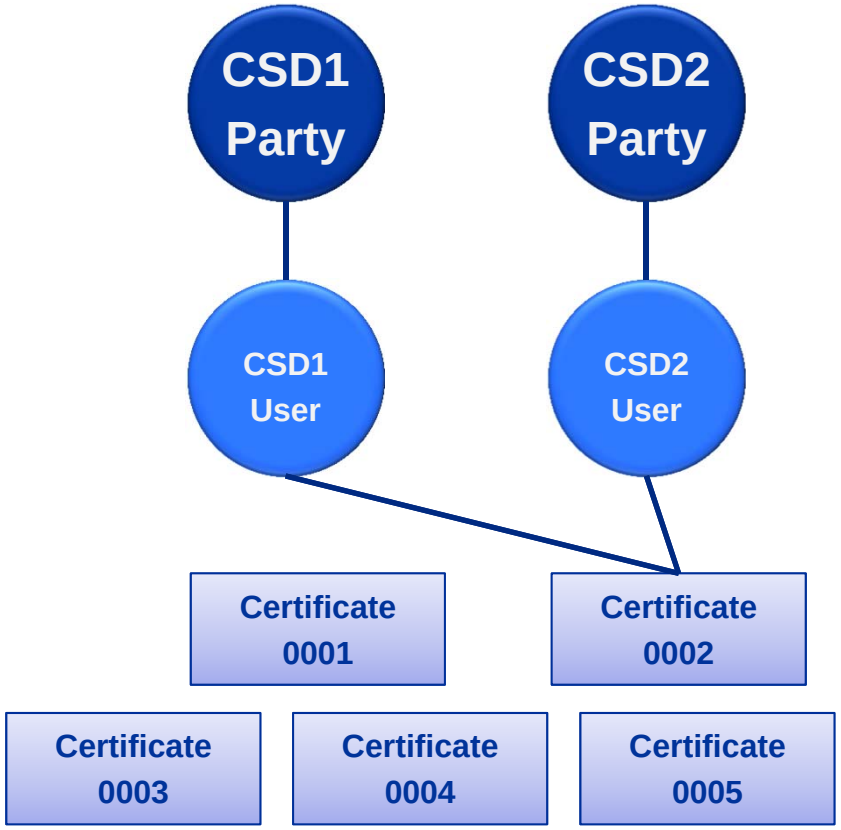
Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Users and Certificates

Refer to section 1.3.2 – Authentication and authorisation in UDFS v2.1

Individuals and applications are identified in T2S by means of digital certificates, which connect them to T2S logical Users. Potentially, any certificate can be linked to any User. With the same certificate, a single individual can access as different logical users within the system.
Administrators are able to view all the Certificates present in the system and link them to the Users under their responsibility.



In this example the same certificate is connected to Users of different CSDs.

The owner of certificate 0002 can access T2S as user of CSD1 and CSD2.

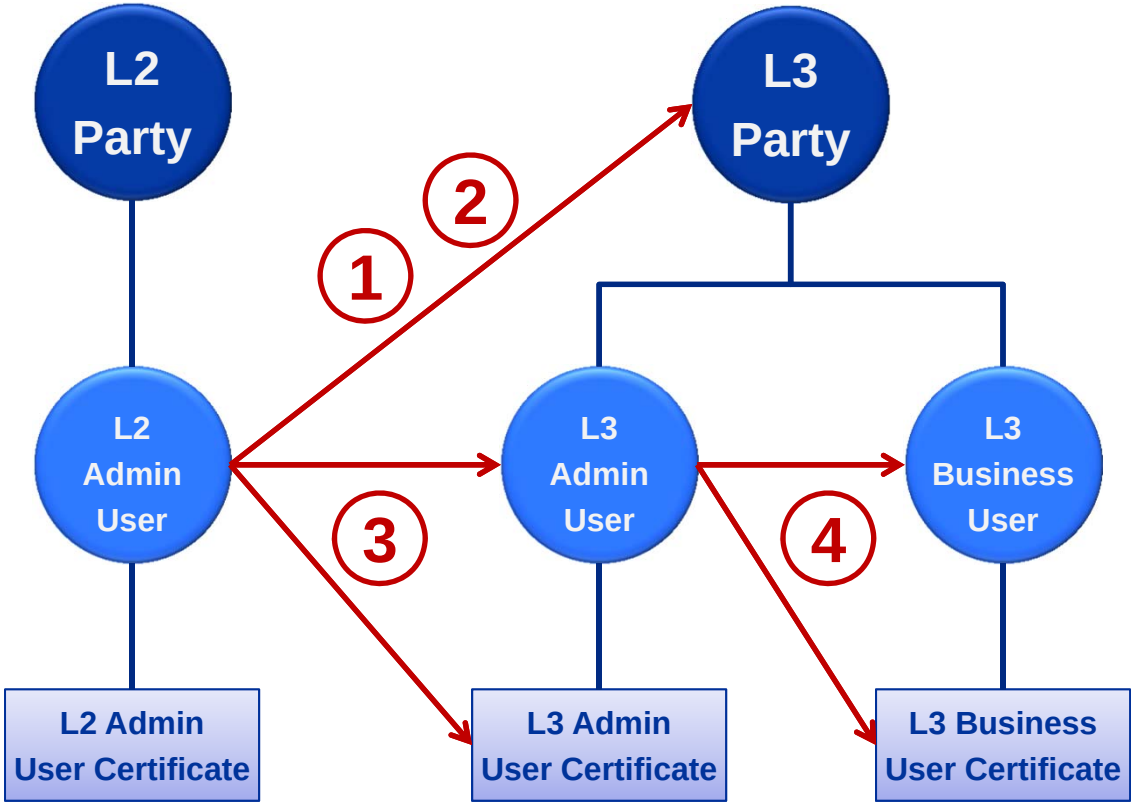
An Administrator of CSD1 can link any T2S certificate with any CSD1 User.

In order to avoid the erroneous creation of such links, it is recommended to maintain them in 4-eyes mode.

EUROPEAN CENTRAL BANK
EUROSYSTEM

Decentralized Access Rights management (I)

Refer to section 1.3.3.2.2 – Configuration of privileges in UDFS v2.1



The setup of a new L3 Party is carried out according to the following steps:

1. *L2 Admin User creates the L3 Party*
2. *L2 Admin User grants privileges/roles to the L3 Party*
3. *L2 Admin User creates L3 Admin User and connects it to the relevant User Certificate*
4. *L3 Admin User can now grant the privileges/roles that are granted to its Party to other users belonging to the same Party.*

Note:
L2 = Level 2 (NCB/CSD Parties)
L3 = Level 3 (Payment Bank/CSD Participant/External CSD Parties)

EUROPEAN CENTRAL BANK
EUROSYSTEM

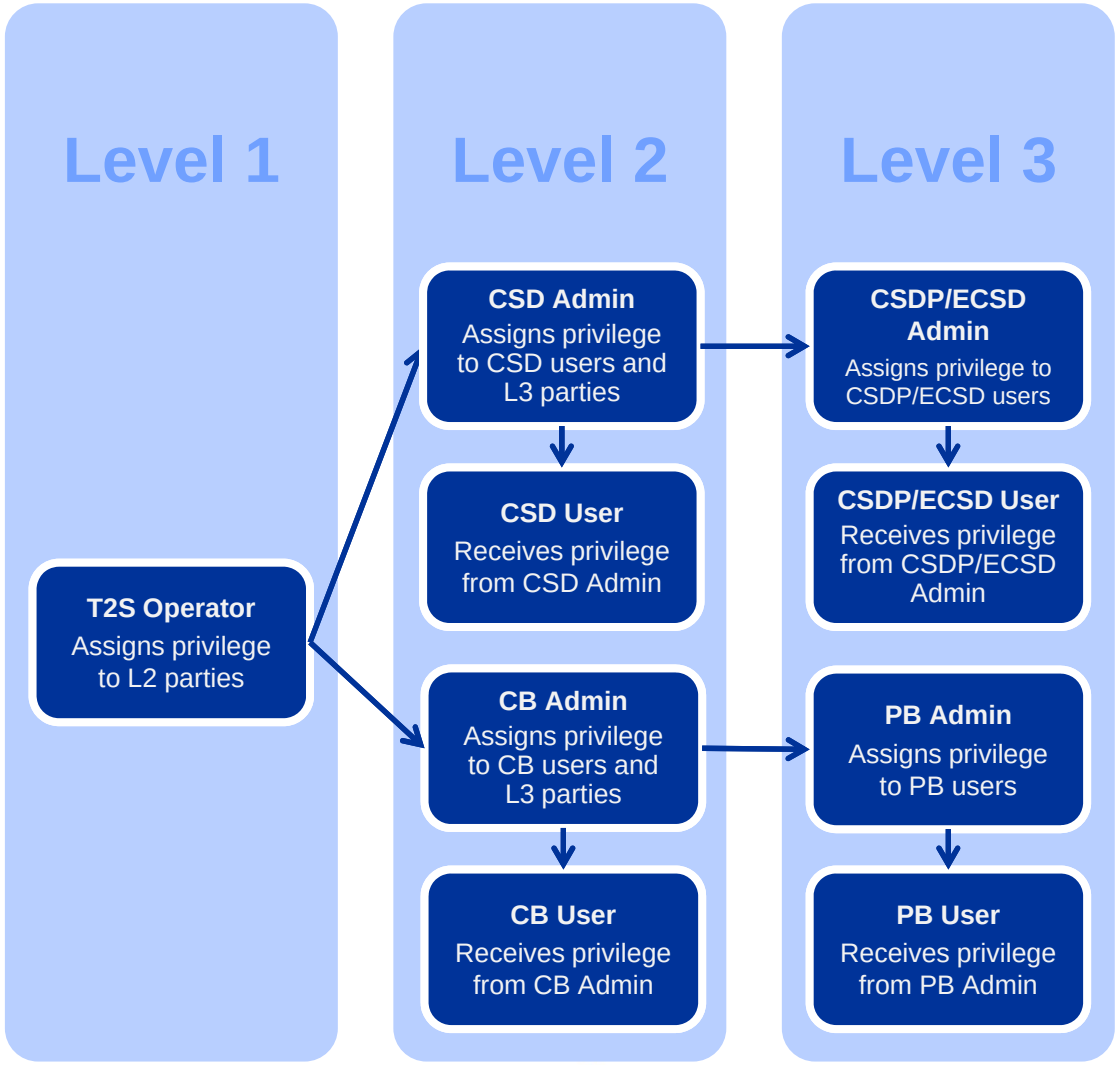
Decentralized Access Rights management (II)

Refer to section 1.3.3.2.2 – Configuration of privileges in UDFS v2.1

The general process described in the previous slide takes place at all levels in T2S.

