General Information (Origin of Request) ☐ User Requirements (URD) ☒ Other User Functional or Technical Documentation (SYS)		
Request raised by: CBF	**Institute:** CSD	**Date raised:** 09/09/2015
Request title: Data scope reduction on party level should also reduce data scope on user level		**Request ref. no:** T2S 0554 SYS
Request type: Common	**Urgency:** Critical	
1. Legal/business importance parameter: High	**2. Market implementation efforts parameter:** Low	
3. Operational/Technical risk parameter: Low	**4. Financial impact parameter:** Medium	
Requestor Category: CSD	**Status:** Authorised at Steering Level	

Reason for change and expected benefits/business motivation:

When an object privilege is granted to a party, role or user, it normally applies on the default data scope for this privilege. E.g. for the privilege to instruct, the default data scope are all accounts owned by the party. However, T2S foresees also the possibility to reduce or extend the data scope of a party, role or user.

Data scope reductions are required, e.g., in cases where a party has special purpose accounts where the positions on those accounts are not freely available for settlement. Examples of such accounts are pledge accounts, accounts used to keep collateral received as collateral taker, or accounts to segregate instructed positions in case of voluntary corporate actions. Such special purpose accounts are normally under the control of the CSD (for custody related segregation) or a collateral management system (for pledge accounts and collateral taker accounts), and those systems would also determine whether a given position can be moved out of those accounts or not.

When configuring such accounts, the CSD would normally remove those special purpose accounts from the data scope of the party owning the account, to ensure that the positions cannot be used for other purpose. Such data scope reductions are required on party level, and also for all users of this party.

With the current setup, if the data scope of a party is reduced on party level, T2S does not reduce the data scope of the users of this party in the same way. In fact, data scope reduction on user level cannot be applied by the CSD (as level 2 entity), but only by the party administrator of the affected party (on level 3). Also, this data scope reduction must be configured for each user separately. This process is risky, error prone and cumbersome.

It is therefore required to adjust the handling of data scope reductions in T2S, so that a data scope reduction applied on party level automatically ensures that the restricted object is also removed from the data scope of each user of this party, independent from whether the object privilege was granted on privilege level or via role.

Description of requested change:

For any object privilege, T2S must ensure that the data scope of a user is always a subset of the data scope of the party of the user. In particular, when the data scope of an object privilege is reduced on party level, T2S must ensure that the restricted object is also removed from the data scope of said object privilege for all users of this party. The same must be applied in case a data scope extension is revoked on party level. Both must be the case for object privileges directly granted to the users, and also for object privileges that are contained in a role which was granted to the user.

Submitted annexes / related documents

User Testing clarification note: UT-PBR-053 (Access rights management cascade process - INC166599/INC167254)

http://www.ecb.europa.eu/paym/t2s/governance/tg/html/meetings/crg_mtg52.en.html

Proposed wording for the Change request:

Proposed wording for the UDFS:

Section 1.3.3.1.8 Data scope:

The description of data scope extension/reduction shall be enriched by adding the following paragraph:

The default data scope of each user can be extended or reduced on the basis of the actual business needs, by means of object privileges. Granting a user with a given privilege on a secured object (or on a secured group) results in extending the data scope of the user by adding the secured object (or the secured group) to the default data scope of the user. Vice versa, denying a user of a given privilege on a secured object (or on a secured group) results in reducing the data scope of the user by removing the secured object (or the secured group) from the default data scope of the user.

"The default data scope can also be extended or reduced at party level. Granting a party with a given privilege on a secured object (or on a secured group) results in extending the data scope of the party by adding the secured object (or the secured group). This allows the party administrator of the grantee party extending the data scope of the users and roles of the party by granting them with the given privilege on the same object (or secured group). Vice versa, denying a party of a given privilege on a secured object (or on a secured group) results in reducing the data scope of the party by removing the secured object (or the secured group) from the default data scope of the party. This automatically results in reducing in the same way the date scope of all the users and roles of the party."

Extending the default data scope of a user can be meaningful in several circumstances.

and the following bullet point:

- Reducing the default data scope of a user can also be meaningful. For example, a CSD Participant may decide, for specific business or organisational reasons, to grant some or all of its users with a selective access to a given sub-set of its securities accounts. This configuration can be obtained by reducing the default data scope of the relevant users, i.e. by denying them the privilege to access this sub-set of securities accounts, which would normally belong to the default data scope of these users.
-
- "A CSD may decide, for some special purpose securities accounts of one of its CSD Participants (e.g. pledge accounts, accounts used to keep collateral received as collateral taker, or accounts to segregate instructed positions in case of voluntary corporate actions), to prevent the CSD Participant instructing on these securities accounts, which normally belong to the default data scope of this CSD Participant. The CSD can setup this configuration by reducing the default data scope of the CSD Participant at party level, i.e. by denying to the party the privileges to instruct on these securities accounts."

