



<b>General Information (Origin of Request)</b>	
<input type="checkbox"/> User Requirements (URD) <input checked="" type="checkbox"/> Other User Functional or Technical Documentation (SYS)	
<b>Request raised by:</b> Operations Managers Group	<b>Institute:</b> ECB
<b>Date raised:</b> 12/12/2013	
<b>Request title:</b> User Access Rights Query	<b>Request ref. no:</b> T2S 0445 SYS
<b>Request type:</b> Common	<b>Urgency:</b> Normal
<b>1. Legal/business importance parameter:</b> High	<b>2. Market implementation efforts parameter:</b> Low
<b>3. Operational/Technical risk parameter:</b> High	<b>4. Financial impact parameter:</b> Medium
<b>Requestor Category:</b> T2S Sub-group	<b>Status:</b> Authorised at Steering level

**Reason for change and expected benefits/business motivation:**

The Framework Agreement (Sch. 10 / Annex-2 Chapter 10.2.4 Review of user access rights) requires T2S Actors to check in regular intervals System users' access rights using a formal process., This aims at ensuring consistency and avoiding any possible security threat by preventing unauthorised user access, which could result in compromising or theft of information and information processing facilities.

In addition to the T2S Information Security requirements also regulatory requirements<sup>1</sup> (Principles for Financial Market Infrastructures) exist that require the execution of regular reviews of access rights associated to users.

In order to comply with these requirements a number of checks are performed:

- Reconciliation of the list of users defined in T2S against the users administration of the respective T2S Actor (excl. ICPs) The aim of such reconciliation is to identify users that should no longer have T2S access (e.g. because they left the organisation);  
Review of the list of users defined in T2S and their last login date/time. This review aims at identifying users that are inactive e.g. who have not used T2S for a certain period of time.
- Reconciliation of the adequacy of access rights associated to users. The aim of this reconciliation is to identify users that have incorrect access rights associated to them (e.g. because they changed responsibilities within their organisation)

T2S does not provide all of the information required via the GUI. Moreover, no specific reports/ queries have been foreseen to comply with the above referred requirements. The OMG participants have indicated that they would require a report/ query in order to perform the above functions for the following reasons:

- The functionalities provided by the GUI are not sufficient, as the information of the last login date/time is not provided via the GUI.  
The GUI does not provide a list of users, it displays the user details one-by-one and other screens need to be opened in order to display the profile information
- In the absence of a report / query, it is not possible to identify users that are still active in T2S; but no longer listed in the user administration of the T2S Actors (excl. ICPs) and vice versa.
- A reconciliation of T2S users, retrieving the individual users and profiles via the T2S GUI would not be operationally feasible specifically in cases where there are a high number of users.

**Description of requested change:**

<sup>1</sup> Furthermore, it should be noted that the Internal Auditors Committee (IAC) of the ECB defines common standards for the audit work in the Eurosystem/ESCB. Currently with regards to TARGET2, internal auditors require that Central Banks keep detailed records with regards to user access.

- A U2A query should be created that allows requesting a current list of all system users (U2A as well as A2A) created per Party that have access to the system at the time the query is requested.. The query, when requested, should return the following current information: when the system user has last logged on, the login name (unique identifier) of the system user, the type of roles/privileges and data access scope (e.g. accounts) the system user has been assigned, a short description of the role/privileges, Party name /organisational unit the user belongs to, a flag if the user is locked, unlocked active or deleted and optionally the date the system user was created and/or deleted.
- The query should be accessible by T2S Actors (excl. ICPs) and should return all users that have been created(including administrator users created for DCPs) or are associated to the Party running the query
- Filtering should be possible to allow to run the query for all users created by the T2S Actor running the query, a selected party, locked, unlocked, active or deleted users
- The above functionality is needed only in U2A mode, where it shall be possible to review the access rights via the GUI and to download the query results in a supported format (csv).In case of need it shall be possible for a T2S Actor to request the T2S Service Desk to run the query during support hours.
- The request to run the query and download the results must be possible at any time during the system opening hours of T2S.