- The T2S Operator creates CB/CSD Parties and CB/CSD Party Administrator Users and manages their access rights.
- CSD/CB Party Administrators create CSD Participant/External CSD/Payment Bank Parties and their respective Party Administrator Users and manage their access rights. They can also grant rights on their own objects to Parties in other System Entities.
- CSD/CB Business Users use the privileges/roles granted to them by their Party Administrators. They can be optionally authorised to grant and revoke privileges to other Users in their Party.
- CSDP/ECSD/PB Party Administrators manage the access rights of their own Parties' Users. They can also be optionally authorised to grant and revoke privileges to other Parties within their System Entity.
- CSDP/ECSD/PB Business Users use the privileges/roles granted to them by their Party Administrators. They can be optionally authorised to grant and revoke privileges to other Users within their Party.

Decentralized Access Rights management (III)



EUROPEAN CENTRAL BANK
EUROSYSTEM

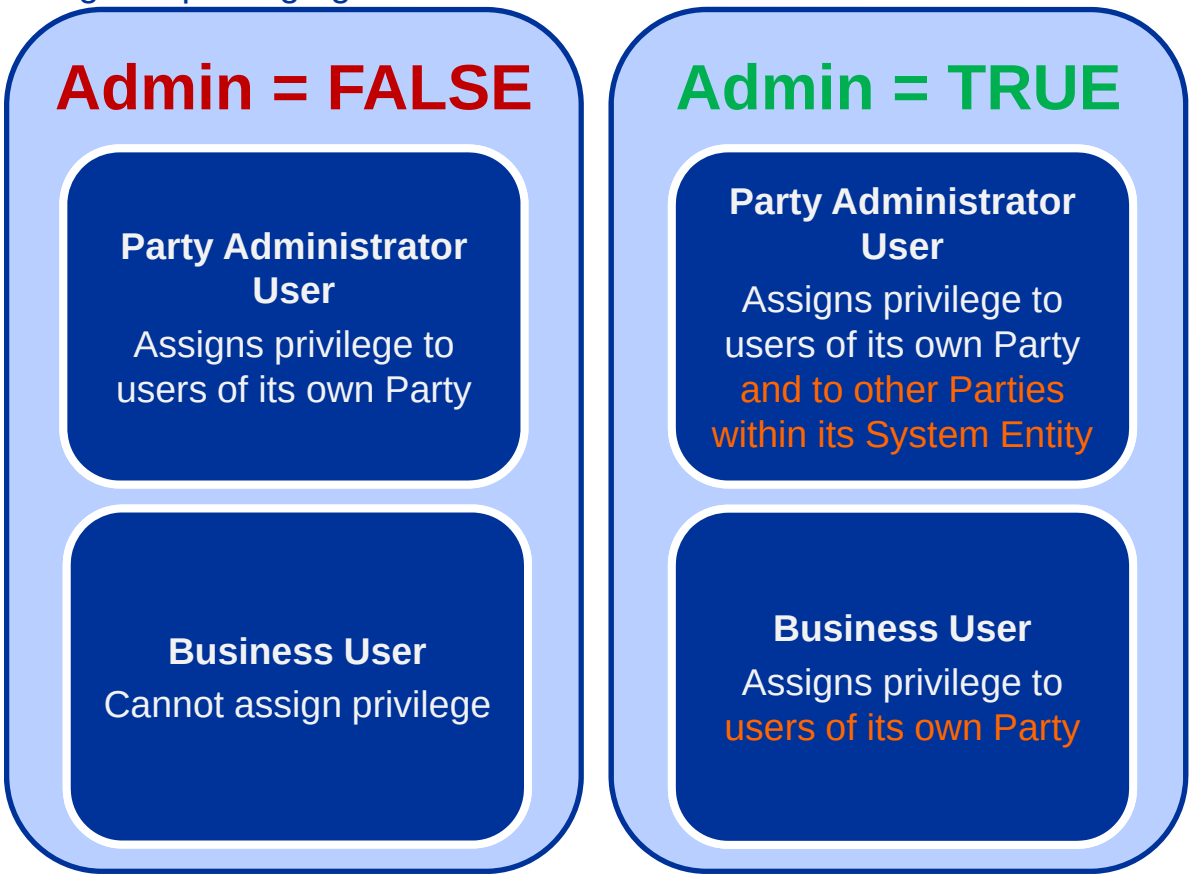
Administration flag

Refer to Table 55 – Privilege Assignment Options in UDFS v2.1

The Administration Flag can be set when granting a Privilege.

The Administration Flag of a privilege granted to a Party affects the Party Administrator User

The Administration Flag of a privilege granted to a User affects the individual Business User directly.



Note: no User can assign privileges to any Party/User on a higher level (e.g. CSD Participant can never assign privileges to its CSD)

EUROPEAN CENTRAL BANK
EUROSYSTEM

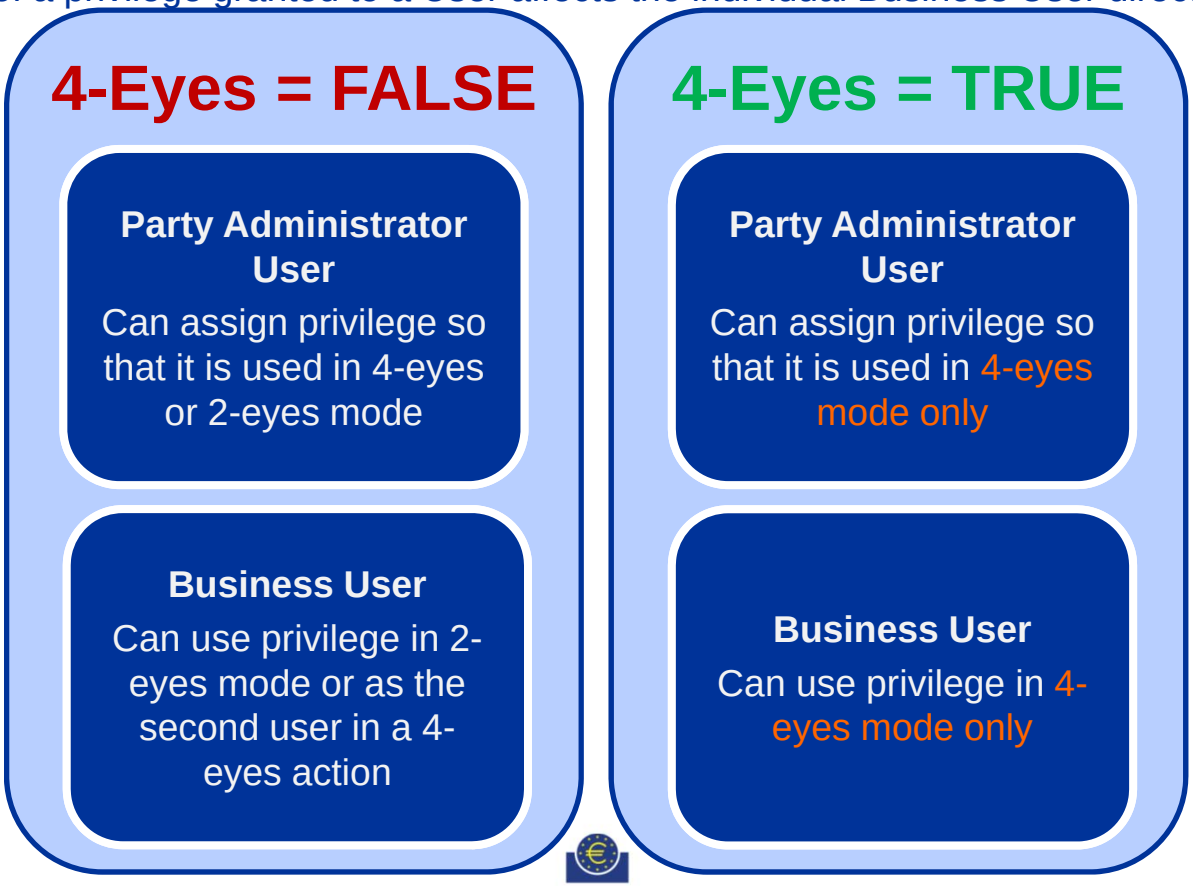
4-Eyes flag

Refer to Table 55 – Privilege Assignment Options in UDFS v2.1

The 4-Eyes Flag can be set when granting a Privilege. A Privilege assigned in 4-Eyes can only be propagated in 4-Eyes.

The 4-Eyes Flag of a privilege granted to a Party affects the Party Administrator User

The 4-Eyes Flag of a privilege granted to a User affects the individual Business User directly.



