



T2S CHANGE REQUEST FORM		
General Information (Origin of Request)		
<input type="checkbox"/> User Requirements (URD) or GUI Business Functionality Document (BFD) <input checked="" type="checkbox"/> Other User Functional or Technical Documentation (SYS)		
Request raised by: Clearstream	Institute: CSD	Date raised: 13/02/2024
Request title: Display name of secured groups in CRDM screens for access right management		Request No.: T2S 0821 SYS
Request type: Common	Classification: Scope Enhancement	Urgency: Normal
1. Legal/business importance parameter¹: Medium		2. Market implementation efforts parameter²: Low
3. Operational/Technical risk parameter³: Low		4. Financial impact parameter⁴: Low
Requestor Category: CSD		Status: Implemented

Reason for change and expected benefits/business motivation:

T2S Change Request T2S-0796-SYS was raised to introduce name and description attributes to secured groups, to allow an unambiguous identification when creating or updating a secured group.

While this Change Request enhances the identification of secured groups during creation and maintenance of secured groups, it does not tackle yet the use of secured groups in the T2S screens to assign object privileges where secured groups are among the Secured Element Types to be assigned. Namely, if secured groups are displayed in the "object privileges" lists, they are still identified by their technical identification only:

The screenshot shows the 'Object Privileges' configuration screen. At the top, there are navigation tabs: 'Access Rights Management', 'Grant/Revoke System Privileges', 'Search', '+ New', and 'Edit'. The main form includes fields for 'Privilege Category' (Security Data Queries), 'Privilege Name' (SEQ_CloseLinksQuery), 'Deny Option' (No), and 'Administration Option' (Yes). Below this is the 'Object Privileges' section with a 'Secured Element Type' dropdown menu currently set to 'Choose...'. Underneath, there are checkboxes for 'Deny Option' and 'Administration Option'. At the bottom, a table lists the configured object privileges:

Secured Element Ty...	Object/Group	Deny Option	4-Eyes Option
Party	TRGTXE2SXXX - ECBDFEFFXXX	No	No

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN.

¹ Legal/business importance parameter was set to "MEDIUM" as the change improves the usability of the system.

² Market implementation effort parameter was set to "LOW" as the change is optional.

³ Operational/technical risk parameter was set to "LOW" as the change is optional.

⁴ Low < 100kEUR < Low-Medium < 200 kEUR < Medium < 400kEUR < High < 700kEUR < Very high

This shall be adjusted:

- *In all screens where secured groups are displayed in "object privileges" lists, the name of the secured group shall be shown in addition to the technical identifier.*

This will allow an unambiguous identification of the secured groups, streamline their handling, and reduce operational risk.

Description of requested change:

In all screens where secured groups are displayed in "object privileges" lists, the name of the secured group shall be shown in addition to the technical identifier.

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the technical identification and the name of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN

The following screens are affected:

- *Grant/Revoke Cross-System Entity Object Privilege - Details Screen:* When secured groups are listed in the "object privileges" list, their "object group" attribute shall show the name of the secured group in addition to the technical identification of the secured group.
- *Grant/Revoke Cross-System Entity Object Privilege – New/Edit Screen:* When secured groups are listed in the "object privileges" list, their "object group" attribute shall show the name in addition to the technical identification of the secured group.
 - When secured groups are added/removed, it is still needed to enter the technical identification of the secured groups to identify it. However, once a secured group is added to the list in this way, its name is displayed in addition.
- *Grant/Revoke Object Privilege – Details Screen:* When secured groups are listed, their "object group" attribute shall show the name of the secured group in addition to the technical identification of the secured group.
- *Grant/Revoke Object Privilege – New/Edit Screen:* When secured groups are listed in the "object privileges" list, their "object group" attribute shall show the name in addition to the technical identification of the secured group.
 - When secured groups are added/removed, it is still needed to enter the technical identification of the secured groups to identify it. However, once a secured group is added to the list in this way, its name is displayed in addition.
- *User Access Rights – List Screen:* When secured groups are listed in the "object privileges" list, their "object group" attribute shall show the name in addition to the technical identification of the secured group. This applies to object privileges listed under "User 'System User' - Role System Privileges" and under "User 'System User' - System Privileges".

Submitted annexes / related documents:

Outcome/Decisions:

- *CRG on 3 April 2024: the CRG agreed to launch the preliminary assessment of CR-821.
- *CRG on 5 June 2024: the CRG agreed to recommend CR-0821 for authorisation by the T2S Steering Level.
- *CSG on 12 June 2024: the CSG agreed to authorise CR-0821.
- *AMI-SeCo on 20 June 2024: the AMI-SeCo agreed with the CRG recommendation of CR-0821 for T2S Steering Level Authorisation.
- *NECSG on 12 June 2024: the NECSG agreed to authorise CR-0821.
- *MIB on 19 June 2024: the MIB agreed to authorise CR-0821.
- *PMG on 8 July 2024: the PMG agreed to launch the detailed assessment of CR-0821 with a view of scoping in R2025.JUN.
- *CRG on 11 September 2024: the CRG agreed to recommend to the PMG the inclusion of CR-0821 in the scope of R2025.JUN.
- *OMG on 11 September 2024: the OMG did not identify any operational impact of the inclusion of CR-0821 in the scope of R2025.JUN.