**Submitted annexes / related documents:**

**Proposed wording for the Change request:**

**User Query**

- The query run via the T2S GUI shall return a current list of all system user references created per Party, the login name (unique identifier) of the system user, the date the system user last accessed T2S, the roles/privileges and data access scope (e.g. accounts) assigned to the system user, a short description of the role/privileges, the Party name/organisational unit the user belongs to, a flag if the account is active or inactive and optionally the date the system user was created and/or deleted. The query shall return the current information as of the time the query is requested
- It shall be possible to select filters and request the query online via the T2S GUI and to download the query results in a supported format (csv). The T2S Service Desk shall have access to this query and a download facility in order to produce it on behalf of T2S Actor in case of need.
- The query should be accessible by T2S Actors (excl. ICPs) and should contain all users that have been created by the respective T2S Actor running the query
- Filtering of the query should be possible to run the query for all, a selected party, locked, unlocked, active or deactivated deleted users
- Specific access rights should be created to allow the allocation of this access rights to dedicated Users/ Administrators.

UDFS:

- 1.6.4.3.3 Query Management Process

QUERY TYPE	INITIATION VIA GUI (U2A MODE)	INITIATION VIA XML MESSAGES (A2A MODE)
Intra-Position Movement Query	x	x
Access Rights Query	x	
Allegement Query	x	

- 1.6.5.7.6 Billing Data Collection Process  
The UDFS section has to be updated to include the new query as service item into table 170 "U2A Queries and Business Items" including definition of a new Business Item
- 3.3.3.31 BillingReportV01  
Update of Excel table for External codes included in section 3.3.3.31 BillingReportV01

UHB:

- The UHB documentation has to be amended in order to contain the description of the new screen search/list screen in the Screen Reference Part. Furthermore, all applicable parts of the Annexes need to be updated (6.1

Usage Indication, 6.2 Sitemap, 6.3.2 Privilege Classes for GUI Screens, 6.3.3.x Privileges for GUI Screens, 6.4.2.x References for Error Messages for GUI Screens.

---

**High level description of Impact:**

---

**Outcome/Decisions:**

- \* CRG meeting of 10 February 2014: The CRG decided to put the Change Request on hold and wait for further clarifications from the OMG.
- \* CRG Telco of 14 March 2014: The CRG decided to launch the detailed assessment on the Change Request.
- \* CRG meeting of 16 July 2014: The CRG took note that the detailed assessment on the Change Request will be ready for the CRG meeting of September 2014.
- \* CRG Telco of 24 September 2014: The CRG decided to recommend the approval of the Change Request.
- \* Advisory Group's advice on 2 October 2014: Following a written procedure, the AG was in favour of the Change Request.
- \* CSG resolution on 2 October 2014: Following a written procedure, the CSG adopted the resolution to approve the Change Request.
- \* CRG meeting of 12 March 2015: The CRG indicated that the Change Request, which was already approved by the Steering Level, is required for the Community Testing for Wave 2. The 4CB will analyse when the Change Request can be available.
- \* OMG meeting of 28-29 May 2015: The OMG did not raise any objection to the addition of the Change Request to the Release 1.1.
- \* Advisory Group meeting on 2 July 2015: The AG was in favour of adding the Change Request to Release 1.1.
- \* CSG resolution on 15 July 2015: Following a written procedure from 9 to 15 July 2015, the CSG adopted the resolution to add the Change Release 1.1.

**EUROSYSTEM ANALYSIS – GENERAL INFORMATION**

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

<b>Impact on major documentation</b>		
Impacted GFS chapter	No impact.	
Impacted UDFS chapter	Section 1.6.4.3.3 Query Management Process  Section 1.6.5.7.6 Billing Data Collection Process Table 170  Section 3.3.3.31 BillingReportV01 Annex UDFS chapter 3.3.3.31.2	New query has to be added to the table "Availability of Queries in A2A and U2A mode"  New query has to be added to the table 170 "U2A Queries and Business Items" including definition of a new Business Item Update of Excel List for External Codes in order to include new Service Items. Available under the following link: <a href="http://www.swift.com/mystandards/T2S/camt.077.001.01_T2S">http://www.swift.com/mystandards/T2S/camt.077.001.01_T2S</a>
Additional deliveries for Message Specification	Update Excel List for External Codes for camt.077	
UHB	Section 2: New 'Search/List' screen The following Annexes need to be updated: Annex: 6.1 Usage Indication Annex: 6.2 Sitemap Annex: 6.3.2 Privilege Classes for GUI Screens Annex: 6.3.3 List of Privileges for GUI Screens Annex: 6.4.2 References for Error Messages for GUI Screens (Also in T2S Operator Version:	New 'Search/List' screen needs to be described incl. the relevant Annexes.