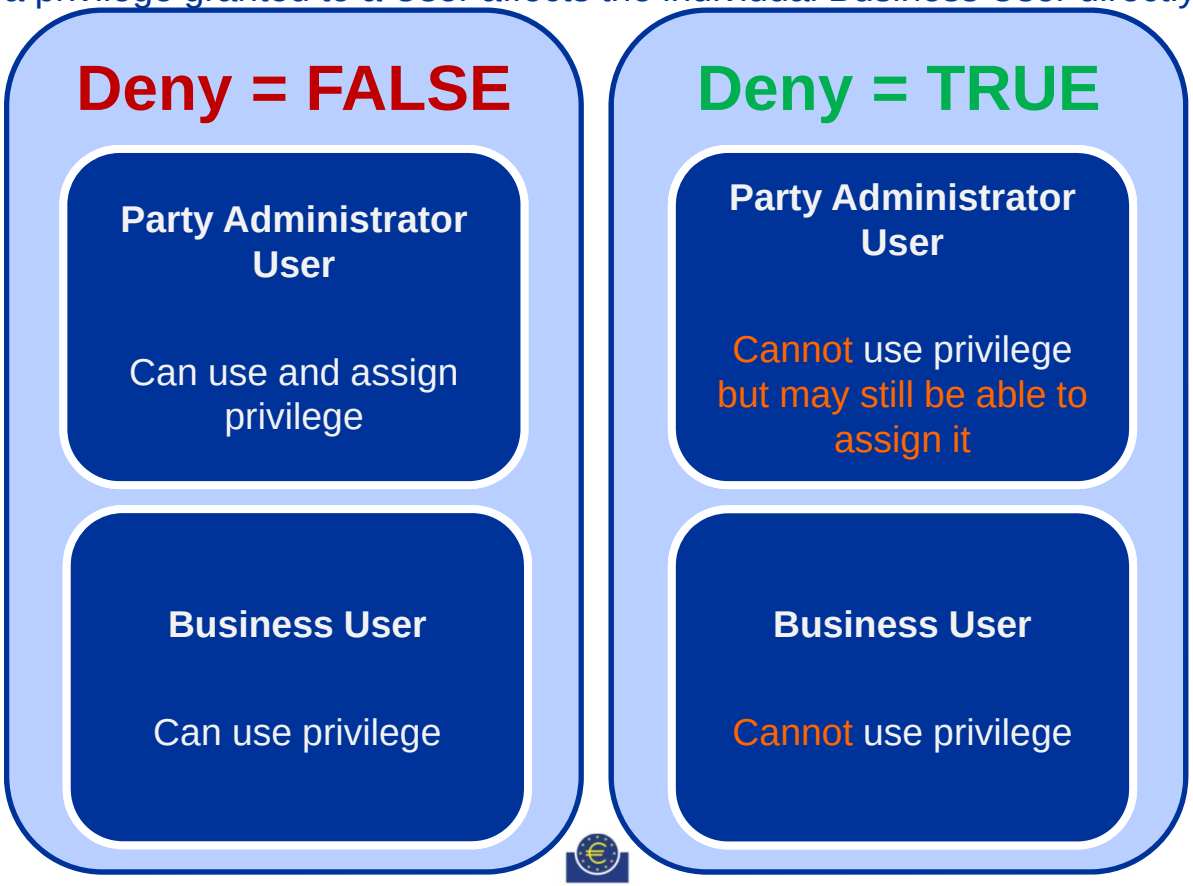
Deny flag

Refer to Table 55 – Privilege Assignment Options in UDFS v2.1

The Deny Flag can be set when granting a Privilege. It is used to block, rather than grant, access to a function or object.

The Deny Flag of a privilege granted to a Party affects the Party Administrator User

The Deny Flag of a privilege granted to a User affects the individual Business User directly.



EUROPEAN CENTRAL BANK
EUROSYSTEM

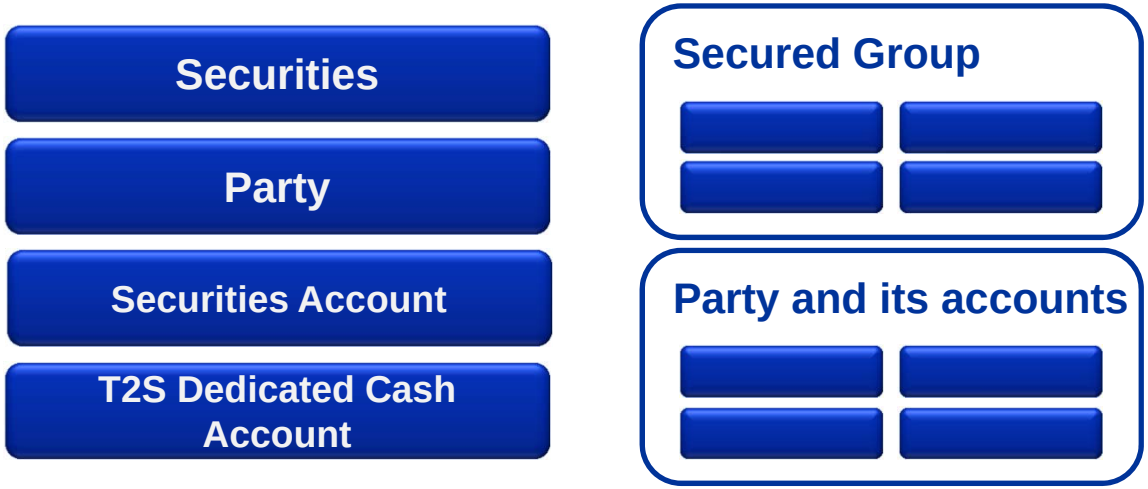
Types of secured objects

Refer to section 1.3.3.1.3 – Secured object and 1.3.3.1.4 – Secured group in UDFS v2.1

Object privileges can be used to grant access to a specific function on a specific **secured object**, e.g.

- Send a settlement instruction on behalf of a given CSD Participant;
- Update a given Party;
- Order a liquidity transfer on a given T2S dedicated cash account.

Only a limited number of objects may be used as secured objects.



A Secured Group contains a homogeneous set of Static Data objects (i.e. a set of Parties or a set of Securities accounts, etc.)

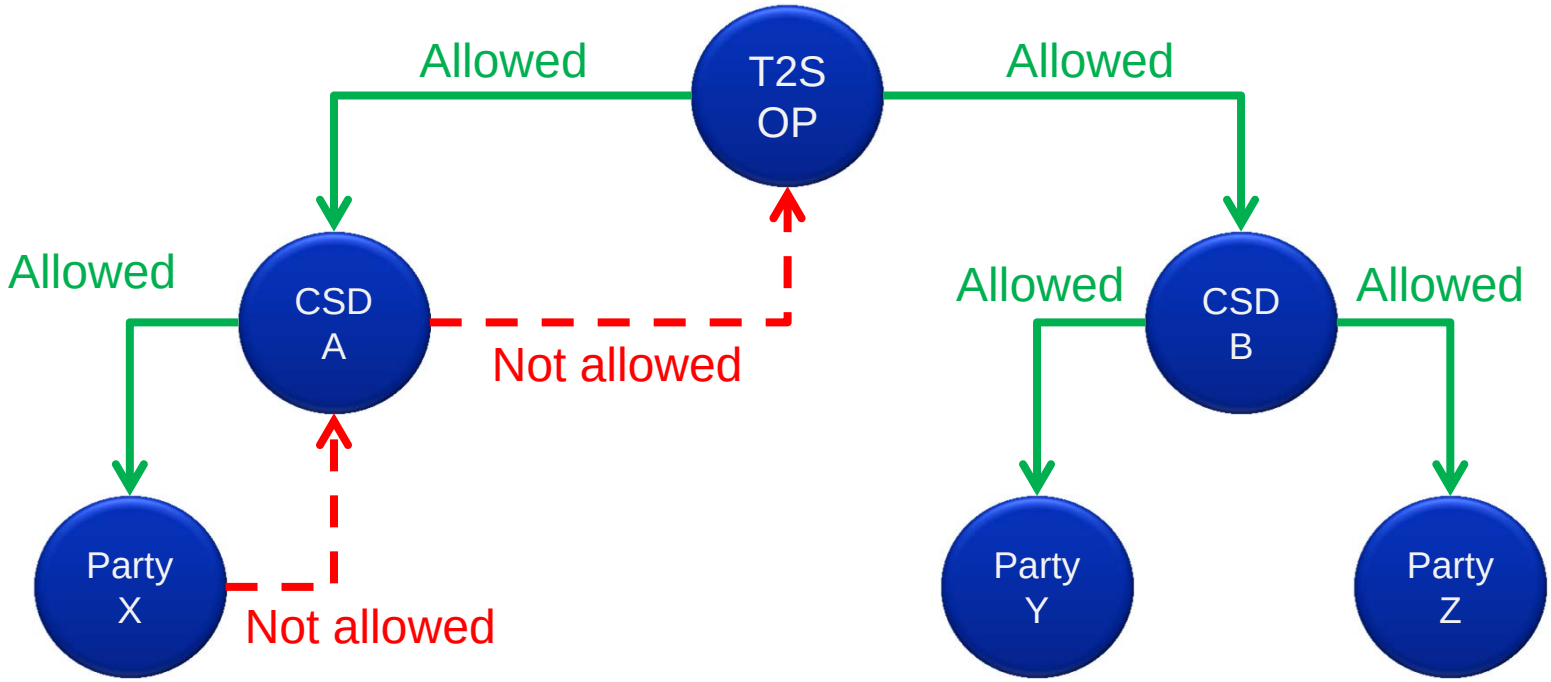
"Party and its accounts" allows to select all the cash/securities accounts that belong to a given party without having to input them individually.

Secured Groups are identified by means of a technical identifier that is automatically assigned upon creation and can be retrieved by querying the specific Secured Group.

Configuration of privileges for Parties (I)

There are two main paths to follow to propagate a privilege across parties: **top-down** and **transversal.**
Both **system** and **object privileges** can be propagated top-down.

