Common Reference Data Management for TIPS

User Handbook

V1.1.0

Author	4CB
Version	1.1.0
Date	31/08/2018

Terms and Abbreviations

The terms and abbreviations are shown in the table below. You find terms with their description and the abbreviations, both in an alphabetical order.

Letter	Description
A	
Alert icon	An *alert* icon is an icon that is shown on an active CRDM screen for those users with appropriate rights to approve a pending action.
A2A	Application-to-application
B	
BIC	Business identifier code
C	
CB	Central Bank
Check box	Square box which can be filled with a checkmark by clicking on it with the mouse. In contrast to the radio button, you can select more than one option with a check box.
D	
DD	Day (e.g. used within the timestamp, every letter stands for one digit)
d	Decimal number
E	
e.g.	For example (Latin: 'exempli gratia')
G	
GUI	Graphical user interface which is a type of user interface which allows users to interact with electronic devices.
H	
hh	Hour (e.g. used within the timestamp, every letter stands for one digit)
I	
i.e.	That is (Latin: 'id est')
IP port	Internet Protocol address port, is the port which
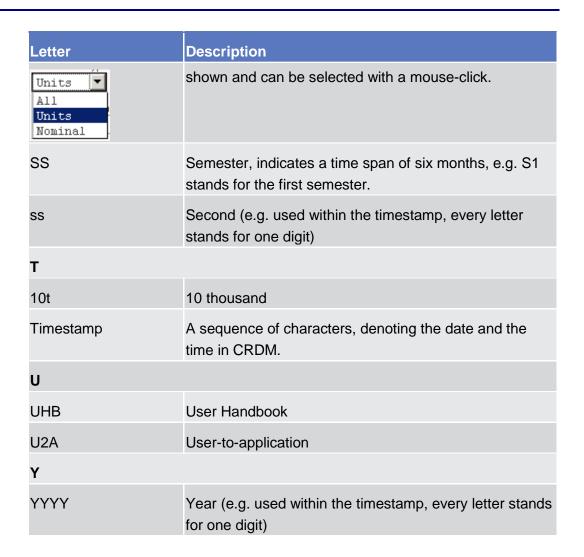
Letter	Description
	connects a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
Incl.	Including
M	
Mouse-over	Additional information for some elements of the GUI is only shown when you move the mouse-pointer to these elements.
MM	Month (e.g. used within the timestamp, every letter stands for one digit)
mm	Minute (e.g. used within the timestamp, every letter stands for one digit)
min.	Minimum
max.	Maximum
10m	10 million
N	
NRO	Non-repudiation of origin (NRO) provides the recipient (CRDM) with the evidence NRO which ensures that the originator (CRDM actor) will not be able to deny having sent the U2A instruction. The evidence of origin is generated by the originator and held by the recipient.
Q	
QQ	Quarter, indicates a time span of three months, e.g. Q2 stands for the second quarter of the year.
R	
Radio button	A type of GUI element which allows the user to choose only one of a predefined set of options.
S	
Select box	A select field in the GUI with an arrow on the right side. By clicking on the arrow, all possible input values are

Letter	Description
	shown and can be selected with a mouse-click.
SS	Semester, indicates a time span of six months, e.g. S1 stands for the first semester.
ss	Second (e.g. used within the timestamp, every letter stands for one digit)
T	
10t	10 thousand
Timestamp	A sequence of characters, denoting the date and the time in CRDM.
U	
UHB	User Handbook
U2A	User-to-application
Y	
YYYY	Year (e.g. used within the timestamp, every letter stands for one digit)

1 Introduction

1.1 Overview of the User Handbook

The CRDM User Handbook, hereinafter called UHB, aims at facilitating the use of the Graphical User Interface of the Common Reference Data Management (CRDM GUI). It is intended for any CRDM user regardless of the focus of activities and describes the full range of functionalities available in user-to-application (U2A) mode. The UHB provides detailed reference information on all GUI screens and step-by-step instructions for typical workflows.

Target Audience
There is only one handbook addressing all actors: central banks (CBs) and payment banks/settlement banks. By referring to the table of contents as well as to the usage indication list, each reader can easily identify the relevant parts.

Related Documentation
The UHB is part of the functional documentation and complements the UDFS. In particular, chapter one of the UDFS contains a detailed description of the business concepts used in CRDM, which are also relevant when using the GUI.

Updates
Updated versions of the UHB will be provided on a regular basis.

1.1.1 UHB Methodology

Several symbols and methodological elements are used throughout the CRDM UHB to ease orientation and help you to find your desired information quickly.

Page Layout
Every page of the main UHB parts has a similar page layout. You can find four different elements:

❙ the header, which shows the chapter and sub-chapter title

❙ the margin column on the left side of each page, which is used for subheadings and information signs

❙ the text column, which contains the main information, tables and screenshots

❙ the footer, which shows the name and the release of the document as well as the page number

Information Signs

Name	Icon	Description
Notice sign		Notice signs are used to highlight useful information. Read its content to find out about hints, action alternatives or other details helping you to improve your usage of the CRDM GUI.
Example sign		Example signs are used to highlight examples, which illustrate the corresponding text, especially when a verbal description is difficult or too extensive.

Links

Links are illustrated throughout the UHB with a little triangle followed by a page number within squared brackets. These links help you to jump to related sections by clicking on them or turning to the relevant page.

Illustration 1: Link illustration

Tables

Tables are used to present information in a clearly arranged format. They consist of a table head and a table body. The body is divided into a left and a right column. The left column contains keywords, for example field names, which are explained in the right column. Subsections within a table are preceded by a heading. The order of the description follows the appearance on the screen from left to right and from top to bottom.

Type Set

Regular text in the UHB is written in Arial Unicode MS font with a size of 11pt. Screen and button names are written in italic letters, GUI paths use the Courier New font. Field names and field values are put in quotation marks if they appear in a context other than their dedicated description.

Element	Format	Example
Screen name	Italic letters	*Data changes – search/list* screen
Button name	Italic letters	*New* button
GUI path	PC code	Common >> Parties >> Parties
Field name or value quotation	'...'	'Opening Date' ; 'Active'

Action Steps   Business scenarios are divided into single action steps. These action steps are numbered sequentially. Intermediate results are described where appropriate and marked with an indented arrow. Each business scenario ends with a final result, indicated by an arrow.

Example

1. Action step 1

2. Action step 2

   ➡ Intermediate result

3. Action step 3

➡ Result

Screenshots   Screenshots are used to illustrate the corresponding text. Note that there might be minor deviations between the screenshot and your screen appearance, according to your access rights or a specific selection you have made. Also, some functions are mutually exclusive and cannot be represented in a single screenshot. In these cases, the screenshot illustrates the more prevalent use of the screen.

Values shown on a screenshot might also deviate from the default values indicated in the description. In these cases, the description is valid rather than the screenshot.
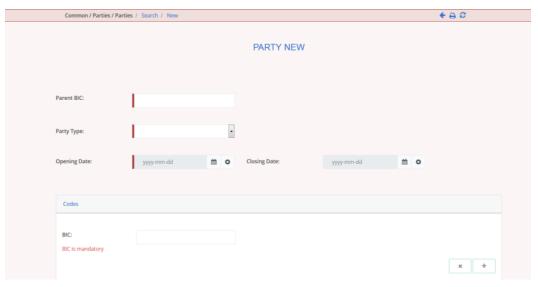
Illustration 2: Screenshot of Party New/Edit screen

1.1.2 UHB Structure

The UHB is structured in three parts and is complemented by an annex.

Part 1   The **introduction** explains the aim, the content and the approach of both the UHB and the GUI. While the first section explains how to use the UHB, the second section focuses on the design and common functionalities of the GUI.

The overview of the UHB includes information about:

❚ The UHB structure [▷ 14]

❚ The UHB methodology

The overview of the GUI consists of information about:

❚ Setup and login procedures

❚ GUI structure, including information about the menu structure, screen structure, screen types, field types and properties, and common buttons and icons

❚ Validation

❚ Communication network and services

❚ User administration

❚ Security and certification services

❚ Online help

Refer to this part if you need information on how to use the UHB or on common functionalities of the GUI.

Part 2   The **screen reference part** starts with a general section serving as a reader's guide for this part. It is followed by the screen descriptions of all screens

contained in the GUI. Each description follows an identical structure which comprises detailed information on all screen fields.

The screen reference part is structured along the first and second GUI menu level, followed by the screens in alphabetical order. Within this alphabetical order, all screen types belonging to the same business function are grouped together to follow the business logic (*search/list* screen, *details* screen, *new/edit* screen).

Refer to this part if you need detailed and precise information on a screen, field or button.

Part 3 The **user instructions part** starts with a general section serving as a reader's guide for this part. It is followed by step-by-step instructions for typical GUI workflows, called business scenarios. Each description follows an identical structure.

Related business scenarios are grouped into comprehensive business packages, which are further grouped into categories.

Refer to this part if you need to know how to carry out an action using the GUI.

Annex The **annex** supplies detailed information complementing the UHB:

▌ Annex Section 4.1 - Sitemap [▶]: Hierarchical, structured illustration of all screens and their interrelations

▌ Annex Section 4.2 - List of privileges [▶]: For each screen, all privileges and their corresponding description are listed

▌ Annex Section 4.3 - List of references for error messages [▶]: For each screen, all references for error messages, the error text and the corresponding description are listed

1.2 Overview of the Graphical User Interface

The GUI is a browser-based application for communication with CRDM in U2A mode. It is based on the ISO norm 9241 'Ergonomics of human system interaction'.

1.2.1 Setup and Login Procedures

Before entering the GUI, make sure that your workstation complies with the hardware and software requirements and implement all necessary preparations (e.g. firewall settings) described below.

Such requirements/preparations may be subject to periodical review/update to comply with changing technical/regulatory scenario.

Hardware requirements

The following hardware requirements are needed:
- Processor: 1 GHz or faster with support for PAE, NX, and SSE2;
- RAM: 1 GB (32-bit) or 2 GB (64-bit);

- Hard disk space: 16 GB (32-bit) or 20 GB (64-bit);
- Graphics card: Microsoft DirectX 9 graphics device with WDDM driver.

Software requirements

- Windows 7 OS required as OS;
- JRE Version: 1.8.0_31 or higher (remark: additional constraints coming from NSP to be verified).

Supported Web-Browsers and Settings

- The following web-browser is supported:
  ❚ Microsoft Internet Explorer (11)

- Java script and java applets are used for validations on the client side therefore 'JavaScript' and 'Cookies' have to be set to 'enabled'.
  According to current Microsoft plans, IE11 will be supported till end of October 2020 and the 4CB plan to keep it in the qualified configurations accordingly. The complete redefinition of the qualified browsers' set and the full replacement of the applet technology will be then defined in the context of the Eurosystem Singe Market Infrastructure Gateway, being part of the ongoing T2/T2S consolidation project in line with the agreed schedule.

GUI Access

- Users are directed to an initial page named ESMIG portal that ensures proper routing to the web applications (currently: "TIPS", "CRDMTIPS") the user has been granted to enter.

NRO specific requirements

- The applet installation on TIPS user side will be triggered with the first attempt to sign an instruction (and each time the user needs to sign one) and is transparent to users once the security warning asking for IBM applet installation is explicitly accepted by the user.

For security reasons, the applet (jar) archive delivered by the provider will be code signed by a trusted certification authority (Thawte) to ensure applet integrity on customer side.

In order to properly execute Thawte certificate revocation checks, customer should ensure proper Certificate Distribution List availability; these could be downloaded from the Internet at the following URLs:

- http://crl.thawte.com/ThawtePremiumServerCA.crl

- http://crl.thawte.com/ThawtePCA.crl
- http://th.symcb.com/th.crl

The TIPS users have to ensure that the security settings of their institutions, i.e. firewalls, allow for installation of the applet.

1.2.2 GUI Structure

This chapter explains the basic elements of the CRDM GUI structure (i.e. structure of the menu and the screens) helping you to navigate through the system and to use it quickly and efficiently.

The first subsection describes the menu structure where screens are grouped hierarchically. Afterwards, the second subsection explains the layout structure common to each screen. The following subsections provide details on the different screen types [▶] and on recurring elements, such as common field types [▶] or buttons and icons [▶].

1.2.2.1 Menu Structure

The GUI menu is structured into four hierarchical menu levels. The first level is presented as a menu bar which leads to the second menu level, where it is possible to choose the functionalities that are common to the shared services and those that are specific for TIPS.

Hint

Depending on your access rights, it is possible that not all menu entries are visible for you. Contact your system administrator to verify that you have the necessary privileges to access all screens relevant to you. The privileges are listed in each screen and business scenario description.

The second, third and fourth menu levels are accessible via mouse-over on the first-level menu item.
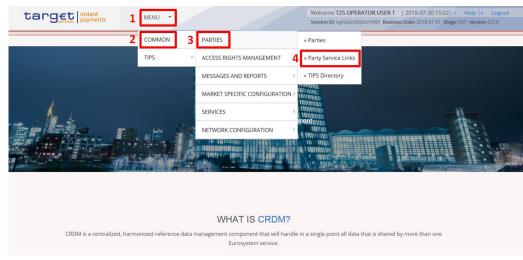
Illustration 3: CRDM menu levels

Position No.	Description
1	Menu level 1
2	Menu level 2
3	Menu level 3
4	Menu level 4

All entries on the third menu level are structural subcategories. To access a screen you have to click on the fourth menu level.

1.2.2.2 Screen Structure

In general, each screen of the CRDM GUI follows the same layout containing a header and a content area.

The header appears at the top of every screen. It contains three main elements providing useful information and helping you to navigate between the different screens as shown in the illustration below.

Header
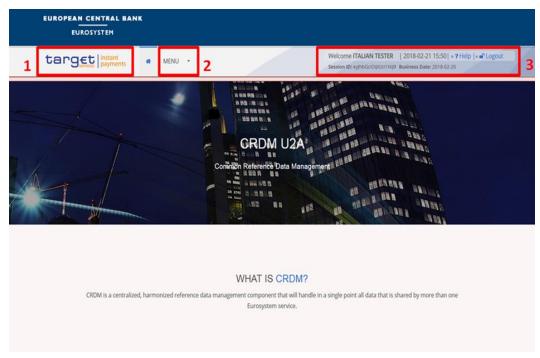
Illustration 4: Header elements

Position No.	Element	Description
1	*CRDM logo* button	... links to the welcome screen.
2	Information panel	... displays your login name, the *logout* and *help* buttons as well as date and time of last data access.
3	Menu bar	... presents the main menu item and allows you to navigate to the screens.

Content Area The content area is the part of the GUI where you can trigger all business actions. It is organised by five main elements which help you to interact properly with the GUI as shown in the illustration below.

To structure large amounts of data, the content area is further separated into frames and sub-frames.
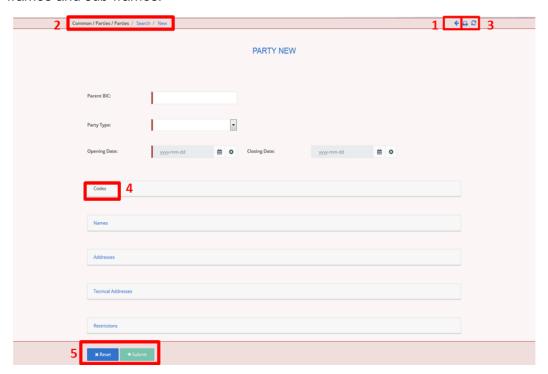
Illustration 5: Content area elements

Position No.	Element	Description
1	*Back* icon	... leads to the previous screen.
2	Breadcrumb	... shows the main path to the current screen.
3	*Print* icon	... prints the screen content.
	Refresh icon	... reloads the screen.