High level description of Impact:

Outcome/Decisions:

* CRG meeting of 17-18 September 2015: The CRG agreed to put the Change Request on hold and agreed to include it in the list of Change Requests for Release 1.2. The CRG considered the Change Request critical for the migration of wave 3 participants.

* CRG teleconference of 1 October 2015: The CRG recommended to launch the detailed assessment on the Change Request.

* Advisory Group's advice on 8 October 2015: Following a written procedure, the AG was in favour of launching the detailed assessment on the Change Request.

* CSG resolution on 9 October 2015: Following a written procedure, the CSG was in favour of launching the detailed assessment on the Change Request.

* OMG on 16 October 2015: During a written procedure from 2 October 2015 to 16 October 2015, the Operations Managers Group did not identify any operational impact of the Change Request.

* CRG meeting of 15 December 2015: The CRG agreed to conclude on its final recommendation on the Change Request during the CRG teleconference of 18 December 2015.

* CRG teleconference of 18 December 2015: The CRG recommended the approval of the Change Request and its addition to Release 1.2.

* PMG meeting on 13 January 2016: During a written procedure from 30 December 2015 to 13 January 2016, the Project Managers Group was in favour of adding the Change Request to Release 1.2.

* OMG on 13 January 2016: During a written procedure from 30 December 2015 to 13 January 2016, the Operations Managers Group did not identify any operational impact. The OMG also was in favour of adding the Change Request to Release 1.2.

* Advisory Group's advice on 21 January 2016: The AG was in favour of approving the Change Request and including it in Release 1.2.

* CSD Steering Group's resolution on 22 January 2016: The CSG took the resolution to approve the Change Request and to include it in Release 1.2.

* CRG meeting of 8-9 February 2016: The CRG recommended to anticipate the Change Request and move it from the T2S Release 1.2 to the T2S Release 1.1.5. In the PMG teleconference of 12 February 2016, it was concluded that the Change Request will be anticipated with other CRs from Release 1.1.5 for EAC delivery whereas the delivery in production was remained in Release 1.2 as agreed initially.

EUROSYSTEM ANALYSIS – GENERAL INFORMATION

Impact On T2S	**Static data management**		**Interface**	
		Party data management		Communication
		Securities data management		Outbound processing
		T2S Dedicated Cash account data management		Inbound processing
		Securities account data management		
	x	Rules and parameters data management		
	Settlement		**Liquidity management**	
		Standardisation and preparation to settlement		Outbound Information Management
		Night-time Settlement		NCB Business Procedures
		Daytime Recycling and optimisation		Liquidity Operations
		Daytime Validation, provisioning & booking	**LCMM**	
		Auto-collateralisation		Instructions validation
				Status management
	Operational services			Instruction matching
		Data Migration		Instructions maintenance
		Scheduling	**Statistics, queries reports and archive**	
		Billing		Report management
		Operational monitoring		Query management
				Statistical information
				Legal archiving
		All modules (Infrastructure request)		
		No modules (infrastructure request)		
		Business operational activities		
		Technical operational activities		

Impact on major documentation		
Document	**Chapter**	**Change**
Impacted GFS chapter		
Impacted UDFS chapter	§.1.3.3.1.8 Data scope	See changes described above.
Additional deliveries for Message Specification		
UHB		
External training materials	T2S_FA_WS_1_Part_4_SD_AR_DIAPO_v00-09 T2S_FA_WS_1_Part_4_SD_AR_v00-09_Webinar	Describe the expected behaviour of the access rights check process in case object privileges are denied to parties.
Other documentations		

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
From a functional viewpoint, the T2S functionality for checking access rights shall be enhanced in a way that, when checking for object privileges, it takes into account both the data scope of the relevant system user and the data scope of its party.
Summary of project risk
No.
Security analysis
No potentially adverse effect was identified during the security assessment.

DG-MIP/MIM

ECB-PUBLIC

11 December 2015

COST ASSESSMENT ON CHANGE REQUESTS

T2S-554-SYS – Data scope reduction on party level should also reduce data scope on user level		
Project phase costs (total)	129,782.98	Euro
Running costs (annual average over cost recovery period)	9,762.07	Euro