Top-down propagation



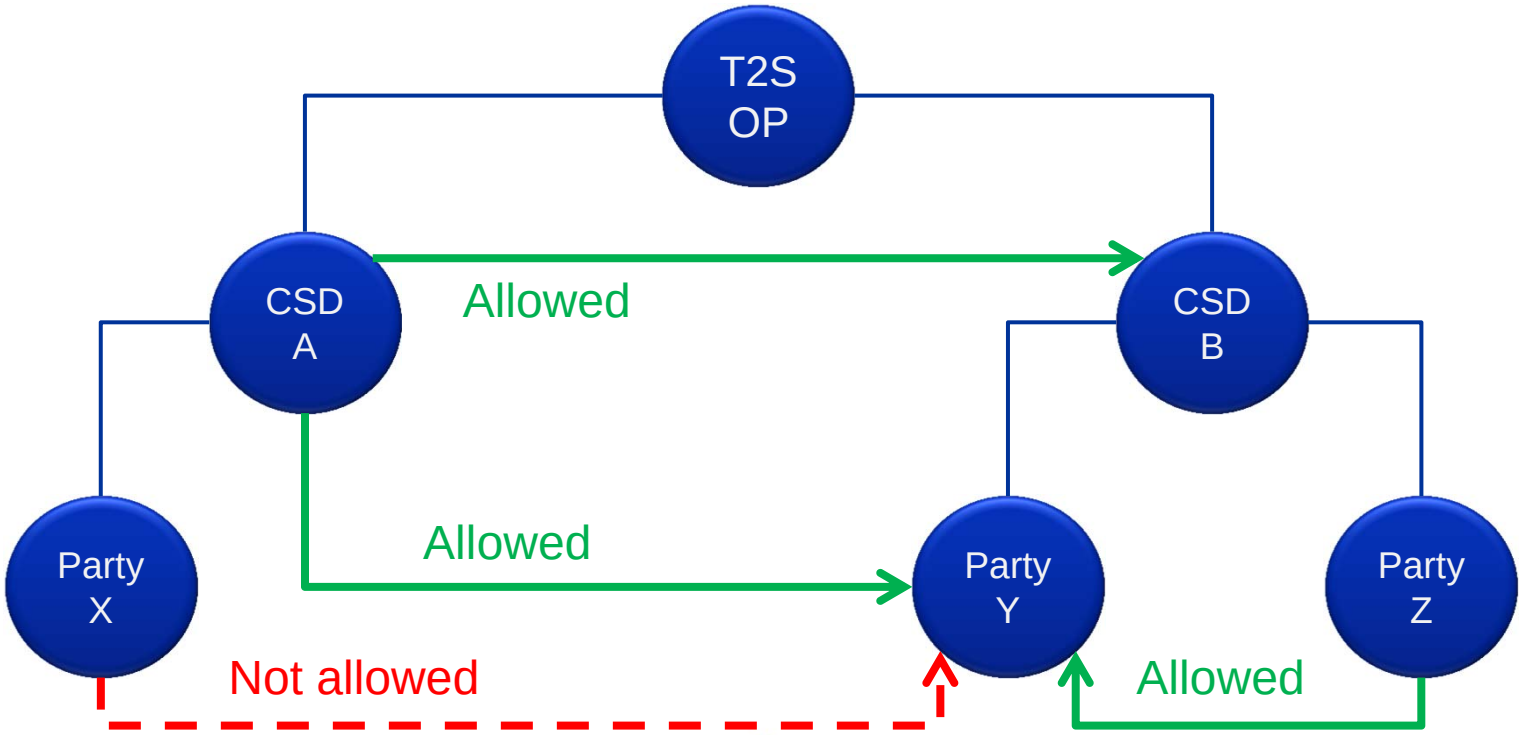
See also “List of privileges and third party receipt” in the Knowledge Base.

EUROPEAN CENTRAL BANK
EUROSYSTEM

Configuration of privileges for Parties (II)

There are two main paths to follow to propagate a privilege across parties: **top-down** and **transversal.**
Only **object privileges** can follow transversal propagation.

Transversal propagation



See also “List of privileges and third party receipt” in the Knowledge Base.

EUROPEAN CENTRAL BANK
EUROSYSTEM

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

T2S documentation (I)

Refer to section 1.3.3.1.2 – Privilege in UDFS v2.1

The UDFS contain a list of privileges that can be used to trigger A2A functions.

Descriptive privilege name

XML message that the privilege enables to use

PRIVILEGE	T2S USER FUNCTION (MESSAGE)
Send New Settlement Instruction/Settlement Restriction on Securities either on a Securities Account or on Behalf of an external CSD	SecuritiesSettlementTransactionInstruction

System = privilege can only be granted at system level.
Object = privilege can be granted at system and object level.

PRIVILEGE TYPE	OBJECT TYPE	DEFAULT DATA SCOPE
Object	Party Securities Account	All Settlement Instructions on Securities Accounts within own System Entity (for CSD) or owned by own Party (for CSD Participant and External CSD)

Secured object types that the privilege can be granted on (only at object level)

Default set of objects on which the privilege applies at system level

Related to issue T2SQ-3107.

EUROPEAN CENTRAL BANK
EUROSYSTEM

T2S documentation (II)

Refer to section 6.3 List of Privileges in UHB v2.1

The UHB contains the privileges for U2A mode (i.e., all the T2S privileges)

Individual screen descriptions list the privileges required to access them and to use all their functionalities…

…this list links to the list for each specific screen in section 6.3…

…which also contains a full list of T2S privileges.

Privileges

To use this screen, you need the following privileges [▸ 2030]:

- Send new settlement instruction/settlement restriction on securities either on a securities account or on behalf of an external CSD
- Send new instruction using a specific instructing party

6.3.3.172 Settlement Instruction - New Screen

⌂ [▸ 215]

Privilege	Privilege Code	Privilege Type	Object Types	Screen Criteria
Send New Settlement Instruction/Settlement Restriction on Securities either on a Securities Account or on Behalf of an external CSD	SIG_SNDSI	Object	Securities Account Party	Securities Account (just for the object)

Class of Privileges	Privilege Name	Privilege Short Name
Settlement General	Send New Settlement Instruction/Settlement Restriction on Securities either on a Securities Account or on Behalf of an external CSD	SIG_SNDSI

The "Privilege Code" is the label that identifies the privilege in the T2S GUI.

Related to issue T2SQ-3107.

T2S documentation (III)

The UHB also includes general usage indications based on the initial privilege assignments to each Party type.

2.5.2.4 Close Link - New Screen

Context of Usage	This screen contains a number of fields regarding close links. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.
	This screen is not relevant for payment bank, external CSD or CSD participant users.

Each screen description also lists whether specific privilege assignments can influence this.

2.5.4.17 T2S Dedicated Cash Account – New/Edit Screen

Context of Usage	This screen contains a number of fields regarding T2S dedicated cash accounts. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.
	This screen is not relevant for CSD, CSD participant or external CSD users unless they are granted with the proper system and object privileges.

Related to issue T2SQ-2616.

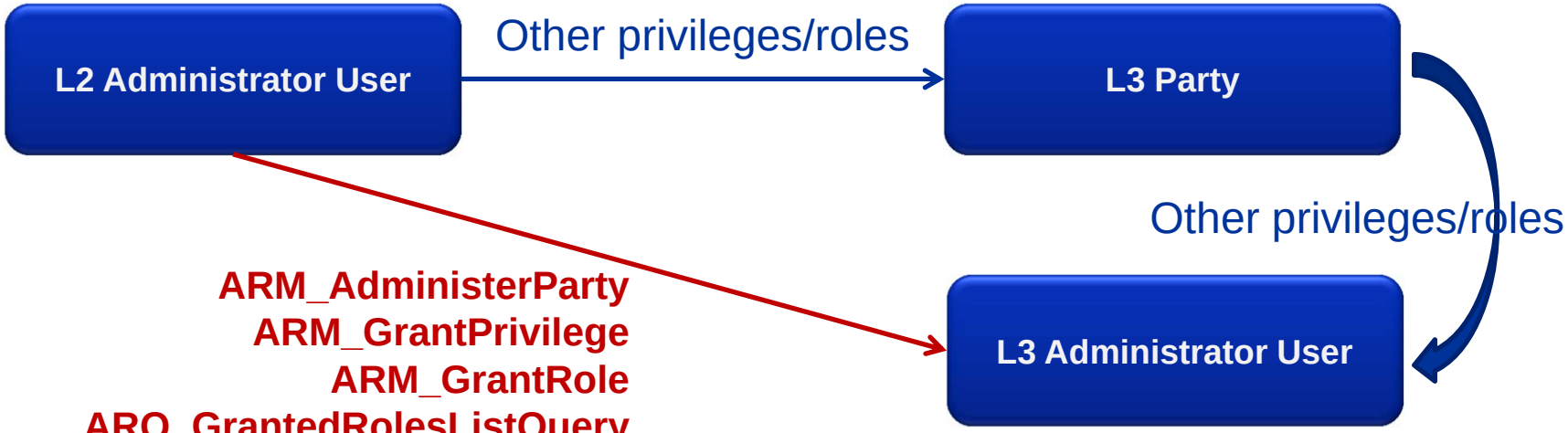
EUROPEAN CENTRAL BANK
EUROSYSTEM

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Administrator privileges (I)

Normally, Level 2 administrators grant privileges to Level 3 parties; then Level 3 administrators propagate them to the users.
In the initial setup phase of a party, however, the Level 2 administrator must grant a specific set of privileges directly to one or more Level 3 users: this is in order to designate them as Party Administrators. These privileges are highlighted in red below.



ARM_AdministerParty
ARM_GrantPrivilege
ARM_GrantRole
ARQ_GrantedRolesListQuery
ARQ_GrantedSysPrivilegesListQuery
ARQ_GrantObjectPrivilegesListQuery

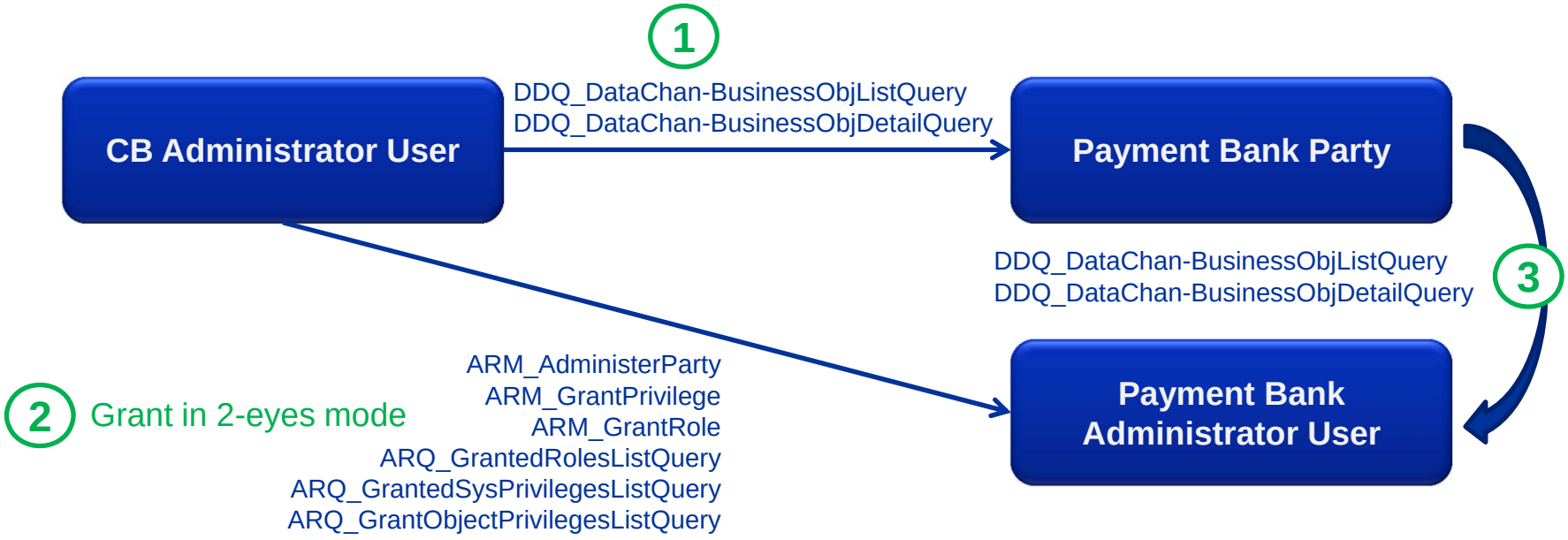
EUROPEAN CENTRAL BANK
EUROSYSTEM

Administrator privileges (II)