Position No.	Element	Description
4	Frame and sub-frame title	... groups related information as a structural function.
5	Button bar	... shows all available buttons for the current screen.

Further information about the icons can be found in the common buttons and icons section.

1.2.2.3 Screen Types

The CRDM GUI consists of the following types of screens, each with a different function:

❚ *Welcome* screen

❚ *Search/List* screen

❚ *Details* screen

❚ *Enter* screen (usually *new* or *edit* screen)

Welcome Screen

The *welcome* screen is the entrance into the CRDM GUI.

Search/List Screen

You can access all *search/list* screens on menu level four.

The *search/list* screen allows you to query the CRDM database using a predefined set of search criteria. After executing a search, a list of data records matching your search criteria is displayed in a table. To select an entry from a list displayed on a *search/list* or *list* screen, click on the desired entry. The background colour of the table line changes to indicate the selected entry. If the search retrieves only one record, the *details* screen is displayed directly, if you are authorised to access the *details* screen, else the record is displayed in the table in the *list* screen. You can browse through the list using the table buttons. Furthermore, it is possible to arrange your search results in ascending or descending order by the columns shown. This does not trigger a refreshed query.

Details Screen

In contrast to the *search/list* screen, you can only access the *details* screens via other screens.

All *details* screens provide you with in-depth information of a previously selected data record.

Before showing the *details* screen, a new query is forwarded to the system to ensure most up-to-date data.

Enter Screen   Similar to the *details* screens, you can only access the *enter* screens through other screens.

Enter screens allow you to enter data, which can be done in two enter modes:

❚ New mode, represented by the *new* screens

❚ Edit mode, represented by the *edit* screens

In general, both modes contain the same fields. In the case of the *new* mode, all fields are blank. In the case of the *edit* mode, existing data are prefilled in the fields. In addition, one past value is reported (if available) which cannot be edited. You can edit the existing currently valid value by changing the content of the field. You can only edit an existing currently valid value provided that there is no future value. Otherwise, you need to delete the existing future value beforehand. You can also enter a new future value by clicking on the *pencil* icon.

1.2.2.4 Field Types and Properties

On *search/list* and *enter* screens, you can enter information via input fields and select fields. Information is displayed in read-only fields.

Field Types

Input Fields   In input fields you can enter text and/or numeric content. Make sure to comply with the format requirements, which are part of each field/screen description.

Input-sensitive fields are input fields with an auto-complete mode that helps you to input data. As soon as you start typing the first characters of the respective data into an input-sensitive field, CRDM automatically proposes possible matching entries from which you can select the desired one.

Illustration 6: Input-sensitive field

🛈   **Hint**

You can use the tab key on your keyboard to navigate through the GUI fields.

BIC8 that are entered via GUI are automatically supplemented to BIC11 by adding 'XXX' in order to unambiguously identify a party.

Select Fields   Select fields are either select boxes, radio buttons or check boxes.

▌ **Select boxes**: Functionally a select box is a way to enter data from a limited list of possible values. In CRDM you can find different types of select boxes, standard select box and auto-complete select box.

▌ **The standard select box** enables you to choose one entry from a predefined set of values. To select an entry, click on the little box with the arrow to open the menu. Then select the desired value by clicking on it.
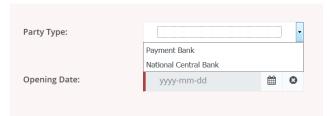
Illustration 7: Standard select box

The **auto-complete select box** enables you to either enter your desired value manually which will be used to reduce the possible set of values in the auto-complete select box to be chosen from or to click on the *auto-complete select box* icon, which provides you with a drop-down menu that shows the 10 first entries of the set of values irrespective of what you might have entered in the text field. In either way (meaning clicking on the icon or start typing an entry with the automatically shown list) up to 10 entries will be shown in the drop-down menu.
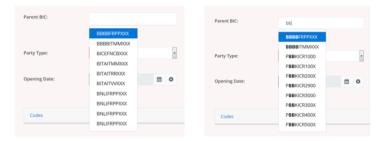
Illustration 8: Auto-complete select box using the *auto-complete select box* icon and auto-complete select box with manually entered values

The **google-style select box** enables you, differently from the auto-complete select box, to make entries and choose values outside the standard set of values to be sent to the back-end for further validation (extended data scope). Due to that possibility of transporting unqualified data the validation of the values is restricted to basic checks and will be carried out mainly in the backend. Apart from that, the google-style select box functions similar to the auto-complete select box.
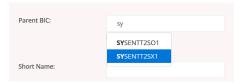
Illustration 9: Google-style select box

Radio buttons: Enable you to make exact selections using one value from a set of options. You can select only one value at the same time. Click on the icon corresponding to the option you would like to select.
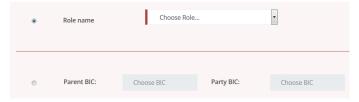
Illustration 10: Radio buttons

Check boxes: Enable you to select more than one value at the same time. Click on the boxes corresponding to the options you would like to select. Selected check boxes contain a check mark.

Illustration 11: Check boxes

Wildcards   A wildcard is a placeholder for characters and it represents any acceptable character or a set of them in a string. In CRDM you can use a wildcard in input fields or google-style fields in all the search screens to search for data widening the result to all the strings matching the pattern. The required number of characters is indicated in the field description. CRDM accepts two possible values:

‘*’ that is a placeholder for one or more characters of the input value;

‘?’ that is a placeholder for exactly one character of the input value.

Examples

CRDM*: The result list contains all data records beginning with 'CRDM'.

*Account: The result list contains all data records ending with 'Account'.

CRD?: The result list contains all data records that have any acceptable character at the end of 'CRD', e.g. 'CRDM', 'CRDX', etc.

The combination of the wildcard '*' is not possible, e.g 'CRD?*' or 'CR**'

The wildcards are always usable in the fields reported before with the following restrictions:

It is possible that to properly search with wildcards you have to insert at least two or four characters. In this case, the minimum number of characters to be entered is reported in the field remarks;

▌ It is possible that a field does not allow wildcards; in this case, this is explicitly mentioned in the Remarks field.

Read-only Fields

In addition to enter and select fields, the CRDM GUI has also read-only fields, which are pre-filled and do not allow data changes.

Field Properties

All field types have specific properties with respect to possible character sets, and mandatory content.

Characters

CRDM operates in British English and uses the SWIFT-x character set to enter data. CRDM uses the UTF-8 character set with the exception of '<', '>' and '&'. Amounts are automatically displayed with decimal points. While negative amounts are displayed in red and marked with a '-', you can only type amounts that are greater than or equal to 0 into input fields.

The GUI does not differentiate between upper and lower case in terms of data input for input fields.

The SWIFT-x character set corresponds with the following content:

Character	Description
a - z	26 small characters of the Latin alphabet
A - Z	26 capital characters of the Latin alphabet
0 - 9	10 numeric characters
/	Solidus (slash)
-	Hyphen
?	Question mark
:	Colon
(	Opening parenthesis
)	Closing parenthesis
.	Full stop
,	Comma
´	Apostrophe
+	Plus
	Space (blank)
CR	Carriage return
LF	Line feed

Hint

CRDM does not process fields (mandatory or optional), that are only filled with blanks. Blanks appearing at the beginning or at the end of a field entry are deleted automatically without any notification. Fields in a *list* or *details* screen, where the dataset was saved without an entry, are filled with '---'.

Mandatory Content

In the GUI all mandatory fields are marked with a red line in the label. All marked fields have to be filled in before you are allowed to proceed.
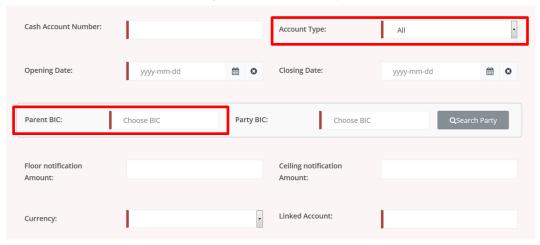
Illustration 12: Mandatory fields

Position No.	Description
1	Mandatory select field
2	Mandatory input field

1.2.2.5 Common Buttons and Icons

While working with the CRDM GUI you will find that some buttons and icons appear regularly. There are three types of common elements:

❙ Basic icons, which you can find on every screen

❙ Utility elements, which represent functions within the content area

❙ Table elements, which you can find below data record lists on *search/list*

The buttons contained in the button bar are variable and therefore explained in the screen descriptions.

Basic Icons

Illustration 13: Basic buttons

Position No.	Element	Description
1	*Back*	... always leads to the previous functional screen. The usage of the *back* icon does not lead to an update or a refresh of the query of the screen. Do not use the *back* button of your web-browser to return to the previous screen, to avoid data loss. The *back* icon is common to all CRDM screens except for the *welcome* and *search* screens. When using the *back* button to go back to screens which include search parameters, the last values input during the same session are retained.
2	Export icon	... exports the data of the executed query from the current screen into a csv-file. If exporting a list, the related search criteria are exported as well whereas detailed data are only exported, if the respective list and the details screen are covered by the same query. Otherwise just the list entry will be exported. The export icon is common to all CRDM screens except for the welcome and the new screens. In addition to the exported data from the screen the following information is exported at the start of the file: name of the exported screen (including menu path), current date, name of the user who triggered the exporting, classification label 'RESTRICTED', timestamp of the export, defined search criteria (query parameters, if applicable), 'CHANGED DATA' when exporting an edit screen which contains amended data that has not been submitted yet.
3	Print icon	... prints the data of the current screen. It is strongly recommended to use this button for generating a clearly arranged overview of data on the printout. The print icon is common to all CRDM screens except for the welcome screen.
4	*Refresh* icon	... reloads the screen. In new and edit modes the screen is locked, so it is not possible to refresh.

Position No.	Element	Description
		The refresh function takes into account the search criteria that were chosen the last time the *search* button was clicked. Those search criteria will be displayed again. Changes that have not yet been saved are lost after using the *refresh* icon. The *refresh* icon is common to all CRDM screens except for the *welcome* screen.

Utility Elements
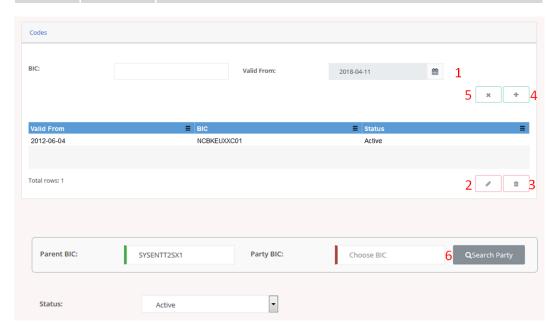
Illustration 14: Utility elements

Position No.	Element	Description
1	*Calendar* icon	... opens a calendar where you can select a day. If applicable, you can also select the time via the *calendar* icon.
2	*Pencil* icon	... enables you to enter a new future value into an input field. In edit mode, you can either change an existing data record or enter a new future one. If you have changed the existing current value before entering a future one, the data are restored. The *pencil* icon is only available on *edit* screens.
3	*Delete row*	... removes the selected row in the corresponding list as

Position No.	Element	Description
	icon	well as fields or sub-frames. The *delete row* icon is only available on *new* and *edit* screens.
4	*Submit changes* icon	... updates the selected row in the corresponding list using the values inserted in the related fields. The *submit changes* icon is only available on *new* and *edit* screens.
5	*Cancel changes* icon	... enables you to leave the selected and edited row without causing any changes. The *cancel changes* icon is only available on *new* and *edit* screens.
6	*Magnifier* icon	... provides the possibility to search for data on other screens. If you are not aware of the exact/correct value, but you know other related data, click on the *magnifier* icon to enter the *search* screen. There you can enter all information known to you and execute a search. By clicking on the *select* button, you are redirected to the initial screen with the desired data entered in the respective fields. The attribute equipped with magnifier icon works otherwise like an auto-complete select box.

Table Elements
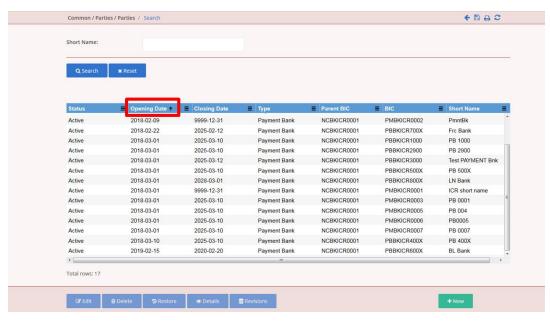
Illustration 15: Table element – Sort icon
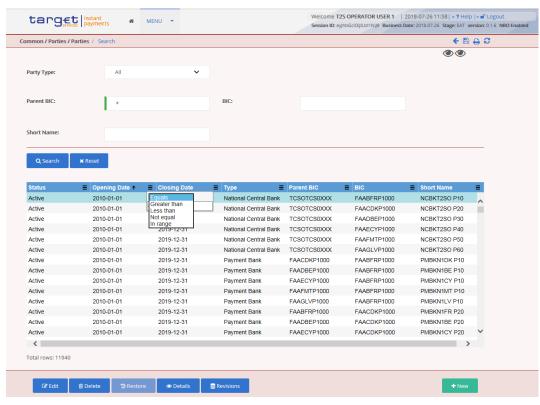
Illustration 16: Table element - Supplementary filters in list objects

Position No.	Element	Description
1	*Sort* icon	... sorts the list in ascending or descending order by clicking on the up or down arrow.
2	*Supplementary filter*	… allows in-memory filtering, depending on the type of fields, of the displayed list of items according to additional criteria as shown below.
		Data fields supplementary filter criteria: ▌ Equals ▌ Greater than ▌ Less than ▌ Not equal ▌ In range
		Text fields supplementary filter criteria: ▌ Equals ▌ Not equal ▌ Starts with ▌ Ends with ▌ Contains ▌ Not contains
		Predefined supplementary filter criteria: It contains an adaptive list of values which is consistent with the related search criterion. E.g. for any Status field, the predefined supplementary filter contains the following values: 'All', 'Active', 'Deleted'.
		When a supplementary filter criterion is used, the list is automatically filtered in memory without submitting the query to the back-end. When applied, any supplementary filter can be removed by individually resetting the corresponding filter.
		If a supplementary filter is applied, a small icon near the column header is displayed, as shown in the

Position No.	Element	Description
		following image.

Status ▼
Active

1.2.3 Validation

In CRDM, all submission processes undergo various validations, which take place in the front-end and/or in the back-end. Only correct entries, fulfilling all predefined criteria, can be further processed. To indicate the status of the recently performed action, CRDM uses two different types of messages to indicate a successful or failed validation as described below.

In addition to the automatic validation carried out by CRDM, human validation can be imposed by using the 4-eyes mode.

Furthermore, non-repudiation of origin (NRO) is implemented for a specified number of screens.

Front-End Validation

As first part of the validation process, the front-end validation takes place without communication to the back-end. The front-end validation includes both the field validation and the cross-field validation. It is carried out after clicking on a button.

The field validation verifies that all entries comply with the required format.

The cross-field validation checks the data consistency between two or more fields/buttons in relation to each other.

Back-End Validation

The back-end validation is the second part of the validation process. After successful front-end validation, your request is submitted to the back-end and checked for compliance with the business validation rules. In case of failure an error message is displayed. You can find a detailed list of all error messages and their description in the annex of the UHB (list of references for error messages [▶]).