	Section 2: New 'Search/List' screen The following Annexes need to be updated: Annex: 6.1 Usage Indication Annex: 6.2 Sitemap Annex: 6.3.2 Privilege Classes for GUI Screens Annex: 6.3.3 Privileges for GUI Screens Annex: 6.4.2 References for Error Messages for GUI Screens)	
Internal training materials	No impact.	
External training materials	No impact.	
Other documentations	Overview basic-simple queries	Add new query and categorize it as basic or complex query
<b>Links with other requests</b>		
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>The proposed solution is based on the development of a new functionality that can be accessed from the T2S GUI.</p> <p>This functionality allows the authorized user of any T2S Actor to:</p> <ul style="list-style-type: none"> <li>• trigger the data retrieval of the access rights for the system users including SOPS (Statistics and Operational Services) users of a given party</li> <li>• download the retrieved data as a file in one of the requested formats (csv) using the standard export functionalities.</li> <li>• Because of the current framework used for implementing Screens, only csv exports are supported.</li> </ul> <p>The new query has to be defined on the basis of the above mentioned search and return criteria. The solution is based on the following assumption:</p> <ul style="list-style-type: none"> <li>- In A2A mode, the concept of login time is not applicable. Consequently, the retrieved data will not include any timestamp for A2A system users. In U2A mode, the concept of login time is applicable only at the level of the certificate owner (who can be related to many system users) and not at the level of each system user. For these reasons, U2A login requests will be expanded in order to store the system user identifier and the last login timestamp of such U2A login requests. On this basis, the retrieved data will include the timestamp of the last login request performed in T2S by each U2A system user.</li> <li>- The granularity of the retrieved data will be the same as in the already available screens for granting/revoking privileges and roles, i.e.: roles and privileges assigned to system users and list of secured objects only in case of extension and/or reduction of the relevant default data scope.</li> </ul> <p>The query shall return a list of all system users including SOPS users (entries in [User] entity) regardless whether they are currently locked from T2S or whether their static data were logically deleted. It shall include for each user its last login time, if it was within the retention period. Its data scope shall not depend on the creator of the system user including SOPS users but on the Party it is associated to.</p> <p>Each authorized user can only retrieve access rights related to the system users including SOPS users linked to the party he/she belongs to. T2S Operator can retrieve access rights related to the system users of any party in T2S, upon request.</p> <p>A new Service Item will be created for the query so that it is subject to Billing.</p> <p>The new query and the respective new screen need to be integrated into the T2S GUI. Therefore the menu and the respective Sitemaps have to be updated.</p> <p>The efforts to implement the change are related to the update of the 4CB documentation (internal and external), adaptation of the T2S software and testing of the User Access Rights Query before its delivery to the users.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• It has to be noted that the queried information does not reflect any certificate related information.</li> <li>• The query will only include information stemming from standard U2A and A2A users. It will not include other application access that is neither tracked by INTF nor SOPS.</li> <li>• The information will be limited to the data availability defined on the basis of the retention period.</li> </ul>	
Summary of project risk	

Late implementation and availability of the change compared to go live date.
--

Security analysis
-------------------

No security impact (do not entail any additional costs related to the implementation of security controls).
---

T2S PROGRAMME OFFICE

ECB-PUBLIC  
15 September 2014**COST ASSESSMENT ON CHANGE REQUESTS**

<b>T2S-0445-SYS User Access Rights Query</b>		
Project phase costs (total)	143,027.87	in Euro
Running costs (annual average over cost recovery period)	12,440.09	in Euro