If the grantee party operates in 4-Eyes mode, two additional privileges are required:

- **DDQ_DataChan-BusinessObjListQuery**
- **DDQ_DataChan-BusinessObjDetailQuery**

However it is not possible to grant them directly to users of a different Party.
Therefore the following procedure is applied:



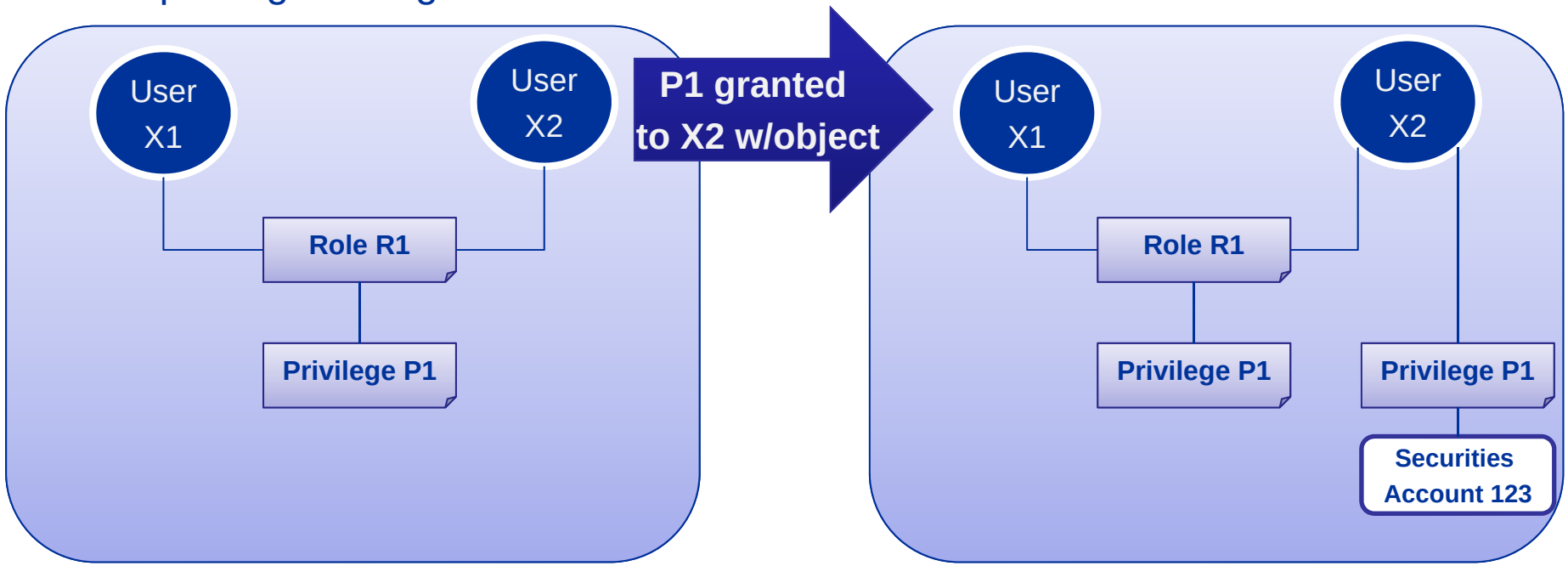
EUROPEAN CENTRAL BANK
EUROSYSTEM

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Directly assigned privileges (I)

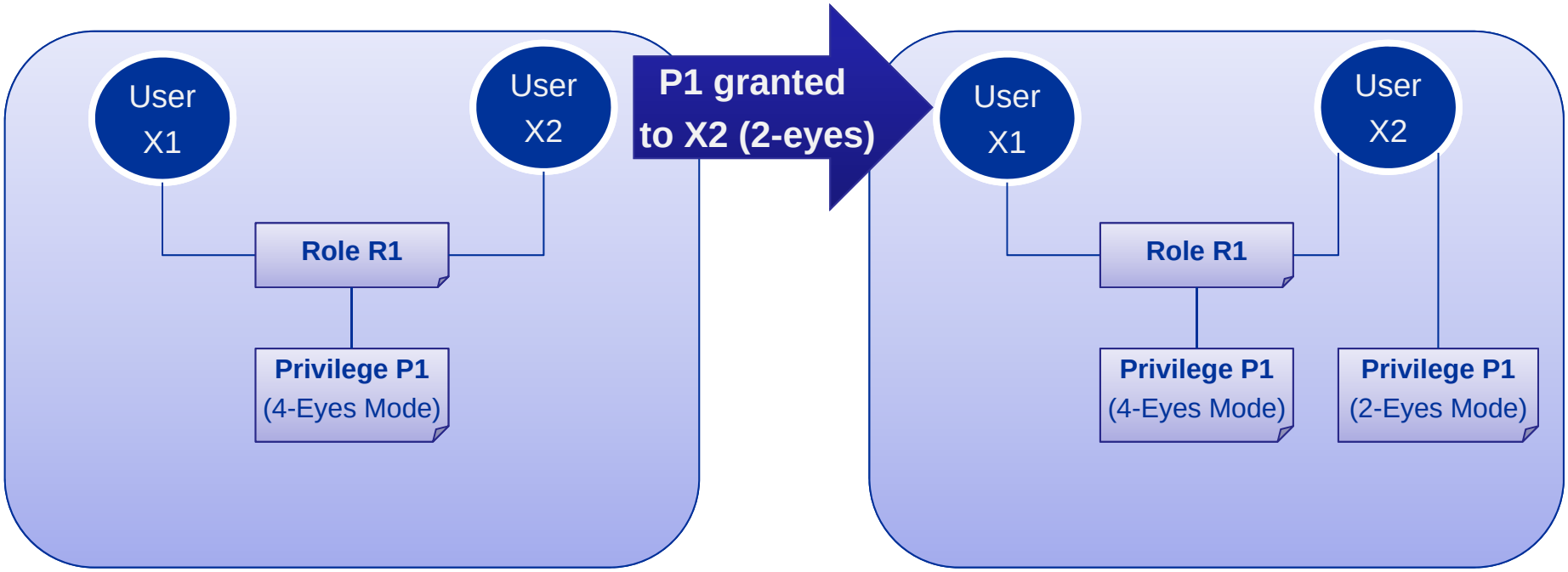
Parties and Users that have a certain privilege assigned via a Role can be granted the same privilege again directly. This is useful, for example, to extend the data scope of a specific User without changing it for all the other Users that have the same Role. **Directly assigned privileges have priority** over the same privileges assigned via role.



In this example User X2 has access to Securities Account 123; User X1 does not.

Directly assigned privileges (II)

Similarly, Users and Parties may receive directly-assigned privileges with different flags than the ones they have via roles. Again, the directly-assigned privileges have priority.



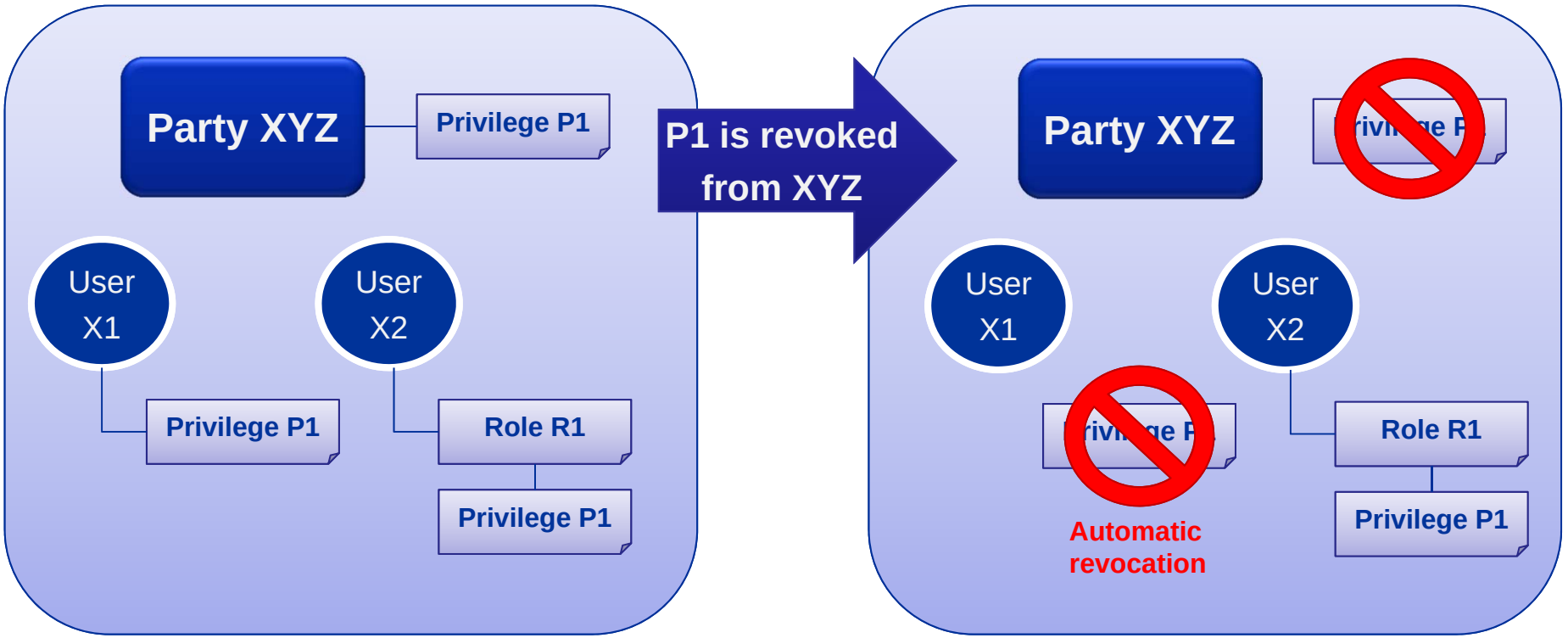
In this example User X2 can only use privilege P1 in 2-eyes mode, while User X1 can only use it in 4-eyes mode.