Result

After each validation, the CRDM GUI informs you about the result. There are two different message types available, the **error message** and the **success message.**

Error Message

Each error message appears as a pop-up on the upper right corner of the screen. In the case of a failed front-end or back-end validation, it indicates the source of the failure, the type of error and a short hint.
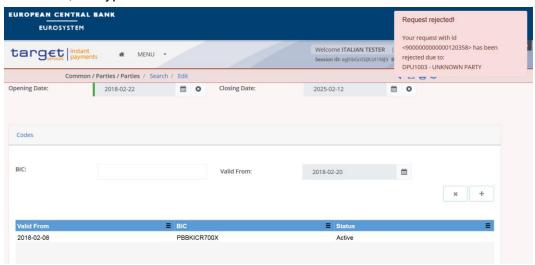
Illustration 167: Error message

Success Message

The success message appears as a pop-up on the upper right corner of the screen. It confirms that your data have been submitted successfully.

If you are working in 4-eyes mode, the success message also provides you with the 4-eyes principle ID.

Illustration 18: Success message

4-Eyes Mode   Depending on the access rights setup, you can use CRDM in 2-eyes or in 4-eyes mode. The 2-eyes mode and the 4-eyes mode apply for *enter* screens (new and edit mode) and for any kind of deletion processes. If you are a 4-eyes mode user, your actions have to be confirmed by a second user in order to be processed.

First User

In 4-eyes mode the first user enters, changes or deletes the data on a screen and afterwards submits the action by clicking on the *submit* button in the button bar. The success message appearing after successful validation includes a 4-eyes principle ID. For the final execution a second user is needed to confirm the action.

Second User

After the first user has entered, changed or deleted the data, a second user (with the required privilege) has to approve or revoke this action via the *data changes* screen [▶] either using the 4-eyes mode ID or the search functionality.

As soon as the data changes are positively approved, CRDM marks these data as approved and they are forwarded to further processing.

Digital Signature – NRO

In order to ensure non-repudiation of origin (NRO) for critical transactions, the use of a digital signature has been implemented for specified screens. This means that the user will be asked to enter a PIN code for signature purposes whenever an instruction is initiated. With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor.
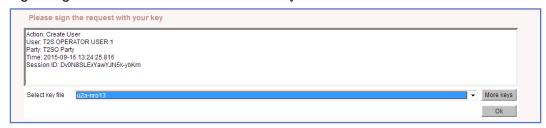
Illustration 19: Digital signature

1.2.4 Communication Network and Services

Refer to the TIPS Connectivity Guide document for details on the communication network and services.

1.2.5 User Administration

Registration

Only registered users have access to the CRDM GUI, therefore registration in CRDM reference data and to the network is necessary prior to the first GUI access. The Registration Guide provides information on how to fill in Registration Forms properly.

After registration the system administrator is given the possibility to grant and revoke privileges to its users within the CRDM GUI as described in both the screen reference part and the user instructions part.

1.2.6 Security and Certification Services

In order to guarantee a secure and safe handling of the information and to protect customer data provided via the GUI, various security elements have been put into place:

❙ Each action requires System or human validation as described in the validation [▶]

❙ The scope of available data and functions is controlled via the management of access rights

❙ The security features provided by the network providers and described in their respective user documentation prevent unauthorised access

1.2.7 Online Help

The content of the UHB can be accessed from the CRDM GUI by clicking on the *help* button. The online help is context sensitive, which means that the screen description corresponding to the current screen is displayed. Other parts of the online help can be reached using the table of contents on the left side of the help window.

2 Screen Reference Part

2.1 General

The screen reference part offers a complete overview of all CRDM GUI screens that are available in U2A mode. Each screen description focuses on a single screen and explains all fields contained therein. An exception is made for the *new* and *edit* screens, which are largely similar and therefore included in a single screen description. The description is always based on and contains only the screenshot of the *edit* screen, but describes deviations for the *new* screen in a separate row for each field or button description.
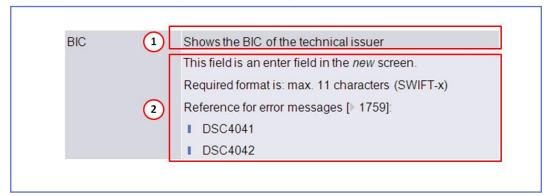
Illustration 17: Example of a *new* and *edit* screen description

Position No.	Element
1	Description relevant for *edit* mode.
2	Description relevant for *new* mode.

In detail, every screen description has the same structure and contains the following elements.

Context of Usage
The context of usage explains what a screen displays, what you can do with the screen and which special features are available for the screen, for example the need for confirmation in 4-eyes mode or usage restrictions. If the export functionality produces more data than shown on the screen (if a *list* screen is based on a detailed query), this is also indicated in the context of usage.

Screen Access
The screen access lists all possible ways to access the screen. This includes navigation via the menu and navigation via other screens.

Examples

Navigation via the menu:

TIPS >> Cash Accounts >> Cash Account >> *cash accounts – search/list* screen

Navigation via other screens:

Common >> Parties >> Parties >> *Technical Address Network Service Link* >> Click on the *new* or *edit* button

When navigating via a *search/list* or *list* screens, a data record has to be selected by clicking on a table row. Afterwards, you can click on specific buttons in the button bar, e.g. the *edit* or *details* button.

Privileges   The privileges segment lists all necessary privileges to access the screens and to use its functions. First, the privileges to access a screen are mentioned, followed by the privileges that are necessary to use all functions on the screen. For further information, refer to the list of privileges [▶To be provided in a later draft, under the Annex chapter].

Reference   The reference lists all business scenarios containing the respective screen (reference to the user instructions part).

Screenshot   You can use the screenshot as orientation for your work with the UHB. All screenshots are based on the maximum of access rights, so deviations are possible if you do not own all privileges which are necessary to use the screen in its full extent. In addition, deviations between the screenshot and the field/button description are possible in the case of mutually exclusive functions and based on a specific selection you have made. Values shown on the screenshot might also deviate from the default values indicated in the description.

In the case of the *new/edit* screen description, the screenshot of the *edit* screen is used. Differences appearing in the *new* screen are explained in the field description.

Field Description   The field description provides all the relevant information related to the respective field name. It is structured in table format with a separate table for each frame. Sub-frames are indicated by subsection headings in the table. The following illustration explains the structure of a field description.

Party
Party

Opening Date*	Enter the date from which the party is open or use the *calendar* icon.
	Required format is: YYYY-MM-DD
	References for error messages [▶To be provided in a later draft, under the Annex chapter]:
	▮ DPC1205
	▮ DPU1206
	▮ DPU1208
	The opening date must be equal to or later than the current date.
	If the current date is later than the opening date, this field is read-only.

Illustration 181: Example of a screen description

Position No.	Element	Description
1	Field name	... indicates the respective name of each screen field.
		Mandatory fields are marked with an asterisk after the field name. In the case of the *new/edit* screen description, the mandatory field is marked with an asterisk in brackets, which indicates that the respective field is either mandatory in the edit or in the new mode. Input and select fields without an asterisk are always optional.
2	Frame name	... indicates the respective name of each screen frame.
3	Sub-frame name	... indicates the respective name of each screen sub-frame.

4	Field description	... indicates the field type and required content. Each field description starts with a keyword, which illustrates your required activity: ▌ 'Shows...' indicates a read-only field [▶] ▌ 'Select...' indicates a select field [▶] ▌ 'Enter...' indicates an input field [▶] If there is an exhaustive list of possible values, these are listed.
5	Required/Displayed format	... indicates all field format requirements related to the fields. If there is more than 1 format requirement, they are separated with a comma. In read-only fields the displayed format is only mentioned, if the field content is ambiguous. This applies especially to date fields. The following keywords are used for the format requirements: ▌ 'Digit' indicates numbers ▌ 'Character' indicates a character from the SWIFT-x character set [▶] ▌ 'Letter' indicates upper and lower case letters of the Latin alphabet

6	Cross-field validations	... indicate interdependencies between fields relevant for the validation of your input. For further details on the validation process, refer to validation [▸].
7	References for error messages	... indicates the code of all possible errors applying to the field during the back-end validation. The corresponding error text and error description is listed in the annex (list of references for error messages [▸To be provided in a later draft, under the Annex chapter]). For further details on the validation process, refer to validation [▸31].
8	Additional information	... indicates the useful information that is for filling in the field.

Buttons   All buttons specific to the screen are listed and described in a table at the end of the screen description. The following illustration explains the structure of a button description.
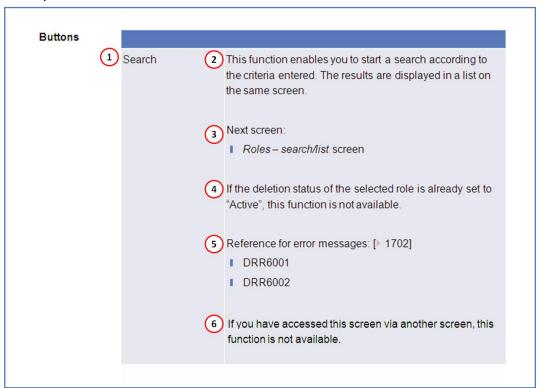
Illustration 192: Example of a button description

Position No.	Element	Description
1	Button name	... indicates the respective name of each button.
2	Button description	... indicates the action that is triggered when clicking on the button. Each button description starts with 'This function enables you...'
3	Next screen	... element lists the screen which is displayed after clicking on a button. If there are various possible next screens depending on your previous actions, all of them are listed.
4	Cross-field validations	... indicate interdependencies between a field and the button relevant for the validation of your input. For further details on the validation process, refer to validation [ ].
5	References for error messages	... indicates the code of all possible errors applying to the button during the back-end validation. The corresponding error text and error description is listed in the annex (list of references for error messages [ ]). For further details on the validation process, refer to validation [ ].
6	Additional information	... indicates useful information regarding the button and/or its function.

For further information on common buttons, refer to Common Buttons and Icons.

2.2 Services

2.2.1 Additional Services

2.2.1.1 Data Changes – Search/List Screen

This screen contains a number of search fields. By inputting the relevant data, you can search for all reference data changes which were initiated in 4-eyes

Context of Usage	mode. You can use this screen to search for items which are waiting for approval, select those and approve or revoke them.
	The search results will be displayed in a list, which is sorted by the values of the column 'Update Date and Time' in descending order (default setting). After selecting an entry, you can proceed further by clicking on the buttons below.
Screen Access	▌ Common >> Services >> Data Changes
Privileges	To use this screen, you need the following privilege [▶]:
	▌ Queued Data Changes Query
References	**User Instructions Part**
	This screen is part of the following business scenarios:
	▌ Initiate an action in 4-eyes mode [▶]
	▌ Approve an action in 4-eyes mode [▶]
Screenshot	
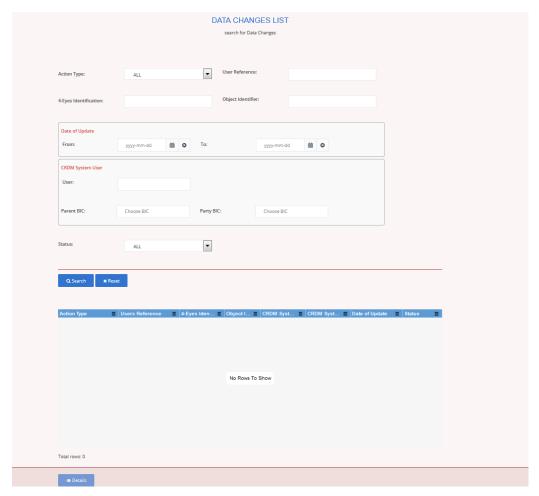
Illustration 23: Data changes – search/list screen

Field Description

Data Changes - Search Criteria	
Action type	Select the type of action initiated by the first user for a dedicated reference data object from the possible values: ❙ All ❙ Each of the actions that can be done in 4-eyes-mode
Users reference	Enter the identification the first user added to his request. Required format is: max. 35 characters (SWIFT-x)
4-Eyes Identification	Enter the identification of the data change, automatically assigned by CRDM to an operation that has to be authorised by a second user. Required format is: max. 35 characters (SWIFT-x)
Object Identifier	Enter the object identifier of the added / changed / deleted object. It is the technical identifier of an object unless a business identifier is available for this object. Required format is: max. 35 characters (SWIFT-x)
From	Enter the lower bound of the date from which the data change was requested. Required format is: YYYY-MM-DD The default value is the current calendar date.
To	Enter the upper bound of the date until which the data change was requested. Required format is: YYYY-MM-DD The default value is the current calendar date.
User	Enter the name of the last user who entered, edited or deleted the reference data.

Party BIC	Enter the BIC of the party which the last user belongs to. Required format is: max. 11 characters (SWIFT-x) If the 'Parent BIC' field is filled in, this field is mandatory.
Parent BIC	Enter the parent BIC of the party which the last user belongs to. Required format is: max. 11 characters (SWIFT-x) If the 'Party BIC' field is filled in, this field is mandatory.
Status	Select the processing status of the data change from the possible values: ❚ All (Default value) ❚ Awaiting approval ❚ Queued ❚ Approved ❚ Rejected ❚ Revoked

Data Changes - List	
Action type	Shows the type of action, from all the actions that can be done in 4-eyes-mode, initiated by the first user for a dedicated reference data object.
Users Reference	Shows the identification by the first user added to his request.
4-Eyes Identification	Shows the identification of the change automatically assigned by CRDM to an operation that has to be authorised by a second user.
Object Identifier	Shows the object identification returned by the subsequent module after successful business validation. This information will not be displayed for all records.

Data Changes - List	
CRDM System User	Shows the name of the last user who entered, edited or deleted the static or dynamic data.
CRDM System Users Party	Shows the BIC of the party which the last user belongs to.
Date of Update	Shows the timestamp when the first user entered, edited or deleted the static or dynamic data. Displayed format is: YYYY-MM-DD hh:mm:ss
Status	Shows the status of the data change from the possible values: ❚ Awaiting approval ❚ Queued ❚ Approved ❚ Rejected ❚ Revoked

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. If the search retrieves only one record, the *details* screen is displayed directly. Next screens: ❚ *Data changes – search/list* screen ❚ *Data change – details* screen [▸]
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Data changes – search/list* screen
Details	This function enables you to display the details of the selected data change. Next screen: ❚ *Data change – details* screen [▸]

2.2.1.2 Data Change – Details Screen

Context of Usage

This screen displays detailed information on the selected reference data changes, changes are highlighted in red. You can check the data and proceed

further by clicking on the buttons below. You can use this screen for approving/revoking reference data changes and to see details of already approved/revoked items.