*PMG on 12 September 2024: the PMG agreed to recommend the inclusion of CR-0821 in the scope of R2025.JUN.

*CSG on 19 September 2024: the CSG approved the implementation of CR-0821 with R2025.JUN.

*NECSG on 19 September 2024: the NECSG approved the implementation of CR-0821 with R2025.JUN.

*MIB on 26 September 2024: the MIB approved the implementation of CR-0821 with R2025.JUN.

Documentation to be updated:

2.3.3.13 Grant/Revoke Cross-System Entity Object Privilege - Details Screen

[...]

Fields [...]
Description

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN.
Deny Option	Shows whether the object privilege is explicitly denied or not.
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the object privilege or not.
Administration Option	Shows whether the party administrator of the grantee party is allowed to grant the same privilege to other parties or not. If not, the privilege can be granted only to users and roles of the same party.

2.3.3.14 Grant/Revoke Cross-System Entity Object Privilege – New/Edit Screen

[...]

Fields [...]
Description

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN.
Deny Option	Shows whether the object privilege is explicitly denied or not.
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the object privilege or not.
Administration Option	Shows whether the party administrator of the grantee party is allowed to grant the same privilege to other parties or not. If not, the privilege can be granted only to users and roles of the same party.

Add/Remove Value	
[...]	

2.3.3.15 Grant/Revoke Object Privilege - Details Screen

[...]

Fields

[...]

Description

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN.
Deny Option	Shows whether the object privilege is explicitly denied or not.
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the object privilege or not.
Administration Option	<p>If the grantee of the privilege is a user or a role, it shows whether the grantee is allowed to grant the same privilege to another user or role of the same party or not.</p> <p>If the grantee of the privilege is a party, it shows whether the party administrator of the grantee party is allowed to grant the same privilege to other parties or not. If not, the privilege can be granted only to users and roles of the same party.</p>

2.3.3.16 Grant/Revoke Object Privilege - New/Edit Screen

[...]

Fields

[...]

Description

Object Privileges	
Secured Element Type	Shows the element type of the object privilege.
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, cash account number, ISIN.
Deny Option	Shows whether the object privilege is explicitly denied or not.
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the object privilege or not.

Administration Option	<p>If the grantee of the privilege is a user or a role, it shows whether the grantee is allowed to grant the same privilege to another user or role of the same party or not.</p> <p>If the grantee of the privilege is a party, it shows whether the party administrator of the grantee party is allowed to grant the same privilege to other parties or not. If not, the privilege can be granted only to users and roles of the same party</p>
Add/Remove Value	
[...]	

2.3.3.25 User Access Rights - List Screen

[...]

Fields Description

[...]

User 'System User' – Role System Privileges - Object Privileges	
Secured Element Type	Shows the element type of the object privilege
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, T2S dedicated cash account number, ISIN.
Deny	Shows the deny option associated to the correspondent object privilege.
4-Eyes	Shows the 4-eyes option associated to the correspondent object privilege.
Administration	Shows the administration option associated to the correspondent object privilege.

User 'System User' – System Privileges	
Privilege Name	Shows the name of the privilege.
Deny	Shows the deny option associated to the correspondent system privilege.
4-Eyes	Shows the 4-eyes option associated to the correspondent system privilege.
Administration	Shows the administration option associated to the correspondent system privilege.

User 'System User' – System Privileges - Object Privileges	
Secured Element Type	Shows the element type of the object privilege
Object/Group	Shows the <u>name and</u> technical identification of the secured group or the object identification, i.e. parent BIC and BIC, security account number, T2S dedicated cash account number, ISIN.
Deny	Shows the deny option associated to the correspondent object privilege.
4-Eyes	Shows the 4-eyes option associated to the correspondent object privilege.
Administration	Shows the administration option associated to the correspondent object privilege.

Preliminary assessment:

- **Financial Impact:** Low
- **Impacted modules:** CRDM
- **Impact on other Eurosystem Services or Projects:** No impact on T2, TIPS or ECMS
- **Risk analysis:** No risks have been identified during PA
- **Findings:**

Amendment of CRDM GUI specifications in order to add the description for secured groups in the following screens:

- Grant/Revoke Cross-System Entity Object Privilege - Details Screen: "Object Privileges" list – Column "Object/Group" – (Technical ID – Description)

- Grant/Revoke Cross-System Entity Object Privilege – New/Edit Screen: “Object Privileges” list – Column “Object/Group” – (Technical ID – Description)
- Grant/Revoke Object Privilege – Details Screen: “Object Privileges” list – Column “Object/Group” – (Technical ID – Description)
- Grant/Revoke Object Privilege – New/Edit Screen: “Object Privileges list – Column “Object/Group” – (Technical ID – Description)
- *User Access Rights – List Screen*: “System Privileges - Object Privileges” List – Column “Object/Group” – (Technical ID – Description)

- **Open issues/ questions to be clarified by the originator:**

None

Detailed assessment:

EUROSYSTEM ANALYSIS – GENERAL INFORMATION			
T2S Specific Components		Common Components	
LCMM			
	Instructions validation		
	Status management		
	Instruction matching		
	Instructions maintenance		
	Penalty Mechanism		
Settlement			
	Standardisation and preparation to settlement		
	Night-time Settlement		
	Daytime Recycling and optimisation		
	Daytime Validation, provisioning & booking		
	Auto-collateralisation		
Liquidity Management			
	Outbound Information Management		
	NCB Business Procedures		
	Liquidity Operations		
T2S Interface		Eurosystem Single Market Infrastructure Gateway (from R6.0 June 2022)	
	Communication		Communication
	Outbound Processing		Outbound Processing
	Inbound Processing		Inbound Processing
Static Data Management (until June 2022)		Common Reference Data Management (from R6.0 June 2022)	
	Party data management		Party data management
	Securities data management		Securities data management
	Cash account data management		Cash account data management
	Securities account data management		Securities account data management
	Rules and parameters data management	X	Rules and parameters data management
Statistics and archive		Statistics and archive	
	Statistical information (until June 2022)		Short term statistical information
	Legal archiving (until June 2022)		Legal archiving (from R6.0)
			Data Warehouse (from R6.0)
Information (until June 2022 containing reference data)		CRDM business interface (from R6.0 June 2022)	
	Report management		Report management
	Query management		Query management
			Communication
			Outbound Processing
			Inbound Processing
Operational Services			
	Data Migration (T2S DMT)		Data Migration (CRDM DMT, from R6.0)
	Scheduling (until June 2022)		Business Day Management (from R6.0)
			Business Day Management business interface (from R6.0)
	Billing (until June 2022)		Billing (from R6.0)
			Billing business interface (from R6.0)
	Operational Monitoring		Operational and Business Monitoring
	MOP Contingency Templates		
Impact on major documentation			

Document	Chapter	Change
Impacted GFS chapter		No impact
Impacted UDFS chapter		No impact
Additional deliveries for Message Specification (UDFS, MyStandards, MOP contingency templates)		No impact
UHB	2.3.3.13 Grant/Revoke Cross-System Entity Object Privilege - Details Screen 2.3.3.14 Grant/Revoke Cross-System Entity Object Privilege – New/Edit Screen 2.3.3.15 Grant/Revoke Object Privilege - Details Screen 2.3.3.16 Grant/Revoke Object Privilege - New/Edit Screen 2.3.3.25 User Access Rights - List Screen	Insertion of the name of the secured group together with the technical identification in all the lists.
External training materials		No impact
Other impacted documentation (FA Sch. 05, FA Sch. 07)		No impact
Impacted GDPR message/ screen fields		No impact
Links with other requests		
Links	Reference	Title

OVERVIEW OF THE IMPACT OF THE REQUEST ON THE T2S SYSTEM AND ON THE PROJECT
Summary of functional, development, infrastructure and migration impacts
<p>CRDM will be amended showing the name defined for the relevant secured group together with technical identification (already foreseen) in the following screens:</p> <ul style="list-style-type: none"> • Grant/Revoke Cross-System Entity Object Privilege - Details Screen: 'Name' will be shown in the column 'Object/Group' for the already inserted groups (Example: "NAME - 123456789) • Grant/Revoke Cross-System Entity Object Privilege – New/Edit Screen: 'Name' will be shown in the column 'Object/Group' for the just inserted groups (Example: "NAME - 123456789) • Grant/Revoke Object Privilege - Details Screen: 'Name' will be shown in the column 'Object/Group' for the already inserted groups (Example: "NAME - 123456789) • Grant/Revoke Object Privilege - New/Edit Screen: 'Name' will be shown in the column 'Object/Group' for the just inserted groups (Example: "NAME - 123456789) • User Access Rights - List Screen: 'Name' will be shown in the columns 'Object/Group' for Role System Privileges - Object Privileges and System Privileges - Object Privileges (Example: "NAME - 123456789). <p>In case the name is not defined for a given Secured Group, only the technical identifier will be shown as currently foreseen (Example: "NAME - 123456789).</p>
Main Cost Drivers:
<ul style="list-style-type: none"> ■ Software changes on the affected CRDM screens [48%] ■ Specification and testing of the changes [33%]
Impact on other TARGET Services and projects
No impact on other Eurosystem Services (T2, TIPS) or projects (ECMS).
Summary of project risk
No risks have been identified during detailed assessment.
Security analysis
No adverse effects have been identified during security assessment.



05 September 2024

Cost assessment on Change Requests

T2S-821-SYS – Display name of secured groups in CRDM screens for access right management			
One-off	Assessment costs*		
	- Preliminary	2,000.00	Euro
	- Detailed	10,000.00	Euro
One-off	Development costs	41,970.92	Euro
Annual	Operational costs		
	- Maintenance costs	3,133.17	Euro
	- Running costs	0.00	Euro

*The relevant assessment costs will be charged regardless of whether the CR is implemented (Cf. T2S Framework Agreement, Schedule 7, par. 5.2.3).