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Cascade effect when revoking privileges (I)

When a privilege is revoked from a Party, the same privilege is also revoked from any User of that Party that possesses the same privilege, but **only** if both the Party and User(s) have the privilege assigned directly (i.e. not via Role).



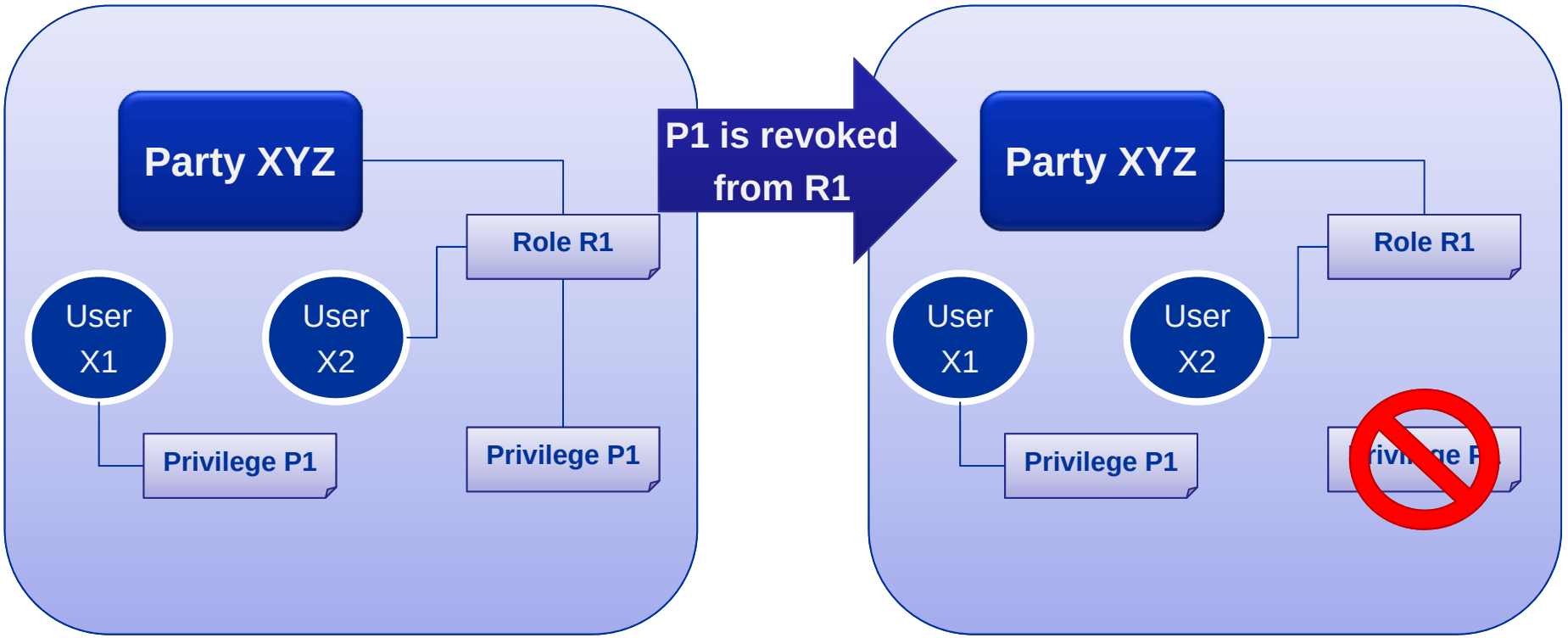
In this example User X2 keeps Privilege P1 even after it is revoked from the Party.

This cascade effect is deferred and carried out at regular intervals. The T2S Operator can schedule it at specific points in time if required.

EUROPEAN CENTRAL BANK
EUROSYSTEM

Cascade effect when revoking privileges (II)

If a privilege is revoked from a role, that has immediate effect on all Users/Parties connected to that role but there is no cascade effect (e.g. Users with the privilege assigned directly will keep it)



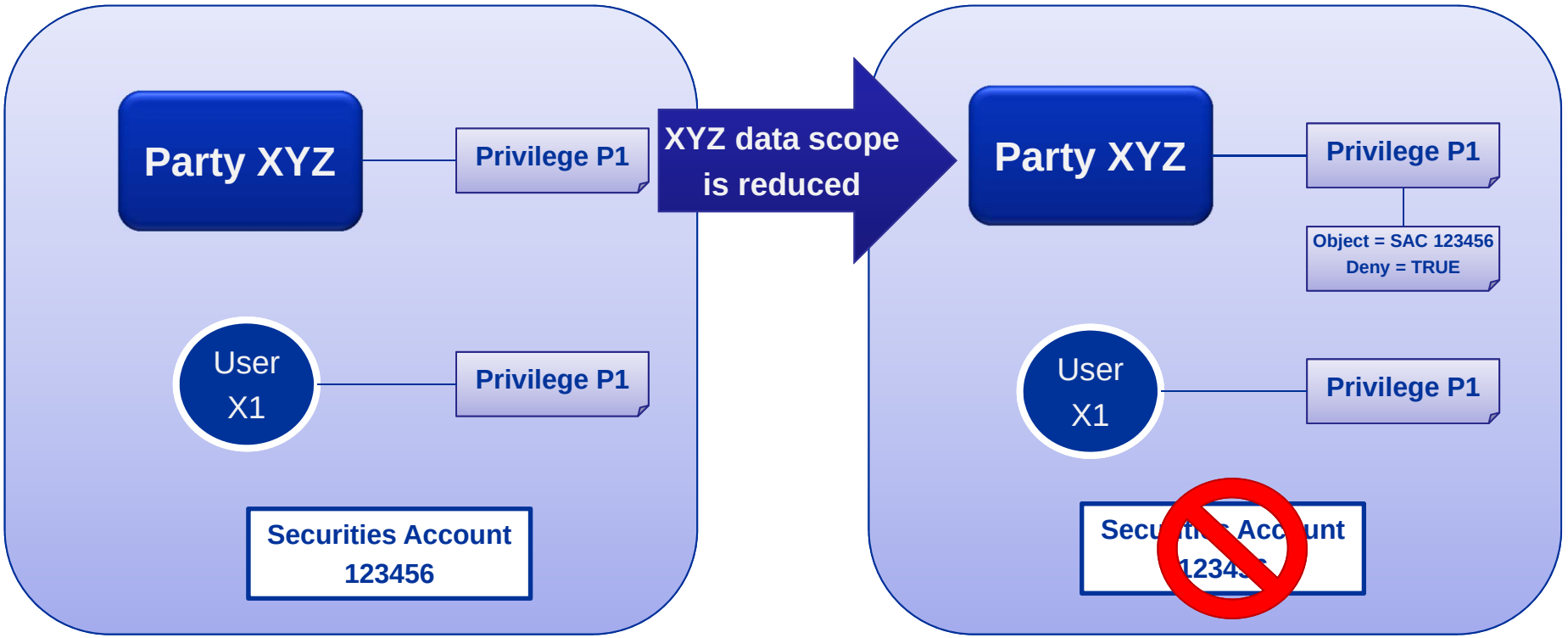
In this example User X1 keeps Privilege P1 even after it is revoked from the Role.

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Effects of data scope reduction at Party level

A data scope reduction (i.e. granting an object privilege with Deny = TRUE) to a Party is automatically propagated to all Users of that Party. This is not reflected by a cascade process, i.e. the privileges are not actually granted to the Users.



After the reduction User X1 is not able to access Securities Account 123456.

This effect is deferred and carried out at regular intervals. The T2S Operator can schedule it at specific points in time if required.

EUROPEAN CENTRAL BANK
EUROSYSTEM

Table of Contents

EUROPEAN CENTRAL BANK
EUROSYSTEM

Change in Privilege granularity

- In scenarios typically related to Change Request implementation, it might be required to introduce new privileges to cover the related user functions with a different granularity.
- For example, a privilege that covers different functionalities may be restricted to a smaller set, while a new privilege is introduced to cover the remaining ones.
- This was the case for Change Request 545.