Screen Access

❚ Common >> Services >> Data Changes >> *search/list* screen >> Click on the *search* and/or *details* button

Privileges

To use this screen, you need the following privilege [▶]:

❚ Data Changes of a Business Object Details Query

References

User Instructions Part

This screen is part of the following business scenarios:

❚ Initiate an action in 4-eyes mode [▶]

❚ Approve an action in 4-eyes mode [▶]

Screenshot

Details of selected data change

| Action Type: | User - Update | 4-eyes Identification: | 9500000000000034009 | Object Identifier: | 9874 |

CRDM System User - First User

| User: | crdmUserTester5 | Party BIC: | PPBKIRC2800 | Parent BIC: | NCBKICR0001 |

CRDM System User - Second User

| User: | crdmUserTester4 | Party BIC: | PPBKIRC2300 | Parent BIC: | NCBKICR0001 |

| Date and Time: | 2018-02-01 14:25:31 | Status: | Approved |

Details of selected data change

Status:	Active	Login Name:	Mario.Rossi	Name:	Mario Rossi
System User Reference:	MarioRossi	Lockout from:		Lockout:	No
Parent BIC:	NCBKICR0001	Party BIC:	PBBKICR6800	Party Type:	Payment Bank
Party Short Name:	PB6800				

List of Modification

| Field Name: | Login Name | Old Value: | JBEK57FNJ | New Value: | Mario.Rossi |

[Approve] [Revoke] [Cancel]

Illustration 24: Data changes – details screen

Field Description

Selected Data Changes	
Action type	Shows the type of action initiated by the first user.
4-Eyes Identification	Shows the identification assigned by CRDM to an operation that has to be approved by a second user.
Object Identifier	Shows the object identification of the reference data object returned by the subsequent module after a successful business validation. The object identifier includes the technical identification of the added, changed or deleted object.
Date and Time	Shows the timestamp when the user has entered the data. Displayed format is: YYYY-MM-DD hh:mm:ss
System User – First User	

Selected Data Changes	
User	Shows the name of the first user who entered, edited or deleted the reference data.
User Party BIC	Shows the BIC of the party which the first user belongs to.
Parent BIC	Shows the parent BIC of the party which the first user belongs to.
System User – Second User	
User	Shows the name of the second user who entered, edited or deleted the static or dynamic data.
User Party BIC	Shows the BIC of the party which the second user belongs to.
Parent BIC	Shows the parent BIC of the party which the second user belongs to.
Status	Shows the processing status of the data change from the possible values:
	▌ Awaiting approval
	▌ Queued
	▌ Approved
	▌ Rejected
Details of selected Data Change	
The whole pane consists of the respective screen of the object that is subject to the 4-eyes-action.	
	• *If the action type is "Delete Data", then the currently active data should be presented in this screen.*
	• *If the action type is "Edit Data", then the new values of the fields (which are pending at that moment and which should be approved) should be presented.*
If the action type is "New Data", then the new values of the fields should be presented.	
List of Modification	
Field Name	Shows the name of the field where the first user has changed data, entered new data or deleted data.
	The following field should only be presented to the user if the action type is "Edit Data".

Selected Data Changes	
Old Value	Shows the old value which is the currently active before the second user approves the changes.
	The following field should only be presented to the user if the action type is "Edit Data".
New Value	Shows the pending value of the field which will be active after the second user approved the changes.
	The following field should only be presented to the user if the action type is "Edit Data".
New Value	Shows the pending value of the field which will be active after the second user approved the changes.
	The following field should only be presented to the user if the action type is "Edit Data".

Buttons

Approve	This function enables you to approve the action initiated by the first user. In case non-repudiation of origin is required: Upon clicking on the approve button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the actor. Next screen: ❚ *Data changes – search/list* screen [▶] This function is only available if the processing status of the data change is set to 'Awaiting Approval' and the system user has the necessary privileges.
Revoke	This function enables you to revoke the action initiated by the first user. In case non-repudiation of origin is required: Upon clicking on the revoke button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the actor. Next screen: ❚ *Data changes – search/list* screen [ ] This function is only available if the processing status of the data change is set to 'Awaiting Approval' and the system user has the necessary privileges.
Copy	This function enables you to copy fields to create a new data change with the same attributes. Next screen: ❚ *Respective new/edit* screen (filled with the values formerly entered by the first user.) This function is only available if the processing status of the data change is set to 'Revoked'.

Cancel	This function enables you to cancel the process and return to the previous screen. Next screen:
	❙ *Data changes – search/list* screen [ ]

2.3 Reference Data

2.3.1 Parties

2.3.1.1 Parties – Search/List Screen

Context of Usage This screen contains a number of search fields. By inputting the relevant data, you can search for parties. The search results will be displayed in a list, which is sorted by the values of the 'Short Name' column in ascending order (default setting). After selecting an entry, you can proceed further by clicking on the buttons below.

Party reference data can only be created and edited by users belonging to the responsible CB or by the Service operator (for 'NCB' party type). Party reference data can only be viewed by users belonging to the responsible CB or to the party itself, while the Service operator can view all party data.

Screen Access ❙ Common >> Parties >> Parties

Privileges To use this screen, you need the following privileges [▶]:

❙ Party list query

❙ Delete party

References **User Instructions Part**

This screen is part of the following business scenarios:

❙ Add a new technical address to a party [▶]

❙ Create a new participant [▶]

❙ Edit an existing participant [▶]

❙ Delete an existing participant [▶]

❙ Create a new technical address service link [▶]

Screenshot
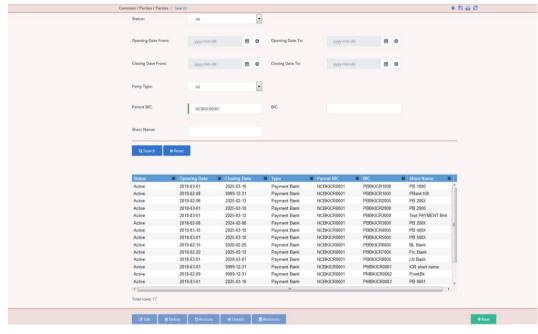
Illustration 25: Parties – search/list screen

Field Description

Party – Search Criteria	
Status	Select the status of the party from the possible values:
	▮ All
	▮ Active (default value)
	▮ Deleted
	References for error messages [▶]:
	▮ DPD1003
	▮ DPD1004
Opening Date – From	Enter the lower bound of the date from which the party is open or use the *calendar* icon.
	Required format is: YYYY-MM-DD
	The lower bound of the opening date must be earlier than or equal to the upper bound.
	References for error messages [ ]:
	▮ DPD1003
	▮ DPD1004
Opening Date – To	Enter the upper bound of the date from which the party is open or use the *calendar* icon.
	Required format is: YYYY-MM-DD
	The upper bound of the opening date must be later than or

Party – Search Criteria	
	equal to the lower bound. References for error messages [ ]: ❚ DPD1003 ❚ DPD1004
Closing Date – From	Enter the lower bound of the date from which the party is closed or use the *calendar* icon. Required format is: YYYY-MM-DD The lower bound of the closing date must be earlier than or equal to the upper bound and later than the lower bound of the opening date. References for error messages [ ]: ❚ DPD1003 ❚ DPD1004
Closing Date – To	Enter the upper bound of the date from which the party is closed or use the *calendar* icon. Required format is: YYYY-MM-DD The upper bound of the closing date must be later than or equal to the lower bound and later than the lower bound of the opening date. References for error messages [ ]: ❚ DPD1003 ❚ DPD1004
Party Type	Select the type of party from the possible values: ❚ All (default value) ❚ Service Operator ❚ Payment bank ❚ National Central Bank (NCB) Reference for error message [ ]: ❚ DPD1005 This field can be already filled in or have fewer values depending on your screen access.
Parent BIC	Enter the parent BIC of the party.

Party – Search Criteria	
	Required format is: max. 11 characters (SWIFT-x) References for error messages [ ]: ❚ DPD1001 ❚ DPD1013 ❚ DPD1180
Party BIC	Enter the BIC of the party. Required format is: max. 11 characters (SWIFT-x) References for error messages [ ]: ❚ DPD1013 ❚ DPD1180
Short Name	Enter the short name of the party. Required format is: max. 35 characters (SWIFT-x)

Parties – List	
Status	Shows the status of the party from the possible values: ❚ Active ❚ Deleted References for error messages [ ]: ❚ DPD1003 ❚ DPD1004
Opening Date	Shows the date from which the party is open. Displayed format is: YYYY-MM-DD References for error messages [ ]: ❚ DPD1003 ❚ DPD1004
Closing Date	Shows the date from which the party is closed. Displayed format is: YYYY-MM-DD References for error messages [ ]: ❚ DPD1003 ❚ DPD1004

Parties – List	
Type	Shows the type of party from the possible values: ▎ Service Operator ▎ Payment bank ▎ National Central Bank (NCB) Reference for error message [ ]: ▎ DPD1005
Parent BIC	Shows the parent BIC of the party. References for error messages [ ]: ▎ DPD1001 ▎ DPD1013 ▎ DPD1180
Party BIC	Shows the BIC of the party. References for error messages [ ]: ▎ DPD1013 ▎ DPD1180
Short Name	Shows the short name of the party.

Buttons

Search	This function enables you to start a search according to the filled in criteria. The results are displayed in a list on the same screen. If the search retrieves a single record, the *details* screen is displayed directly. Next screens: ▎ *Parties – search/list* screen ▎ *Party – details* screen [ ]
Reset	This function enables you to set default search criteria and blanks out all other criteria. Next screen: ▎ *Parties – search/list* screen

Edit	This function enables you to edit the details of the selected party. Next screen: ▎ *Party – edit* screen [▸] If the status of the selected party is set to 'Deleted', this function is not available. If you have accessed this screen via another screen, this function is not available.
Delete	This function enables you to delete the selected party, after confirmation. Next screen: ▎ *Parties – search/list* screen If the status of the selected party is already set to 'Deleted', this function is not available. References for error messages [▸]: ▎ DPD1001 ▎ DPD1003 ▎ DPD1030 If you have accessed this screen via another screen, this function is not available.

Restore	This function enables you to restore a previously deleted party.
	Next screen:
	▮ *Parties – search/list* screen
	If the status of the selected party is already set to 'Active', this function is not available.
	References for error messages [▸]:
	▮ DPD1001
	▮ DPD1004
	▮ DPD1005
	▮ DPD1013
	▮ DPD1021
	▮ DPD1024
	▮ DPD1040
	▮ DPD1180
	▮ DPD1207
	▮ DPD1208
	If you have accessed this screen via another screen, this function is not available.
Details	This function enables you to display the details of the selected party.
	Next screen:
	▮ *Party – details* screen [▸]
	If you have accessed this screen via another screen, this function is not available.
Revisions	This function enables you to display the revisions of the selected party.
	Next screen:
	▮ *Revisions/audit trail – list* screen [▸]
	If you have accessed this screen via another screen, this function is not available.

New	This function enables you to create a new party.
	Next screen:
	▮ *Party – new* screen [▸]
	If you have accessed this screen via another screen, this function is not available.

2.3.1.2 Party – Details Screen

Context of Usage
This screen displays detailed information on the selected party. You can check the data and proceed further by clicking on the buttons below.

Party reference data can only be viewed and edited by users belonging to the responsible CB, or by the Service operator (for 'NCB' party type). Users belonging to the party itself can only view their data.

Screen Access
▮ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *search* and/or *details* button

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

▮ Party reference data query

▮ Delete party

▮ Technical address network service link details query

References
User Instructions Part

This screen is part of the following business scenarios:

▮ Add a new technical address to a party [▸]

▮ Create a new technical address service link [▸]

▮ Delete an existing participant [▸]

▮ Edit an existing participant [▸]

Screenshot

← 🗎 🖨 ⟳

PARTY DETAILS

Status:	Active
Parent BIC:	SYSENTT2SX1
Opening Date:	2012-09-10

Closing Date: 2031-01-01

Party Type: National Central Bank

Codes

Valid From ≡	BIC ≡	Status ≡
2012-08-06	NCBKEMAXC50	Active

Total rows: 1

Names

Valid From ≡	Long Name ≡	Short Name ≡
2012-08-06	Long Name for Test Party	Test Party

Total rows: 1

Addresses

Valid From ≡	Street ≡	House Number ≡	Postal Code ≡	City ≡	State or Province ≡	Country Code ≡
2012-08-06	LARGO GUIDO CAR...	1	00044	FRASCATI	RM	IT

Total rows: 1

Tecnical Addresses

Technical Address ≡
PMBKEUXXC01
UNCHECKED-ADDRESS

Total rows: 2

Restrictions

Restriction Type ≡	Valid From ≡	Valid To ≡
	No Rows To Show	

Total rows: 0

☑ Edit   🗑 Delete   ⟳ Restore   ≡ Revisions $ Cash Accounts   📇 Technical Address Network Services Links

Illustration 26: Party – details screen

Field Description

Party	
Status	Shows the status of the party from the possible values: ▌ Active ▌ Deleted If the status is set to 'Active', the selected party cannot be restored. If the status is set to 'Deleted' the selected party cannot be edited or deleted. References for error messages [▶]: ▌ DPD1003 ▌ DPD1004

Party	
Parent BIC	Shows the parent BIC of the party. References for error messages [▶]: ▌ DPD1001 ▌ DPD1013 ▌ DPD1180
Party Type	Shows the type of party from the possible values: ▌ Service Operator ▌ Payment bank ▌ National Central Bank (NCB) References for error message [▶]: ▌ DPD1005 ▌ DPD1024
Opening Date	Shows the date from which the party is open. Displayed format is: YYYY-MM-DD References for error messages [▶]: ▌ DPD1003 ▌ DPD1004

Party
Party

Closing Date	Shows the date from which the party is closed. Displayed format is: YYYY-MM-DD References for error messages [ ]: ▎ DPD1003 ▎ DPD1004
Party Code	
Valid from	Shows the date from which the BIC is valid for the displayed Party. Displayed format is: YYYY-MM-DD
BIC	Shows the BIC of the party. References for error messages [ ]: ▎ DPD1013 ▎ DPD1180
Party Name	
Valid from	Shows the date from which the name of the party is valid. Displayed format is: YYYY-MM-DD
Long Name	Shows the full name of the party.
Party Short Name	Shows the short name of the party.

Address
Address

Actual Address	
Valid from	Shows the date from which the address of the party is valid. Displayed format is: YYYY-MM-DD
Street	Shows the street name of the address of the party.
House Number	Shows the house number of the address of the party.
Postal Code	Shows the postal code of the address of the party.

Address	
City	Shows the city of the address of the party.
State or Province	Shows the state or province of the address of the party.
Country Code	Shows the country code of the address of the party. Reference for error message [ ]: ▌ DPD1021

Technical Addresses	
Technical Address	
Technical Address	Shows the unique technical address of the party. Reference for error message [ ]: ▌ DPD1040 There can be more than one technical address, but each one must be unique.

Buttons

Edit	This function enables you to edit the details of the selected party. Next screen: ▌ *Party – new/edit* screen [▶] If the status of the selected party is set to 'Deleted', this function is not available.
Revisions	This function enables you to display the revisions of the selected party. Next screen: ▌ *Revisions/audit trail – list* screen [▶]
Cash Accounts	This function enables you to display the cash accounts related to the selected party. Next screen: ▌ *Cash accounts – search/list* screen [▶]

Technical Addresses Network Links	This function enables you to display the network services linked to the party's technical addresses. Next screen: ❚ *Technical addresses network services links – details* screen [▶]
Restore	This function enables you to restore the displayed party Next screen: ❚ *Parties – search/list* screen [▶] If the status of the selected party is already set to 'Active', this function is not available. References for error messages [▶]: ❚ DPD1001 ❚ DPD1004 ❚ DPD1005 ❚ DPD1013 ❚ DPD1021 ❚ DPD1024 ❚ DPD1040 ❚ DPD1180 ❚ DPD1207 ❚ DPD1208
Delete	This function enables you to delete the selected party, after confirmation. Next screen: ❚ *Parties – search/list* screen [▶] If the status of the selected party is already set to 'Deleted', this function is not available. References for error messages [▶]: ❚ DPD1001 ❚ DPD1003 ❚ DPD1030

2.3.1.3 Party – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding parties. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.