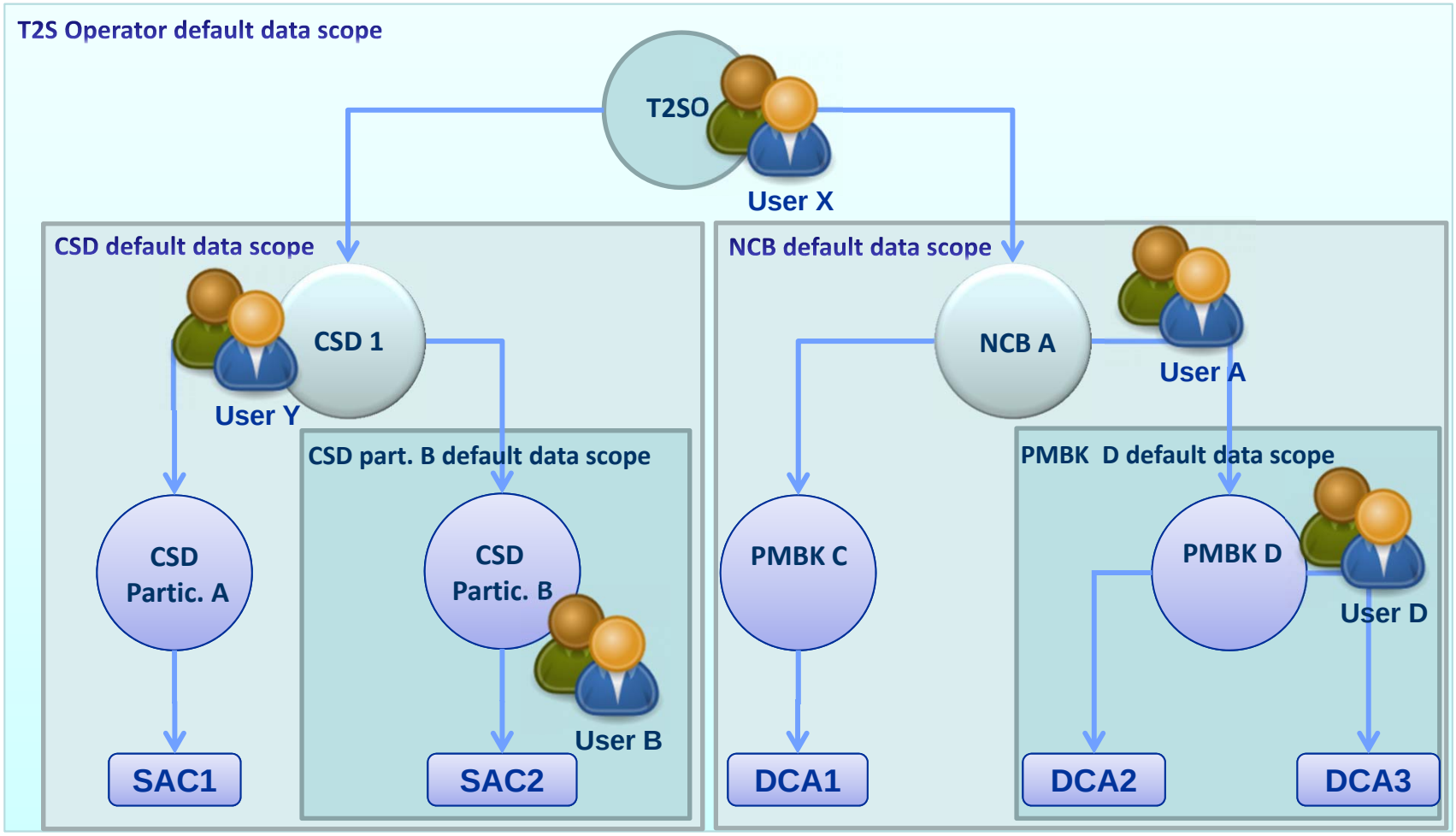
BEFORE CR545	
User function	**System Privilege**
Release regular pending settlement instructions	Release Party Hold Settlement Instruction
Release pending reverse auto-collateralisation instructions	Release Party Hold Settlement Instruction

AFTER CR545	
User function	**System Privilege**
Release regular pending settlement instructions	Release Party Hold Settlement Instruction
Release pending reverse auto-collateralisation instructions	Release Party Hold Autocollat Instruction

Change in Privilege granularity (II)

- This implies that grantees that had the “old” privilege may require only that one or both, while grantees that did not have the “old” privilege may require one.
- In other words, there is a “cutover” phase where the new privilege needs to be granted to all grantees that are required to use it.
- The following slides illustrate this cutover process by using the example of CR 545.

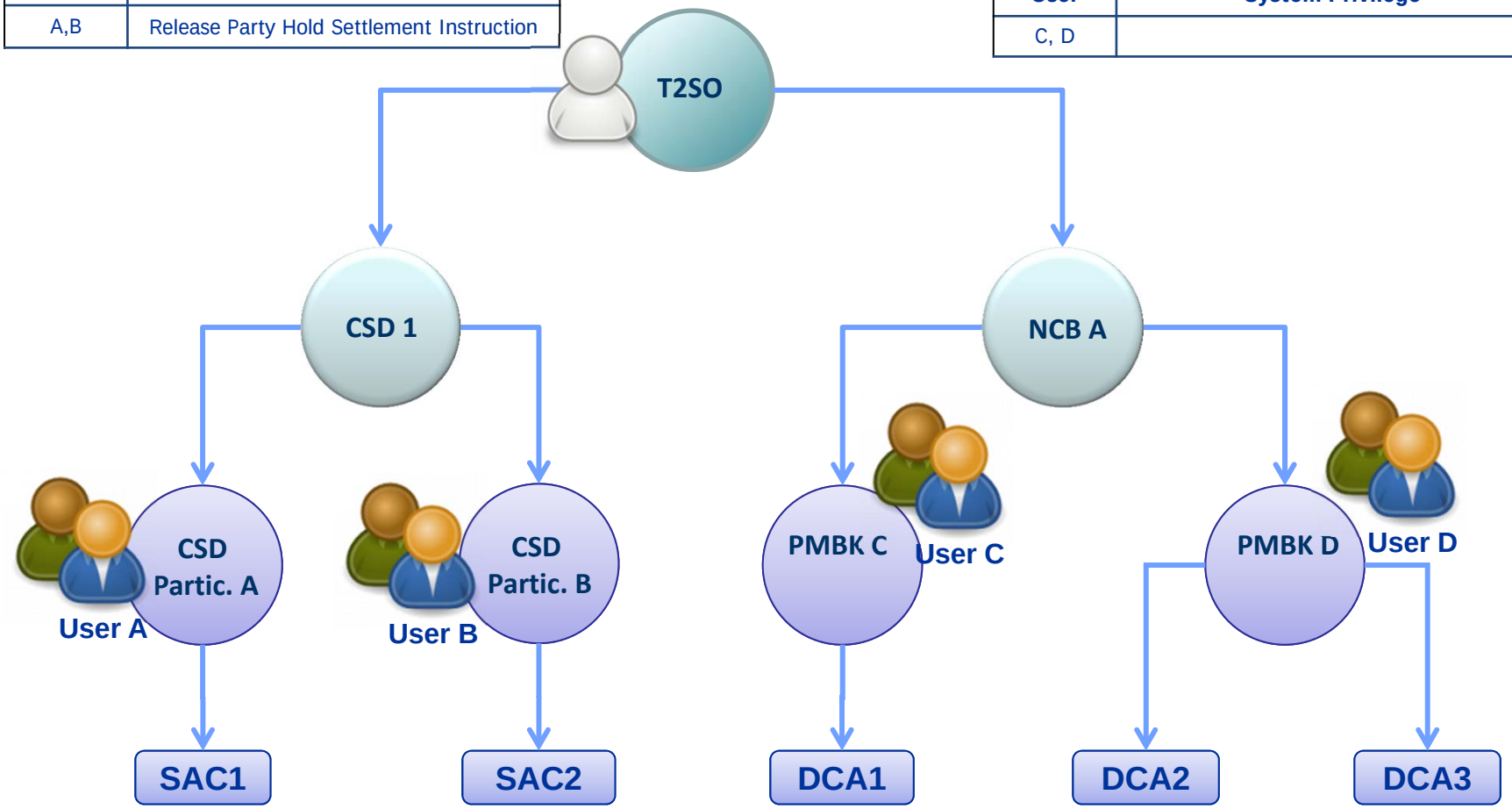
Default data scope diagram



Situation before the cutover

User	System Privilege
A,B	Release Party Hold Settlement Instruction

User	System Privilege
C, D	

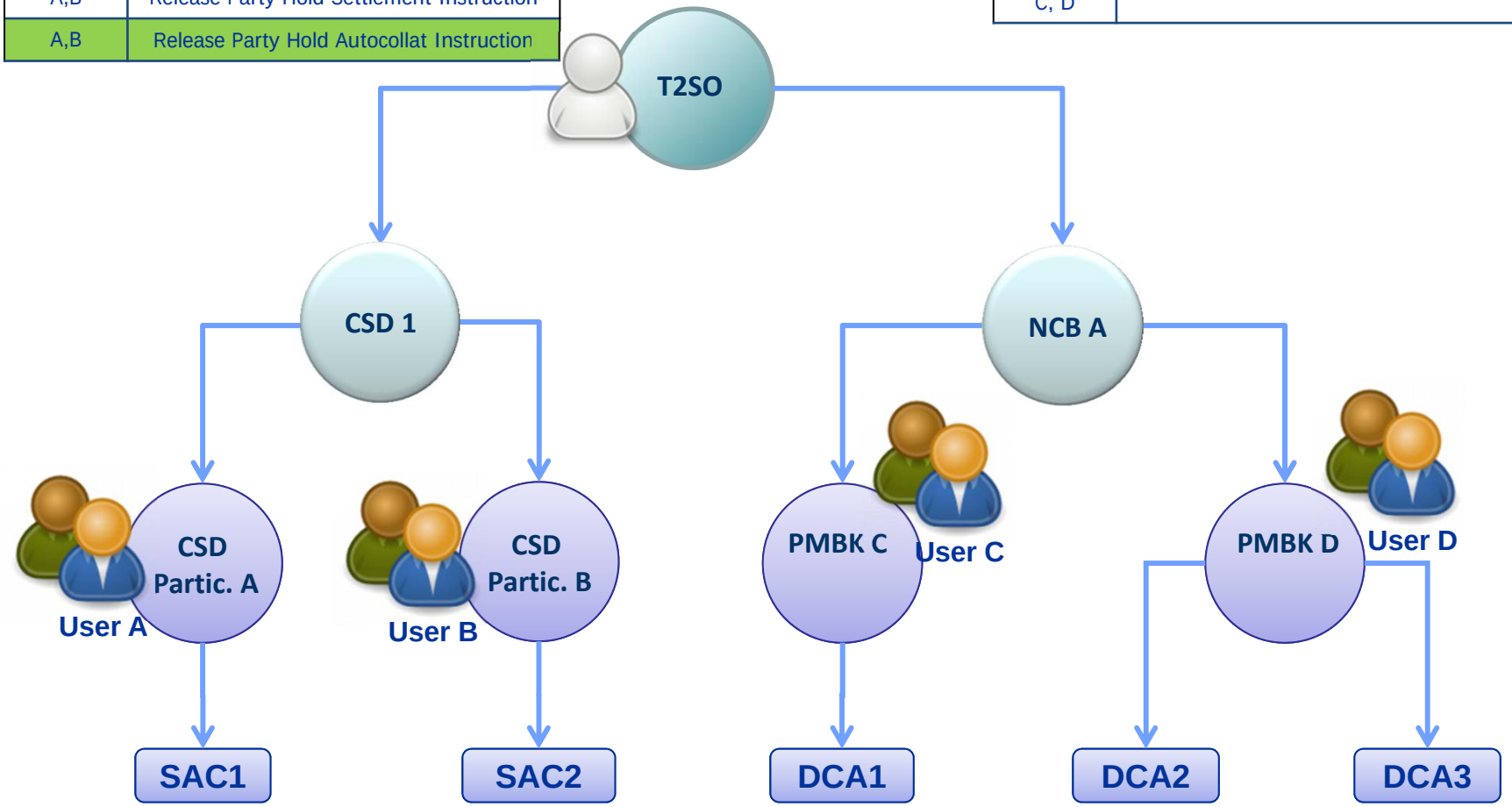


EUROPEAN CENTRAL BANK
EUROSYSTEM

Situation after the cutover

User	System Privilege
A,B	Release Party Hold Settlement Instruction
A,B	Release Party Hold Autocollat Instruction