If there are old, current and future data available in the *edit* screen, the old and the current data are displayed above the entry fields, which contain the future values. Only one future value is possible at a time. If there is no future value, the current values can be edited. If you edit a future value, the current value remains valid until the validity date of the future record is reached.

You can use this screen either in 2-eyes or in 4-eyes mode.

Screen Access

❚ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *new* or *edit* button

❚ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *search* and/or *details* button >> *Party – details* screen >> Click on the *edit* button

Privileges

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

❚ Create party

❚ Update party

❚ Create technical address network service link

References

User Instructions Part

This screen is part of the following business scenarios:

❚ Add a new technical address to a party [▶]

❚ Create a new participant [▶]

❚ Edit an existing participant [▶]

❚ Create a new technical address service link [▶]

Screenshot

arties / Parties / Search / Details / Edit

PARTY UPDATE

Parent BIC: SYSENTT2SX1

Party Type: National Central Bank

Opening Date: 2012-09-10

Closing Date: 2031-01-01

Codes

BIC:

Valid From: 2018-03-30

Valid From	BIC	Status
2012-08-06	NCBKEMAXC50	Active

Total rows: 1

Names

Short Name:

Long Name:

Valid From: 2018-03-30

Valid From	Long Name	Short Name
2012-08-06	Long Name for Test Party	Test Party

Total rows: 1

Illustration 27: Party – edit screen

Field Description

Party	
Party	
Parent BIC	Shows the parent BIC of the party. This is a mandatory enter field in the *new* screen. Required format is: max. 11 characters (SWIFT-x) References for error messages [▶]: ❚ DPC1001 ❚ DPU1001 ❚ DPU1013
Party Type	Select the type of the party from the possible values: ❚ Payment bank References for error messages [▶]: ❚ DPC1002 ❚ DPC1005
Opening Date	Enter the date from which the party is open or use the *calendar* icon. Required format is: YYYY-MM-DD References for error messages [▶]: ❚ DPC1205 ❚ DPU1206 ❚ DPU1208 The opening date must be equal to or later than the current date. If the current date is later than the opening date, this field is read-only.
Closing Date	Enter the date from which the party is closed or use the *calendar* icon. Required format is: YYYY-MM-DD References for error messages [▶]: ❚ DPC1206 ❚ DPU1003 ❚ DPU1205 ❚ DPU1207

Party
❙ DPU1208
The closing date must be equal to or later than the current date and later than the opening date.

Party Code	
Status	Shows the status of the corresponding party code.
	Possible values are:
	❙ Active
	❙ Deleted
Options	Information on functions (icons) can be found in Common Buttons and Icons. Deletion is not possible for the current party code. In case a future value exists the update is possible for future record only.
Valid from	Shows the date from which the BIC of the party is valid. Displayed format is: YYYY-MM-DD
	References for error messages [ ]:
	❙ DPC1300
	❙ DPU1009
	❙ DPU1500
	❙ DPU1501
	If you want to add a future value in the *edit* screen, this field is a mandatory enter field.
	This field is not available in the *new* screen.
BIC	Enter the BIC of the party.
	Required format is: max. 11 characters (SWIFT-x)
	References for error messages [ ]:
	❙ DPC1013
	❙ DPC1180
	❙ DPU1001
	❙ DPU1005
	❙ DPU1013
	❙ DPU1180
	If you leave this field blank in the *edit* screen, the existing

Party
future value is cancelled.

Party Name	
Valid from	Shows the date from which the party name is valid.
	Displayed format is: YYYY-MM-DD
	References for error messages [ ]:
	❚ DPC1302
	❚ DPU1009
	❚ DPU1500
	If you want to add a future value in the *edit* screen, this field is a mandatory enter field. This field is not available in the *new* screen.
Party Long Name	Enter the full name of the party.
	Required format is: max. 350 characters (SWIFT-x)
	Reference for error message: [▶]
	❚ DPU1005
Party Short Name	Enter the short name of the party.
	Required format is: max. 35 characters (SWIFT-x)
	Reference for error message: [▶]
	❚ DPU1005
Options	Information on functions (icons) can be found in Common Buttons and Icons. In case a future value exists the update is possible for future record only.

Address
Actual Address

Valid from	Shows the date from which the address of the party is valid.
	Displayed format is: YYYY-MM-DD
	References for error messages [ ]:
	❚ DPC1301
	❚ DPU1009

Address	
	▌ DPU1010 ▌ DPU1500 If you want to add a future value in the *edit* screen, this field is a mandatory enter field.
Street	Enter the street name of the address of the party. Required format is: max. 70 characters (SWIFT-x) Reference for error messages [▶]: ▌ DPU1005
House Number	Enter the house number of the address of the party. Required format is: max. 16 characters (SWIFT-x) Reference for error messages [ ]: ▌ DPU1005
Postal Code	Enter the postal code of the address of the party. Required format is: max. 16 characters (SWIFT-x) Reference for error messages [▶]: ▌ DPU1005
City	Enter the city of the address of the party. Required format is: max. 35 characters (SWIFT-x) Reference for error messages [ ]: ▌ DPU1005
State or Province	Enter the state or the province of the address of the party. Required format is: max. 35 characters (SWIFT-x) Reference for error messages [▶]: ▌ DPU1005
Country Code	Select the country code of the address of the party from the drop-down menu. References for error messages [ ]: ▌ DPC1021 ▌ DPU1005 ▌ DPU1021

Address	
Options	Information on functions (icons) can be found in Common Buttons and Icons. In case a future value exists the update is possible for future record only.

Technical Addresses	
Address Value	Enter the technical address of the party. Required format is: max. 256 characters (UTF-8 except '>','<', '&') References for error messages [▶]: ❚ DPU1005 ❚ DPU1006 ❚ DPU1007 At least 1 technical address has to be defined[1]. There can be more than 1 technical address, but each one must be unique. You can add, edit or remove only 10 rows at a maximum. This field is also available as a show field for existing records.
Options	Information on functions (icons) can be found in Common Buttons and Icons.

Restrictions	
Type	Enter the restriction type applying to the party. Required format is: max. 35 characters (SWIFT-x) References for error messages [ ]: ❚ DPC1024 ❚ DPC1025 ❚ DPU1005 ❚ DPU1024 ❚ DPU1025 ❚ DPU1300 You can add, edit or remove only 10 rows at a maximum.

---

[1] In case the Party do not use the A2A channel a fake value (es.xxx) may be inserted

Restrictions
Duplicate Restriction –Valid From combinations are not allowed and you will be shown an error message to indicate 'Duplicate key fields'. There are 2 possible cases when this error message is shown: ▌ New entry in sub-table with a duplicate key ▌ When in one session (prior submitting) a row is deleted and a new row with the same values (from the deleted entry) in key fields is entered. This field is also available as a show field for existing records.

Valid from	Enter the date and time from which the restriction is valid or use the calendar icon. Required format is: YYYY-MM-DD hh:mm This date must be earlier than the 'Valid To' date of the restriction. To set an immediate restriction, input the timestamp '1000-01-01-00.01' References for error messages []: ▌ DPC1025 ▌ DPC1208 ▌ DPU1009 ▌ DPU1025 ▌ DPU1207 ▌ DPU1208 ▌ DPU1300 ▌ DPU1500 You can add, edit or remove only 10 rows at a maximum. Duplicate Restriction –Valid From combinations are not allowed and you will be shown an error message to indicate 'Duplicate key fields'. There are 2 possible cases when this error message is shown: ▌ New entry in sub-table with a duplicate key ▌ When in one session (prior submitting) a row is deleted and a new row with the same values (from the deleted entry) in key fields is entered

Restrictions
	This field is also available as a show field for existing records.
Valid to	Enter the date and time until which the restriction is valid or use the *calendar* icon. Required format is: YYYY-MM-DD hh:mm This date must be later than the 'Valid From' date of the restriction. To instantly remove a restriction, input the timestamp '9999-12-31-23.59' References for error messages [ ]: ❚ DPC1025 ❚ DPC1207 ❚ DPU1005 ❚ DPU1207 ❚ DPU1300 You can add, edit or remove only 10 rows at a maximum. This field is also available as a show field for existing records.
Options	Information on functions (icons) can be found in Common Buttons and Icons.

Buttons

Submit	This function enables you to create or edit a party.

Next screen:
▌ *Party – details* screen [▶]

References for error messages [▶]:
▌ DPC1001
▌ DPC1002
▌ DPC1005
▌ DPC1013
▌ DPC1021
▌ DPC1024
▌ DPC1025
▌ DPC1180
▌ DPC1205
▌ DPC1206
▌ DPC1207
▌ DPC1208
▌ DPC1300
▌ DPC1301
▌ DPC1302
▌ DPU1001
▌ DPU1003
▌ DPU1005
▌ DPU1006
▌ DPU1007
▌ DPU1009
▌ DPU1010
▌ DPU1013
▌ DPU1021
▌ DPU1024
▌ DPU1025
▌ DPU1030
▌ DPU1180

	▌ DPU1205
	▌ DPU1206
	▌ DPU1207
	▌ DPU1208
	▌ DPU1300
	▌ DPU1500
	▌ DPU1501
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ▌ *Parties – search/list* screen [▶]
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ▌ *Party – new/edit* screen
Technical Addresses Network Links	This function enables you to associate the technical addresses, already defined to the party, to a network service. This button is not available in the new screen. The button is enabled when you enter the edit screen. As soon as an item is added to the 'Technical addresses' sub-table, the button is disabled until you submit all the changes. Next screen: ▌ *Technical addresses network services links – new/edit* screen [▶]

2.3.1.4 Technical Addresses Network Services Link – Details Screen

Context of Usage This screen displays detailed information on the selected technical addresses network services link. You can check the data and proceed further by clicking on the buttons below.

Screen Access ▌ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *search* and/or *details* button >> *Party – details* screen >> Click on the *technical address network services links* button

Privileges To use this screen, you need the following privilege [▶]:

▌ Technical address network service link details query

References **User Instructions Part**

This screen is not part of a business scenario.

Screenshot

Illustration 28: Technical addresses network services link – details screen

Field Description

Technical Address Network Services Links	
Status	Shows the status of the corresponding technical address network service link.
Technical Address	Shows the unique technical address of the party.
Network Service	Shows the name of the network service.

2.3.1.5 Technical Addresses Network Services Link – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding technical addresses network services links. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.
You can use this screen either in 2-eyes or in 4-eyes mode.

This screen is not relevant for payment bank users.

Screen Access

▌ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *new* or *edit* button >> *Parties – new/edit* screen >> Click on the *technical addresses network services links* button

▌ Common >> Parties >> Parties >> *Parties – search/list* screen >> Click on the *search* and/or *details* button >> *Party – details* screen >> Click on the *edit* button >> *Party – edit* screen >> Click on the *technical addresses network services links* button

Privileges

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

❚ Create technical address network service link

❚ Delete technical address network service link

References

User Instructions Part

This screen is part of the following business scenario:

❚ Create a new technical address service link [▶]

Screenshot

Common / Parties / Parties / Search / Details / Edit / /tech-address-net-link/1145?editMode=true

TECHNICAL ADDRESSES NETWORK SERVICES
LINKS

Status	Technical Address	Network Service
Active	PMBKEUXXC01	NETWORK1
Active	PMBKEUXXC01	NETWORK4

Total rows: 2

Technical Address: PMBKEUXXC01   Network Service: NETWORK4

➕ Submit Row   🗑 Delete Row   ↺ Restore Row   ✖ Reset   ← Back to Party
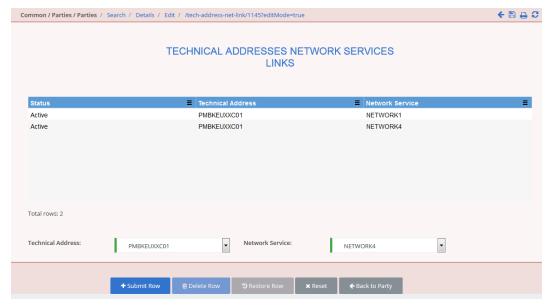
Illustration 29: Technical addresses network services link – edit screen

Field Description

Technical Address Network Services Links	
Status	Shows the status of the corresponding technical address network service link.
Technical Address	Shows the unique technical address of the party.
Network Service	Shows the name of the network service.
Add/Delete Tech. Address Network Service Link	
Technical Address	Select the unique technical address of the party from the drop-down menu. References for error messages [▶]: ❚ DPC3003 ❚ DPC3005
Network Service	Select the name of the network service from the drop-down menu.

Technical Address Network Services Links	
	Reference for error message [ ]: ❚ DPC3004

Buttons

Submit Row	This function enables you to create a new technical address network service link according to the information entered. Next screen: ❚ *Technical addresses network services link – new/edit* screen References for error messages [▶]: ❚ DPC3001 ❚ DPC3002 ❚ DPC3003 ❚ DPC3004 ❚ DPC3005 ❚ DPC3006
Delete Row	This function enables you to the delete the selected technical address network service link from the list. Next screen: ❚ *Technical addresses network services link – new/edit* screen If the status of the selected technical address network service link is already set to 'Deleted', this function is not available. References for error messages [ ]: ❚ DPD3001 ❚ DPD3003

Restore Row	This function enables you to restore a previously deleted technical address network service link.
	Next screen:
	❚ *Technical addresses network services link – new/edit* screen
	If the status of the selected technical address network service link is already set to 'Active, this function is not available.
	References for error messages [▶]:
	❚ DPD3004
	❚ DPD3005
	❚ DPD3006
	❚ DPD3007
	❚ DPD3008
	❚ DPD3009
Back to Party	This function enables you to cancel the process and return to the previous screen.
	Next screen:
	❚ *Party – new/edit* screen [▶]
Revisions	This function enables you to display the revisions of the selected technical addresses network services link.
	Next screen:
	❚ *Revisions/audit trail – list* screen [▶]

2.3.1.6 Party Service Link – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search the Service to which a Party is linked. The search results are displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access ❚ Common >> Parties >> Party Service Links

Privileges

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

❚ Delete Party-Service Link

❚ Party-Service Link List Query

Screenshot
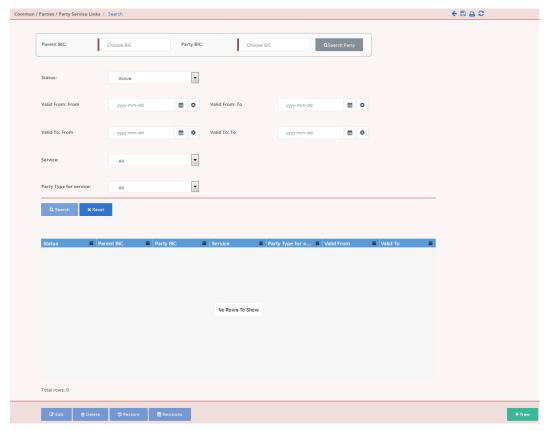
Illustration 30: Party Service Link – search/list screen

Field Description

Party Service Link – Search Criteria	
Parent BIC	Enter the Parent BIC of the party. Required format is: max. 11 characters (SWIFT-x)
Party BIC	Enter the Party BIC of the party. Required format is: max. 11 characters (SWIFT-x)
Status	Shows the status of the Party Service Link from the possible values: ▌ Active ▌ Deleted If the status is set to 'Deleted', the selected Party Service Link cannot be deleted or edited. If the status is set to 'Active', the selected Party Service Link cannot be restored.
Opening Date From	Enter the lower bound for the opening date of the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD
Opening Date To	Enter the upper bound for the opening date of the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date – to' must be greater than the 'Opening Date – from'.
Closing Date From	Enter the lower bound of the search range for the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD
Closing Date To	Enter the upper bound of the search range for the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD
Service	Select the Service from the possible values: ▌ All (default value) ▌ TIPS

Party Service Link – Search Criteria	
Party Type for Service	Select the Party Type the Party can have for the Service from the possible values: ▌ All (default value) ▌ TIPS Operator ▌ TIPS Central Bank ▌ TIPS Participant ▌ TIPS Reachable Party

Party Service Link – List	
Status	Shows the status of the Party Service Link from the possible values: ▌ Active ▌ Deleted If the status is set to 'Deleted', the selected Party Service Link cannot be deleted or edited. If the status is set to 'Active', the selected Party Service Link cannot be restored.
Parent BIC	Shows the parent BIC of the Party related to the Party Service Link.
Party BIC	Shows the party BIC of the Party related to the Party Service Link. References for error message: [▶] ▌ DPD4003 ▌ DPD4007
Service	Shows the Service which is associated to the Party. Possible values are: ▌ TIPS References for error message: [▶] ▌ DPD4005 ▌ DPD4005

Party Service Link – List	
Party Type for Service	Shows the Party type associated to the Party. Possible values are: ❚ TIPS Operator ❚ TIPS Central Bank ❚ TIPS Participant ❚ TIPS Reachable Party
Valid From	Shows the opening date of the Party Service Link. Displayed format is: YYYY-MM-DD
Valid To	Shows the closing date of the Party Service Link. Displayed format is: YYYY-MM-DD

Buttons

Search Party	This function enables the user to visualize the Search Parties screen in order to find the Parent/Party BIC of the Searched Party
Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. Next screens: ❚ *Party Service Link – search/list* screen [ ]
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Party Service Link – search/list* screen [▸]
Edit	This function enables you to edit the details of the selected Party Service Link. Next screen: ❚ *Party Service Link – edit* screen [ ] If the status of the selected Party Service Link is already set to 'Deleted' this function is not available.
Delete	This function enables you to delete the selected Party Service Link, after confirmation.

	Next screen:
	❚ *Party Service Link – search/list* screen
	If the status of the selected Party Service Link is already set to 'Deleted', this function is not available.
	References for error messages: [▶]
	❚ DPD4001
	❚ DPD4002
Restore	This function enables you to restore a previously deleted Party Service Link.
	Next screen:
	❚ *Party Service Link – search/list* screen
	If the status of the selected Party Service Link is already set to 'Active' this function is not available.
	References for error messages: [▶]
	❚ DPD4003
	❚ DPD4004
	❚ DPD4005
	❚ DPD4006
	❚ DPD4007
Revisions	This function enables you to display the revisions of the selected party.
	Next screen:
	❚ *Revisions/audit trail – list* screen [▶]
New	This function enables you to create a new Party Service Link.
	Next screen:
	❚ *Party Service Link – new* screen [▶]

2.3.1.7 Party Service Link – New/Edit Screen

Context of Usage
This screen contains a number of fields regarding The Party Service Links that can be assigned to an Actor. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. This screen is relevant for CB users.

Screen Access ❚ Common >> Parties >> Party Service Links >> *Party Service Links – search/list* screen >> Click on the *new* or *edit* button

Privileges To use this screen, you need the following privileges [▶]:

❚ Create Party Service Links

❚ Update Party Service Links

Screenshot
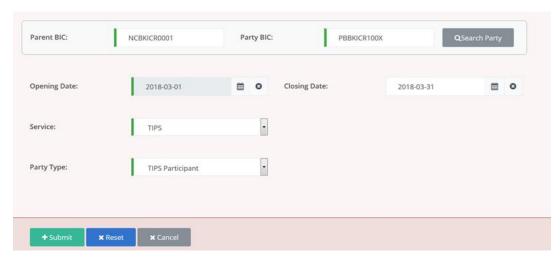
Illustration 31: Party Service Link – new/edit screen

Field Description

Party Service Link	
Parent BIC	Enter the Parent BIC of the party. Required format is: 11 characters (SWIFT-x)
Party BIC	Enter the Party BIC of the party. Required format is: 11 characters (SWIFT-x) References for error message: [▶] ▍ DPC4009 ▍ DPU4008
Opening Date	Enter the opening date of the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date' must be equal to or later than the current business date. References for error messages [▶]: ▍ DPC4004 ▍ DPC4008 ▍ DPU4003 ▍ DPU4004
Closing Date	Enter the closing date of the Party Service Link or use the calendar icon. Required format is: YYYY-MM-DD The 'Closing Date' must be equal to or later than the 'Opening Date' and the current business date. References for error messages [▶]: ▍ DPC4005 ▍ DPC4008 ▍ DPU4005 ▍ DPU4007

Service	Select the Service for which the Party should be enabled from the drop down menu. Possible values are: ❚ TIPS Reference for error messages [▶]: ❚ DPC4003
Party Type for Service	Select the Type of Party the Party will be for the Service Possible values are: ❚ TIPS Operator ❚ TIPS Central Bank ❚ TIPS Participant ❚ TIPS Reachable Party References for error messages [▶]: ❚ DPC4006 ❚ DPC4007

Buttons
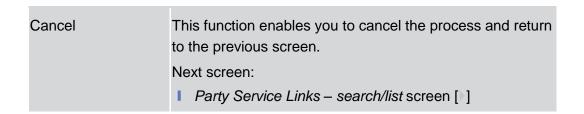
Search Party	This function enables the user to visualize the Search Parties screen in order to find the Parent/Party BIC of the Party
Submit	This function enables you to create or edit a Party Service Link. Next screen: ❙ *Party Service Links – search/list* screen [ ] References for error messages [ ]: ❙ DPC4001 ❙ DPC4002 ❙ DPC4003 ❙ DPC4004 ❙ DPC4005 ❙ DPC4006 ❙ DPC4007 ❙ DPC4008 ❙ DPC4009 ❙ DPU4001 ❙ DPU4001 ❙ DPU4002 ❙ DPU4003 ❙ DPU4004 ❙ DPU4005 ❙ DPU4006 ❙ DPU4007 ❙ DPU4008
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ❙ *Party Service Links – new/edit* screen

Cancel	This function enables you to cancel the process and return to the previous screen.
	Next screen:
	❚ *Party Service Links – search/list* screen [ ]

2.3.1.8 TIPS Directory – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for TIPS directory objects. The search results will be displayed in a list, which is sorted by the values of the 'User BIC' column in ascending order (default setting).

In addition, by clicking on the relevant buttons on the top of the screen, it is be possible to download the last and the previous version of the TIPS Directory in Full or Update mode.

Screen Access

❚ Common >> Parties >> TIPS Directory

Privileges

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

❚ TIPS Directory query

References

User Instructions Part

This screen is not part of any business scenario:

Screenshot
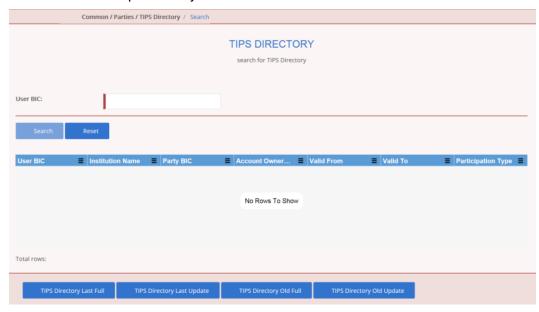
Illustration 3220: TIPS Directory – Search/List Screen

Field Description

TIPS Directory – Search Criteria	
User BIC	Enter the User BIC you want to search. Required format is: max. 11 characters (SWIFT-x)

TIPS Directory – List	
User BIC	Shows the BIC configured as Authorised Account User in TIPS. This BIC identifies one and only one TIPS Account or CMB in TIPS and it is the BIC that shall be used to address Instant Payments in TIPS.
Institution Name	Shows the name stored in the CRDM BIC Directory together with the User BIC.
Party BIC	Shows the BIC that identifies a TIPS Participant or a Reachable Party in TIPS. This BIC is for information purpose only and it allows grouping all User BICs configured by a given TIPS Participant or Reachable Party. It cannot be used to address Instant Payments in TIPS.
Account Owner BIC	Shows the BIC of the TIPS Participant owning the TIPS Account for which the User BIC has been authorised, also through a CMB.
Valid From	Shows the date from which the BIC is valid. Displayed format is: YYYY-MM-DD
Valid To	Shows the date until which the BIC is valid. Displayed format is: YYYY-MM-DD
Participation Type	Shows the type of participation of the User BIC. Possible values are: ❚ TIPS Participant ❚ Reachable Party

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen.
Reset	This function enables you to set default search criteria and blanks out all optional criteria.
TIPS Directory Last Full	This function enables you to download the Full version of the last TIPS directory.

TIPS Directory Last Update	This function enables you to download the Delta version of the last TIPS directory.
TIPS Directory Old Full	This function enables you to download the Full version of the previous TIPS directory.
TIPS Directory Old Update	This function enables you to download the Delta version of the previous TIPS directory.

2.3.2 Cash Account

2.3.2.1 Limits – Search/List Screen

Context of Usage   This screen contains a number of search fields. By inputting the relevant data, you can search to limits applicable to your TIPS Credit Memorandum Balances. The search results are displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access   ❚ TIPS >> Cash >> Limits

Privileges   To use this screen, you need the following privileges [▶]:

❚ Delete Limit

❚ Limit query

Screenshot
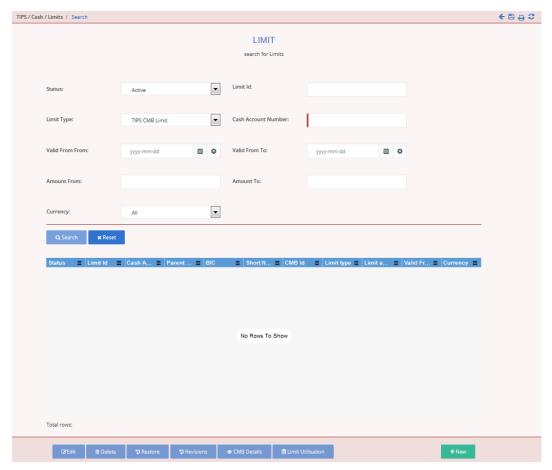
Illustration 33: Limit – Search/list screen

Field Description

Limit – Search Criteria	
Status	Select the status of the limit from the possible values:
	❚ All
	❚ Active (default value)
	❚ Deleted
	Reference for error messages [▶]
	❚ DRD9004
Limit id	Enter the technical ID of the limit
	Required format is: Integer, no wildcard possible
Limit type	Select the type of the limit from the possible values:
	❚ TIPS CMB Limit
Cash Account Number	Enter the TIPS Credit memorandum Balance number the limit is linked to
Valid From - From	Enter the lower bound for the opening date of the Limit or use the calendar icon. Required format is: YYYY-MM-DD
Valid From - To	Enter the upper bound for the opening date of the Limit or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date – to' must be greater than the 'Opening Date – from'.
Amount From	Enter the lower amount of the limit. Required format is: max. 18 digits followed by up to 5 decimals
Amount To	Enter the upper amount of the limit. Required format is: max. 18 digits followed by up to 5 decimals
Currency	Select the currency of the account from the drop-down menu. The default value is 'all'.

Limit – List	
Status	Shows the status of the limit from the possible values: ▮ Active ▮ Deleted If the status is set to 'Deleted', the selected limit cannot be deleted or edited. If the status is set to 'Active', the selected limit cannot be restored. Reference for error messages: [▶] ▮ DRD9004
Limit id	Shows the technical ID of the limit.
Cash Account	Shows the Cash Account number of the CMB the limit is linked to.
Parent BIC	Shows the parent BIC of the holder of the TIPS Account related to the relevant TIPS Credit Memorandum Balance.
BIC	Shows the party BIC of the holder of the TIPS Account related to the relevant TIPS Credit Memorandum Balance.
Short Name	Shows the Short name of the holder of the TIPS Account related to the relevant TIPS Credit Memorandum Balance.
CMB id	Shows the number of the TIPS Credit Memorandum Balance the limit is related to
Limit type	Shows the type of Limit from the possible values: ▮ TIPS CMB Limit
Limit amount	Shows the amount of the limit. Format is : max. 18 digits followed by up to 5 decimals
Valid from	Shows the opening date of the Limit. Displayed format is: YYYY-MM-DD
Currency	Shows the currency of the TIPS Credit Memorandum Balance account linked to the limit.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. Next screens: ❚ *Limit – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Limit – search/list* screen
Edit	This function enables you to edit the details of the selected limit. Next screen: ❚ *Limit – edit* screen [▶] If the status of the selected limit is already set to 'Deleted' this function is not available.
Delete	This function enables you to delete the selected limit, after confirmation. Next screen: ❚ *Limit – search/list* screen If the status of the selected limit is already set to 'Deleted', this function is not available. Reference for error messages: [▶] ❚ DRD9001
Restore	This function enables you to restore a previously deleted limit. Next screen: ❚ *Limit – search/list* screen If the status of the selected limit is already set to 'Active' this function is not available. References for error messages: [▶] ❚ DRD9004 ❚ DRD9205

Revisions	This function enables you to display the revisions of the selected limit. Next screen: ❚ *Revisions/audit trail – list* screen [▶] If the status of the selected limit is set to 'Deleted', this function is not available.
CMB Details	This function enables the user to enter the CMB related to the selected limit This field is not relevant for TIPS and therefore disabled.
Limit Utilisation	This function enables the user to display the "Limit utilisation" screen. This field is not relevant for TIPS and therefore disabled.
New	This function enables you to create a new limit. Next screen: ❚ *Limit – new* screen [▶]

2.3.2.2 Limit – New/Edit Screen

Context of Usage   This screen contains a number of fields regarding limits applicable to your TIPS Credit Memorandum Balance. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.