User	System Privilege
C, D	



EUROPEAN CENTRAL BANK
EUROSYSTEM

New privilege scenarios

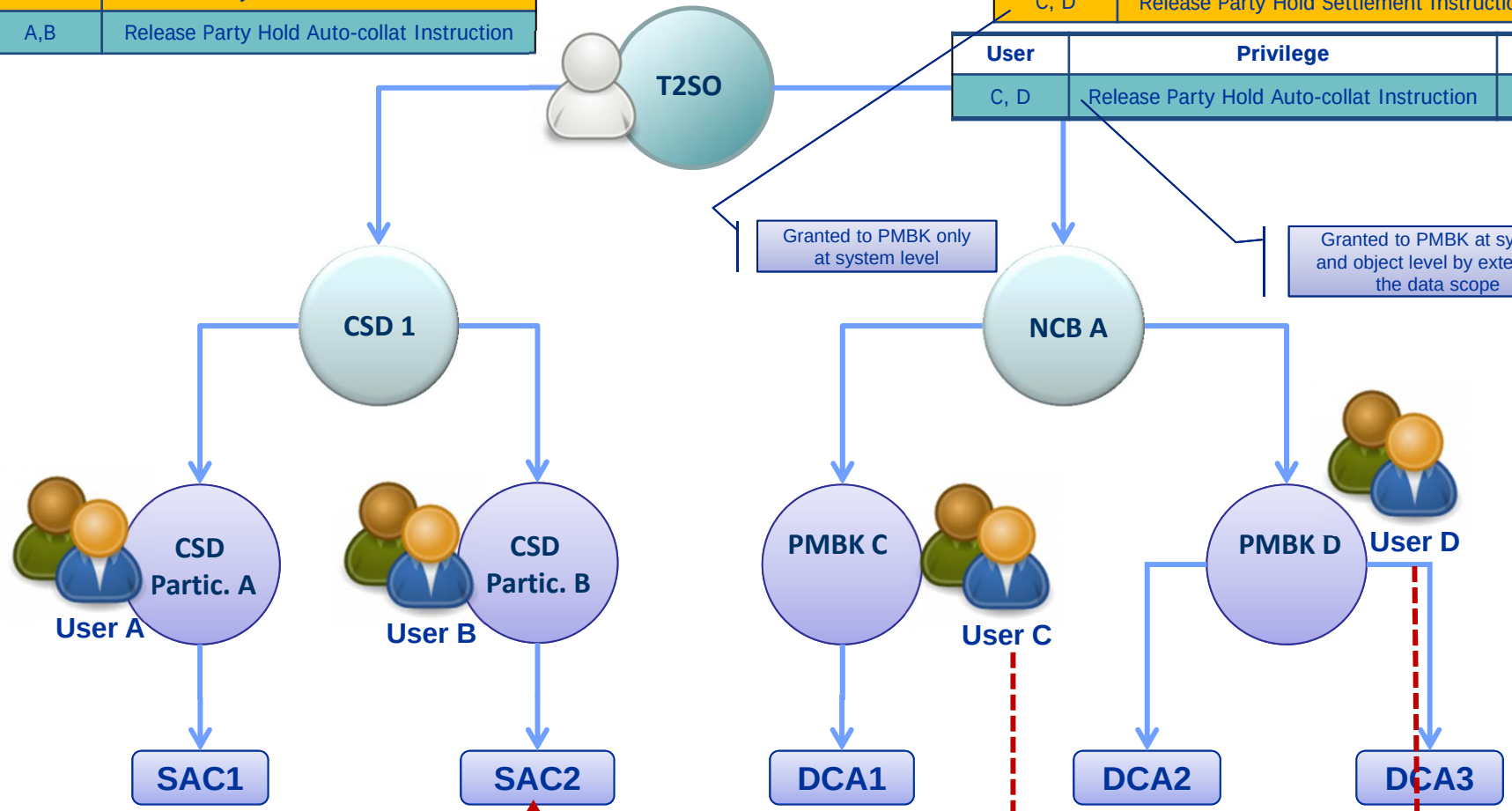
- The following slides describe the cutover process for two different scenarios.
- In **scenario I**, CSD Participant users keep using the user function related to the new privilege. Therefore the new privilege is granted to them.
- In **scenario II**, CSD Participant users cease using the user function related to the new privilege. Therefore the new privilege (if it was previously granted to them) must be revoked.
- In both scenarii, Payment Bank users receive both privileges, but with different data scope settings: one is left at default (i.e. the privilege is only granted on system level) while the other includes an object grant as well.

Scenario I: CSD also keeps the new privilege

User	System Privilege
A,B	Release Party Hold Settlement Instruction
A,B	Release Party Hold Auto-collat Instruction

User	System Privilege
C, D	Release Party Hold Settlement Instruction

User	Privilege	Object
C, D	Release Party Hold Auto-collat Instruction	SAC 2



EUROPEAN CENTRAL BANK
EUROSYSTEM

Scenario I: Privileges granted

- Privileges granted to the cash side users:
  - **Release Party Hold Settlement Instruction on a securities account.** This privilege that has been transferred from the securities side to the cash side without adding any object. As the default data scope of the PMBK/NCB has no securities accounts, this privilege will have no objects in their data scope.
  - **Release Party Hold Auto-collateralisation Instruction on a securities account**. The privilege should be granted also adding the relevant objects (i.e. the relevant securities accounts) by extending the default data scope (from empty to the granted objects) for this privilege.
  - Both privileges need to be granted from by the NCB to the PMBK as system privileges (i.e. cannot be granted directly by the CSD to the PMBK) and only afterwards the new privilege can be granted by the CSD to the PMBK as object privilege on a specific SAC.

- Privileges granted to the securities side users:
  - **Release Party Hold Settlement Instruction on a Securities account**. Even if no objects are added, given that this time the securities accounts will be part of the scope (in principle their default data scope), the privilege will contain the securities accounts of the default data scope .
  - **Release Party Hold Auto-collateralisation Instruction on a Securities account**. This time the securities accounts will be part of the scope (in principle their default data scope).

Scenario I: T2S behaviour

- If a Payment Bank user tries to release a normal settlement instruction, the message will be accepted by Interface (where “Release Party Hold Settlement Instruction” system privilege is checked) but rejected at LCMM level since the privilege “Release Party Hold Settlement Instruction” is not granted at object level for the securities account of the settlement instruction.
- If a Payment Bank user tries to release an autocollateralisation settlement instruction, the message will be accepted by Interface (where “Release Party Hold Settlement Instruction” system privilege is checked) and also at LCMM level since the privilege “Release Party Hold Auto-collat ” is granted at object level for the securities account of the settlement instruction.
- The users of the payment Banks have 2 options when instructing:
  a) Send the release instruction using as instructing party: the CSD Participant (i.e. the PBMK as client of the CSD). In this case, the user would also need the privilege “Send new instruction using a specific Instructing Party” since the user would not belong to the party indicated in the instructing party. Check performed under BR MVCP121.
  b) Send the release instruction using as instructing: party the payment bank as participant of the NCB. In this case, the user belongs to the party of the instructing party and the abovementioned privilege is not needed.
- The CSD (and its participants) will still be able to release all type of instructions, since both privileges “Release Party Hold on Settlement Instructions” and “Release Party Hold Auto-collateralisation Instructions” are granted to his users and the securities account is in their data scope.

Scenario II: Privilege shifted to PMBK

User	System Privilege
A,B	Release Party Hold Settlement Instruction
~~A,B~~	~~Release Party Hold Auto-collat Instruction~~

User	System Privilege
C, D	Release Party Hold Settlement Instruction

User	Privilege	Object
C, D	Release Party Hold Auto-collat Instruction	SAC 2

T2SO

Revoke the privilege "Release Party Hold Auto Collat Inx" to the Parties

Granted to PMBK only at system level

Granted to PMBK at system and object level by extending the data scope

CSD 1

NCB A

CSD Partic. A

User A

CSD Partic. B

User B

PMBK C

User C

PMBK D

User D

SAC1

SAC2

DCA1

DCA2

DCA3

EUROPEAN CENTRAL BANK
EUROSYSTEM

Scenario II: Privileges granted

- Privileges granted to the cash side users:
  - **Release Party Hold Settlement Instruction on a securities account**. This privilege that has been transferred from the securities side to the cash side without adding any object. As the default data scope of the PMBK/NCB has no securities accounts, this privilege will have no objects in their data scope.
  - **Release Party Hold Auto-collateralisation Instruction on a securities account**. The privilege should be granted also adding the relevant objects (i.e. the relevant securities accounts) by extending the default data scope (from empty to the granted objects) for this privilege.
  - Both privileges need to be granted from by the NCB to the PMBK as system privileges (i.e. cannot be granted directly by the CSD to the PMBK) and only afterwards the new privilege can be granted by the CSD to the PMBK as object privilege on a specific SAC.
- Privileges granted to the securities side users:
  - **Release Party Hold Settlement Instruction on a Securities account.** Even if no objects are added, given that this time the securities accounts will be part of the scope (in principle their default data scope), the privilege will contain the securities accounts of the default data scope.
  - The CSD **should revoke** the privilege "**Release Party Hold Auto-collateralisation Instruction**" to all its participants.

Scenario II: T2S behaviour

- Same behaviour for the cash side users than for scenario I.
- The CSD participants users will not be able to release Auto-collateralisation Instructions, since the privilege “Release Party Hold Auto-collateralisation Instructions” has been revoked by the CSD.

Thank you for your attention

www.t2s.eu

EUROPEAN CENTRAL BANK

EUROSYSTEM