Screen Access   ❚ TIPS >> Cash >> Limits >> *Limit – search/list* screen >> Click on the *new* or *edit* button

Privileges   To use this screen, you need the following privileges [▶]:

❚ Create Limit
❚ Update Limit

Screenshot

TIPS / Cash / Limits / Search / New

LIMIT NEW

Cash Account Number: Choose...   Authorised BIC:

Limit Type: TIPS CMB Limit   Limit Amount:

Valid From: 2018-02-14   Time: 00 : 00

+ Submit   **✗ Reset**   **✗ Cancel**
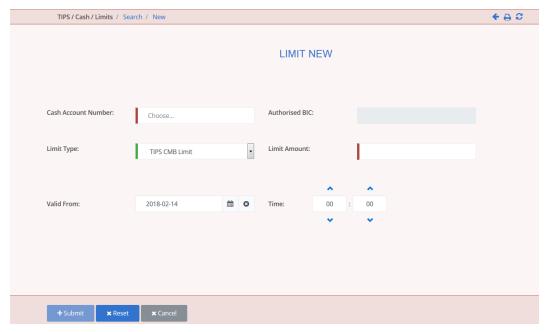
Illustration 34: Limit – new/edit screen

Field Description

Limit	
Cash Account number	Enter the unique number identifying the TIPS Credit Memorandum Balance the limit is related to. This field is a mandatory enter field in the new screen. Required format is: max. 34 characters (SWIFT-x) References for error message [▶]: ▌ DRC9001 ▌ DRC9052
Authorised BIC	Shows the BIC authorised on the cash account for whom the limit is inserted. This field is visible and editable only if the field Limit Type is different from "TIPS CMB". Required format is: max. 11 characters (SWIFT-x) This field is not relevant for TIPS and therefore disabled.
Limit type	Select the limit type from the possible values: ▌ TIPS CMB Limit References for error messages: [▶] ▌ DRC9058 ▌ DRC9100
Limit amount	Enter the amount of the limit. Required format is: max. 18 digits followed by up to 5 decimals References for error messages: [▶] ▌ DRC9100 ▌ DRC9800 ▌ DRU9800
Valid from	Enter the date from which the limit is valid or use the calendar icon. Required format is: YYYY-MM-DD Reference for error messages: [▶] ▌ DRC9205
Time	Select the time of the date from which the limit is valid. Format is hh:mm

Buttons

Submit	This function enables you to create or edit a Limit. Next screen: ❚ *Limit – search/list* screen [▶] References for error messages [▶]: ❚ DRC9001 ❚ DRC9052 ❚ DRC9058 ❚ DRC9100 ❚ DRC9205 ❚ DRC9800 ❚ DRU9001 ❚ DRU9003 ❚ DRU9800
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ❚ *Limit – new/edit* screen
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ❚ *Limit – search/list* screen [▶]

2.3.2.3 Cash Accounts – Search/List Screen

Context of Usage
This screen contains a number of search fields. By inputting the relevant data you can search for Cash accounts. The search results will be displayed in a list, which is sorted by the values of the 'Party BIC' column in ascending order (default setting). After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access
❚ TIPS >> Cash >> Cash Accounts

Privileges
To use this screen, you need the following privileges [▶]:
❚ Delete Cash account list query
❚ Cash account reference data query

▌ Cash account list query

References   **User Instruction Part**

This screen is part of the following business scenarios:

▌ Edit an existing Cash Account [▶]

▌ Delete an existing Cash Account [▶]

Screenshot
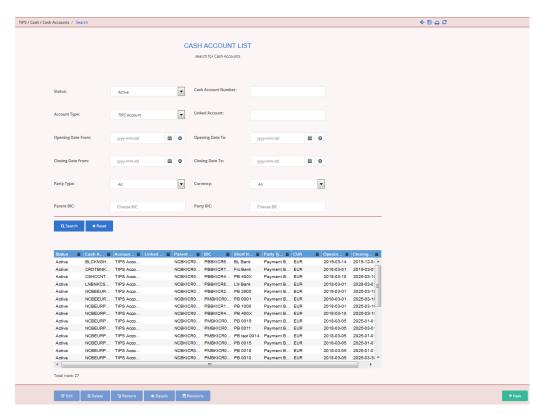
Illustration 35: Cash Account – search/list screen

Field Description

Cash Accounts – Search Criteria	
Status	Select the status of the cash account from the possible values: ▮ All (default value) ▮ Active ▮ Deleted References for error messages: [▶] ▮ DCD1003 ▮ DCD1012
Cash Account Number	Enter the number of the Cash Account. Required format is: max. 34 characters (SWIFT-x)
Account Type	Select the type of the cash account from the possible values: ▮ All (default value) ▮ TIPS account ▮ TIPS transit account ▮ TIPS credit memorandum balance References for error messages: [▶] ▮ DCD1013 ▮ DCD1014 ▮ DCD1555
Linked Account	Enter the number of the cash account to which the TIPS Credit Memorandum Balance can be linked
Opening Date – from	Enter the lower bound for the opening date of the account or use the calendar icon. Required format is: YYYY-MM-DD
Opening Date – to	Enter the upper bound for the opening date of the account or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date – to' must be greater than the 'Opening Date – from'.
Closing Date – from	Enter the lower bound for the closing date of the account

Cash Accounts – Search Criteria	
	or use the calendar icon. Required format is: YYYY-MM-DD The 'Closing Date – from' must be later than the 'Opening Date – from'.
Closing Date – to	Enter the upper bound for the closing date of the account or use the calendar icon. Required format is: YYYY-MM-DD The 'Closing Date – to' must be later than the 'Closing Date – from'.
Party type	Select the type of party from the possible values: ❚ All (default value) ❚ Payment bank ❚ National Central Bank Reference for error message: [▶] ❚ DCD1555
Currency	Select the currency of the account from the drop-down menu. The default value is 'all'. References for error messages: [▶] ❚ DCD1082 ❚ DCD1207
Parent BIC	Enter the parent BIC of the party. Required format is: min. 2 characters, max. 11 characters (SWIFT-x) Reference for error message: [▶] ❚ DCD1083
Party BIC	Enter the BIC of the party. Required format is: min. 2 characters, max. 11 characters (SWIFT-x)

Cash Accounts – List	
Status	Shows the status of the cash account from the possible values: ❚ Active ❚ Deleted If the status is set to 'Deleted', the selected cash account cannot be deleted or edited. If the status is set to 'Active', the selected cash account cannot be restored. References for error messages: [▶] ❚ DCD1003 ❚ DCD1012
Cash Account Number	Shows the identification of the cash account.
Account Type	Shows the type of cash account from the possible values: ❚ TIPS Account ❚ TIPS Transit Account ❚ TIPS Credit Memorandum Balance
Linked Account	Shows the Cash Account to which the TIPS Credit Memorandum Balance is linked when the Account type is TIPS Credit Memorandum Balance.

Cash Accounts – List	
Parent BIC	Shows the parent BIC of the account. Reference for error message: [▶] ❙ DCD1083
BIC	Shows the party BIC of the account. Reference for error messages: [▶] ❙ DCD1083
Short Name	Shows the party short name of the account.
Party type	Shows the type of party from the possible values: ❙ Payment bank ❙ National Central Bank Reference for error message: [▶] ❙ DCD1555
Currency	Shows the currency of the cash account. References for error messages: [▶] ❙ DCD1082 ❙ DCD1207
Opening Date	Shows the opening date of the cash account. Displayed format is: YYYY-MM-DD References for error messages: [▶] ❙ DCD1003 ❙ DCD1012
Closing date	Shows the closing date of the cash account. Displayed format is: YYYY-MM-DD References for error messages: [▶] ❙ DCD1003 ❙ DCD1012

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. If the search retrieves a single record, the details screen is displayed directly. Next screens: ❚ Cash accounts – search/list screen [▶] ❚ Cash account – details screen [▶] Reference for error messages: [▶] ❚ DCD1001
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Cash accounts – search/list* screen
Edit	This function enables you to edit the details of the selected cash account. Next screen: ❚ *Cash account – edit* screen [▶] If the status of the selected cash account is already set to 'Deleted' this function is not available.
Delete	This function enables you to delete the selected cash account, after confirmation. Next screen: ❚ *Cash accounts – search/list* screen If the status of the selected cash account is already set to 'Deleted', this function is not available. References for error messages: [▶] ❚ DCD1003 ❚ DCD1012 ❚ DCD1014 ❚ DCD1030
Restore	This function enables you to restore a previously deleted

	cash account.
	Next screen:
	▌ *Cash accounts – search/list* screen
	If the status of the selected cash account is
	already set to 'Active' this function is not available.
	References for error messages: [▶]
	▌ DCD1001
	▌ DCD1012
	▌ DCD1013
	▌ DCD1082
	▌ DCD1085
	▌ DCD1086
	▌ DCD1532
Details	This function enables you to display the details of the selected cash account.
	Next screen:
	▌ *Cash account – details* screen [▶]
Revisions	This function enables you to display the revisions of the selected cash account.
	Next screen:
	▌ *Revisions/audit trail – list* screen [▶]
New	This function enables you to create a new cash account.
	Next screen:
	▌ *Cash account – new* screen [▶]

2.3.2.4 Cash Account – Details Screen

Context of Usage   This screen displays detailed information on the selected cash account. You can check the data and proceed further by clicking on the buttons below.

Screen Access   ▌ TIPS >> Cash >> Cash Accounts >> *Cash Accounts – search/list* screen >> Click on the *search* and/or *details* button >> Click on the *search* and/or *details* button

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

- ▮ Cash account reference data query

- ▮ Delete Cash account list query

Screenshot
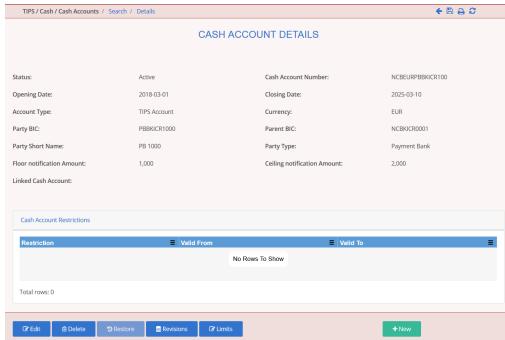
Illustration 36: Cash Account – details screen

Field Description

Cash Account	
Status	Shows the status of the cash account from the possible values: ❚ Active ❚ Deleted If the status is set to 'Deleted', the selected cash account cannot be deleted or edited. If the status is set to 'Active', the selected cash account cannot be restored.
Cash Account Number	Shows the unique number of the cash account.
Opening date	Shows the opening date of the cash account. Displayed format is: YYYY-MM-DD References for error messages [▶]: ❚ DCD1003 ❚ DCD1012
Closing date	Shows the closing date of the cash account. Displayed format is: YYYY-MM-DD References for error messages [▶]: ❚ DCD1003 ❚ DCD1012
Account type	Shows the type of cash account from the possible values: ❚ TIPS Account ❚ TIPS Transit Account ❚ TIPS Credit Memorandum Balance References for error messages [▶]: ❚ DCD1013 ❚ DCD1014 ❚ DCD1555
Currency	Shows the currency of the cash account. References for error messages [▶]: ❚ DCD1207

Cash Account	
	▌ DCD1082
Party BIC	Shows the BIC of the party. Reference for error message [▶]: ▌ DCD1083
Parent BIC	Shows the parent BIC of the party. Reference for error message [ ]: ▌ DCD1083
Party Short Name	Shows the short name of the party.
Party Type	Shows the type of party that owns the account. Reference for error message [ ]: ▌ DCD1555
Floor notification Amount	Shows the lower threshold for notifying the cash manager.
Ceiling notification Amount	Shows the upper threshold for notifying the cash manager.
Linked Cash Account	Shows the number of the Cash Account to which the TIPS Credit Memorandum Balance is linked in case the Account type is TIPS Credit Memorandum Balance.

Restrictions	
Type	Shows the type of restriction related to the cash account. Reference for error message [▶]: ▌ DCD1084
Valid from	Shows the date and time from which the cash account restriction is valid. Displayed format is: YYYY-MM-DD hh:mm
Valid to	Shows the date and time until which the cash account restriction is valid. Displayed format is: YYYY-MM-DD hh:mm

Buttons

Edit	This function enables you to edit the details of the selected cash account. Next screen: ❚ *Cash account – edit* screen [▶] If the status of the selected cash account is already set to 'Deleted' this function is not available.
Delete	This function enables you to delete the selected cash account, after confirmation. Next screen: ❚ *Cash accounts – search/list* screen [ ] If the status of the selected cash account is already set to 'Deleted', this function is not available. References for error messages [▶]: ❚ DCD1001 ❚ DCD1003 ❚ DCD1014 ❚ DCD1030
Restore	This function enables you to restore a previously deleted cash account. Next screen: ❚ *Cash accounts – search/list* screen [▶] If the status of the selected cash account is already set to 'Active', this function is not available. References for error messages [▶]: ❚ DCD1012 ❚ DCD1013 ❚ DCD1082 ❚ DCD1083 ❚ DCD1084 ❚ DCD1085 ❚ DCD1086 ❚ DCD1207 ❚ DCD1532

Buttons

	▌ DCD1555
Revisions	This function enables you to display the revisions of the selected cash account. Next screen: ▌ *Revisions/audit trail – list* screen [▶]
Limits	This function enables you to display the limits related to the selected cash accounts. Next screen: ▌ *Limits – search/list* screen [▶] If the status of the selected cash account is already set to 'Deleted', this function is not available.
New	This function enables you to create a new cash account. Next screen: ▌ *Cash account – new* screen [▶]

2.3.2.5 Cash Account – New/Edit Screen

Context of Usage   This screen contains a number of fields regarding 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 relevant for CB users.

Screen Access   ▌ TIPS >> Cash >> Cash Accounts >> *Cash Accounts – search/list* screen >> Click on the *new* or *edit* button

Privileges   To use this screen, you need the following privileges [▶]:

▌ Create cash account

▌ Update cash account

References   **User Instruction Part**

This screen is part of the following business scenario:

▌ Create a Cash Account [▶]

Screenshot
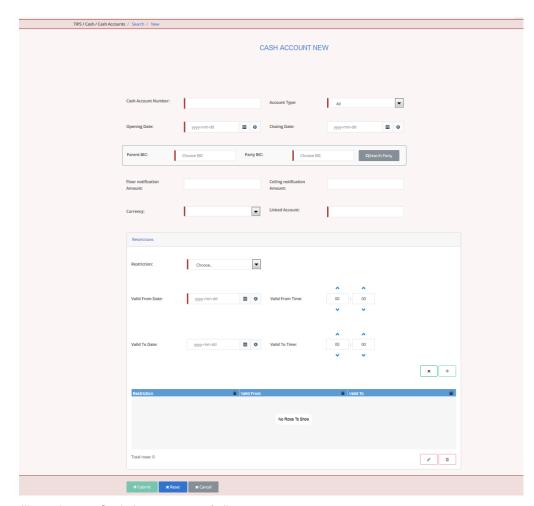
Illustration 37: Cash Account – new/edit screen

Field Description

Cash Account

Cash Account number	Shows the unique number identifying the account. Reference for error message [▶]: ▌ DCC1103 This field is a mandatory enter field in the new screen. Required format is: max. 34 characters (SWIFT-x)
Account type	Shows the type of the cash account from one of the possible values: ▌ TIPS account ▌ TIPS Transit account ▌ TIPS Credit Memorandum Balance Reference for error message [ ]: ▌ DCC1532
Opening date	Enter the opening date of the cash account or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date' must be equal to or later than the current business date. References for error messages [▶]: ▌ DCC1205 ▌ DCU1213 The field is read-only if the opening date is in the past.
Closing date	Enter the closing date of cash account or use the calendar icon. Required format is: YYYY-MM-DD The 'Closing Date' must be equal to or later than the 'Opening Date' and the current business date. References for error messages [ ]: ▌ DCC1210 ▌ DCC1532 ▌ DCU1210 ▌ DCU1313

Cash Account	
Parent BIC	Shows the parent BIC of the party holding the account. This field is mandatory in the new screen. You can choose to either enter the parent BIC of the party holding the account or to select it from the suggested items in the drop-down menu. Required format is: max. 11 characters (SWIFT-x) References for error messages [ ]: ▌ DCC1001 ▌ DCC1524 ▌ DCU1001
Party BIC	Shows the BIC of the party holding the account. This field is mandatory in the new screen. You can choose to either enter the BIC of the party holding the account or to select it from the suggested items in the drop-down menu. Required format is: max. 11 characters (SWIFT-x) References for error messages [ ]: ▌ DCC1001 ▌ DCC1524 ▌ DCU1001
Party Short name	Shows the Party short name of the owner of the account. The field is visible only in Edit function and is read-only.
Party type	Shows the Party type of the owner of the account. The field is visible only in Edit function and is read-only.

Cash Account	
Floor notification Amount	Enter the lower threshold for notifying the cash manager. Required format is: max. 15 digits incl. decimal point (thereof max. 5 decimal places and decimal point) In case this amount is not specified or it is set to zero, no floor notification will be triggered. In order to configure a floor threshold that triggers a notification when a balance becomes negative, the threshold value should be set to 0.01. References for error messages [ ]: ❙ DCC1101 ❙ DCC1800 ❙ DCU1101 ❙ DCU1313 ❙ DCU1800
Ceiling notification Amount	Enter the upper threshold for notifying the cash manager. Required format is: max. 15 digits incl. decimal point (thereof max. 5 decimal places and decimal point) In case this amount is not specified or it is set to zero, TIPS will not trigger any ceiling notification. In order to configure a ceiling threshold that triggers a notification when a balance becomes positive, the threshold value should be set to 0.01. References for error messages [ ]: ❙ DCC1101 ❙ DCC1800 ❙ DCU1101 ❙ DCU1800
Currency	Select the currency of the cash account from the drop-down menu. References for error messages [ ]: ❙ DCC1100 ❙ DCC1207 ❙ DCC1530

Cash Account
▌ DCC1531 ▌ DCU1218

Linked Account	Shows the number of the cash account to which the cash account can be linked.

Restrictions

Restrictions	You can choose to either enter the restriction type or to select it from the suggested items in the drop-down menu. References for error messages [ ]: ▌ DCC1024 ▌ DCC1300 ▌ DCC1555 ▌ DCU1024 ▌ DCU1217 ▌ DCU1300 This field is also available as a show field for existing records. Duplicate Restriction Type-Valid From combinations are not allowed and you will be shown an error message to indicate 'Duplicate key fields'. There are two possible cases when this error message is shown: ▌ New entry in sub-table with a duplicate key ▌ When in one session (prior submitting) a row is deleted and a new row with the same values (from the deleted entry) in key fields is entered
Valid from	Enter the date and time from which the cash account restriction is valid or use the calendar icon. Required format is: YYYY-MM-DD hh:mm References for error messages [ ]: ▌ DCC1025 ▌ DCC1208 ▌ DCC1209 ▌ DCC1300 ▌ DCU1211 ▌ DCU1214

Restrictions
▌ DCU1216   ▌ DCU1219   ▌ DCU1300   This field is also available as a show field for existing records.   Duplicate Restriction Type-Valid From combinations are not allowed and you will be shown an error message to indicate   'Duplicate key fields'. There are 2 possible cases when this error message is shown: ▌ New entry in sub-table with a duplicate key   ▌ When in one session (prior submitting) a row is deleted and a new row with the same values (from the deleted entry) in key fields is entered

| Valid to | Enter the date and time until which the cash account restriction is valid or use the calendar icon.
 Required format is: YYYY-MM-DD hh:mm

 References for error messages [▶]:
 ▌ DCC1212
 ▌ DCC1300
 ▌ DCU1212
 ▌ DCU1220
 ▌ DCU1300
 This field is also available as a show field for existing records. |

Buttons

Search Party	This function enables the user to activate "Parties". It is visible only in creation mode.
Submit	This function enables you to create or edit a cash account. Next screens: ▌ *Cash account – details* screen [▶] References for error messages [▶]:

- DCC1001
- DCC1024
- DCC1025
- DCC1100
- DCC1101
- DCC1103
- DCC1205
- DCC1206
- DCC1207
- DCC1208
- DCC1209
- DCC1210
- DCC1212
- DCC1300
- DCC1530
- DCC1531
- DCC1532
- DCC1555
- DCC1601
- DCC1800
- DCU1001
- DCU1003
- DCU1024
- DCU1030
- DCU1040
- DCU1101
- DCU1204
- DCU1206
- DCU1207
- DCU1210
- DCU1211
- DCU1212
- DCU1213
- DCU1216

	▌ DCU1217
	▌ DCU1218
	▌ DCU1219
	▌ DCU1220
	▌ DCU1300
	▌ DCU1313
	▌ DCU1532
	▌ DCU1555
	▌ DCU1600
	▌ DCU1800
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ▌ *Cash account – edit* screen
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ▌ *Cash accounts – search/list* screen [ ]

2.3.2.6 Authorised Account User – Search/list Screen

Context of Usage This screen contains a number of fields regarding Authorised Account Users. By inputting the relevant data, you can search for Authorised Account Users. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access ▌ TIPS >> Cash >> Authorised Account Users

Privileges To use this screen you need the following privilege [▶]:
▌ Delete Authorised Account User
▌ Authorised Account User Query

References **User Instructions Part**

This screen is part of the following business scenario:
▌ Delete an Authorised Account User [▶]

Screenshot
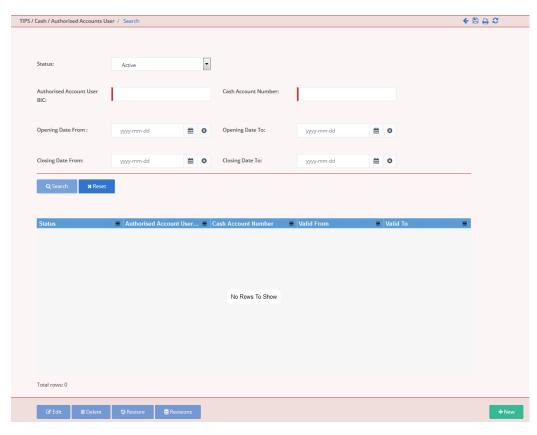
Illustration 38: Authorised Account User List – search screen

Field Description

Authorised Account User – Search criteria	
Status	Select the status of the Authorised Account User from the possible values: **|** All **|** Active (default value) **|** Deleted
Authorised Account User BIC	Enter the BIC of the Authorised Account User. Required format is: max. 11 characters (SWIFT-x)
Cash Account Number	Enter the TIPS Cash Account the BIC is authorised to use. Required format is: max. 34 characters (SWIFT-x)
Opening Date From	Enter the lower bound for the opening date of the Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD
Opening Date To	Enter the upper bound for the opening date of the Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD

Authorised Account User – Search criteria	
	The 'Opening Date – to' must be greater than the 'Opening Date – from'.
Closing Date From	Enter the lower bound of the search range for the Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD
Closing Date To	Enter the upper bound of the search range for the Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD

Authorised Account User – List	
Status	Shows the status of the Authorised Account User from the possible values: ❙ Active ❙ Deleted If the status is set to 'Deleted', the selected Authorised Account User cannot be deleted or edited. If the status is set to 'Active', the selected Authorised Account User cannot be restored.
Authorised Account User BIC	Shows the BIC of the Authorised Account User.
Cash Account Number	Shows the TIPS Cash Account the BIC is authorised to use. Required format is: max. 34 characters (SWIFT-x)
Valid from	Enter the opening date of the Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date' must be equal to or later than the current business date.
Valid to	Enter the closing date of Authorised Account User or use the calendar icon. Required format is: YYYY-MM-DD The 'Closing Date' must be equal to or later than the

Authorised Account User – List
'Opening Date' and the current business date.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. Next screens: ❚ *Authorised Account User – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Authorised Account User – search/list* screen

Edit	This function enables you to edit the details of the selected Authorised Account User. Next screen: ❚ *Authorised Account User – edit* screen [▶] If the status of the selected Authorised Account User is already set to 'Deleted' this function is not available.
Delete	This function enables you to delete the selected Authorised Account User, after confirmation. Next screen: ❚ *Authorised Account User – search/list* screen If the status of the selected Authorised Account User is already set to 'Deleted', this function is not available. References for error messages: [▶] ❚ DCD2001 ❚ DCD2002 ❚ DCD2008
Restore	This function enables you to restore a previously deleted Authorised Account User. Next screen: ❚ *Authorised Account User – search/list* screen If the status of the selected Authorised Account User is already set to 'Active' this function is not available. References for error messages: [▶] ❚ DCD2003 ❚ DCD2004 ❚ DCD2005 ❚ DCD2006 ❚ DCD2007
Revisions	This function enables you to display the revisions of the selected Authorised Account User. Next screen: ❚ *Revisions/audit trail – Authorised Account User* screen [▶]

New	This function enables you to create a new Authorised Account User.
	Next screen:
	❙ *Authorised Account User – new* screen [▶]

2.3.2.7 Authorised Account User – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding Authorised Account User. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. This screen is relevant for CB and Payment Bank users. You can use this screen in 2-eyes or in 4-eyes mode.

Screen Access

❙ TIPS >> Cash >> Authorised Account Users >> *Authorised Account User – search/list* screen >> Click on the *new* or *edit* button

Privileges

To use this screen you need the following privileges [▶]:

❙ Create Authorised Account User

❙ Update Authorised Account User

References

User Instruction Part

This screen is part of the following business scenarios:

❙ Create an Authorised Account User [▶]

Screenshot

AUTHORISED ACCOUNT USER NEW

Authorised Account User BIC:

Cash Account Number:

Valid From: yyyy-mm-dd

Valid To: yyyy-mm-dd

+ Submit   ✖ Reset   ✖ Cancel
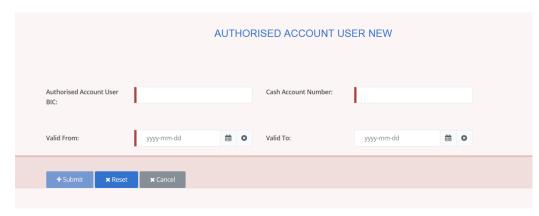
Illustration 39: Authorised Account User – new/edit screen

Field Description

Authorised Account User	
Authorised Account User BIC	Enter the BIC of the Authorised Account User. Required format is: max. 11 characters (SWIFT-x) Reference for error messages [ ]: ❙ DCC2003
Cash Account Number	Enter the TIPS Cash Account Required forma is: max. 34 characters (SWIFT-x) References for error messages [ ]: ❙ DCC2002 ❙ DCU2002
Valid From	Enter the date from which the li Authorised Account User is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages: [ ] ❙ DCC2004 ❙ DCU2003 ❙ DCU2004
Valid To	Enter the date and time until which the Authorised Account User is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages: [ ]: ❙ DCC2005 ❙ DCU2005

Buttons

Submit	This function enables you to create or edit an Authorised Account User.
	Next screen:
	▮ *Authorised Account User – search/list* screen [▸]
	References for error messages [▸]:
	▮ DCC2001
	▮ DCC2002
	▮ DCC2003
	▮ DCC2004
	▮ DCC2005
	▮ DCC2006
	▮ DCC2007
	▮ DCU2001
	▮ DCU2002
	▮ DCU2003
	▮ DCU2004
	▮ DCU2005
	▮ DCU2006
	▮ DCU2007
Reset	This function enables you to set all fields to default value and blanks out all optional fields.
	Next screen:
	▮ *Authorised Account User – new/edit* screen
Cancel	This function enables you to cancel the process and return to the previous screen.
	Next screen:
	▮ *Authorised Account User – search/list* screen [▸]

2.3.3 Access Rights

2.3.3.1 Certificate Distinguished Names – Search/List Screen

This screen contains a number of search fields. By inputting the relevant data, you can search for certificate distinguished names. The search results will be

Context of Usage

displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

There is no usage restriction for this screen.

Screen Access Privileges

▮ Common >> Access Rights Management >> Certificate Distinguished Names

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

▮ Certificate query

▮ Delete certificate distinguish name

References

User Instructions Part

This screen is part of the following business scenario:

▮ Create a new user certificate distinguished name [▶]

Screenshot

Common / Access Rights Management / Certificate Distinguished Names / Search		← 🖫 🖨 🔄

| Status: | Active ▾ | Certificate Distinguished Name: | |

🔍 Search   ✖ Reset

Status	☰	Certificate Distinguished Name	☰
Active		prova1 t2s	
Active		prova2 t2s usermain	
Active		prova3 crdm mainuser	
Active		prova4 noMainuser	
Active		prova5 crdm noMainUser	
Active		prova6 crdm noMainUser	
Active		Certificate Test Dmt	
Active		test21	
Active		TEST CERT2	
Active		TEST CERT3	
Active		TEST CERT4	
Active		TIPS CERT1	
Active		T2S CERT1	
Active		SERIALNUMBER=MARKDEFF-U-9515e70f, CN=Dennis Asquino, T=Payment and Account Management O…	
Active		cn=IT:995907900,cn=users,dc=ac,dc=bankit,dc=it	

Total rows: 57

🗑 Delete   ↺ Restore   ☰ User Certificate Distinguished Name Links   ＋ New

Illustration 40: Certificate distinguished name – search/list screen

Field Description

Certificate Distinguished Names – Search Criteria	
Status	Select the status of the certificate distinguished name from the possible values: ▌ All ▌ Active (default value) ▌ Deleted References for error messages [▶]: ▌ DRDA003 ▌ DRDA004
Certificate Distinguished Name	Enter the distinguished name of the certificate. Required format is: max. 256 characters (UTF-8 except '>', '<', '&') Reference for error message [ ]: ▌ DRDA002

Certificate Distinguished Names – List	
Status	Shows the status of the certificate distinguished name from the possible values: ▌ Active ▌ Deleted If the status is set to 'Deleted', the selected certificate distinguished name cannot be deleted. If the status is set to 'Active', the selected certificate distinguished name cannot be restored. References for error messages [▶]: ▌ DRDA003 ▌ DRDA004
Certificate Distinguished Name	Shows the distinguished name of the certificate. Reference for error message [ ]: ▌ DRDA002

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. Next screen: ❚ *Certificate distinguished names – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Certificate distinguished names – search/list* screen
New	This function enables you to create a new user certificate distinguished name. Next screen: ❚ *Certificate distinguished name – new* screen [▶]
Delete	This function enables you to delete the selected certificate distinguished name, after confirmation. Next screen: ❚ *Certificate distinguished names – search/list* screen If the status of the selected certificate distinguished name is already set to 'Deleted', this function is not available. References for error messages [▶]: ❚ DRDA001 ❚ DRDA003 ❚ DRDA010

Restore	This function enables you to restore a previously deleted certificate distinguished name.
	Next screen:
	❚ *Certificate distinguished names – search/list* screen
	If the status of the selected certificate distinguished name is already set to 'Active', this function is not available.
	References for error messages [▶]:
	❚ DRDA001
	❚ DRDA002
	❚ DRDA004
Revisions	This function enables you to display the revisions of the selected certificate distinguished name.
	Next screen:
	❚ *Revisions/audit trail – list* screen [▶]
User certificate Distinguished Name Links	This function enables you to display the user certificate distinguished name links.
	Next screen:
	❚ *User certificate distinguished name links – search/list* screen [▶]

2.3.3.2 Certificate Distinguished Names – New Screen

Context of Usage This screen contains a number of fields regarding certificate distinguished names. You can enter new data. Afterwards you can proceed by clicking on the buttons below. You can use this screen in 2-eyes or in 4-eyes mode.

There is no usage restriction for this screen.

Screen Access ❚ Common >> Access Rights Management >> Certificate Distinguished Names >> *Certificate distinguished names – search/list* screen >> Click on the *new* button

Privileges To use this screen, you need the following privilege [▶]:

❚ Create certificate distinguished name

References **User Instructions Part**

This screen is part of the following business scenario:

❚ Create a new user certificate distinguished name [▶]

Screenshot

Common / Access Rights Management / Certificate Distinguished Names / Search / New

CERTIFICATE DISTINGUISHED NAME NEW

Certificate Distinguished
Name:

+ Submit   × Reset   × Cancel

Illustration 41: Certificate distinguished name – new screen

Field Description

Certificate Distinguished Name	
Certificate Distinguished Name	Enter the distinguished name of the certificate. Required format is: max. 256 characters (UTF-8 except '>', '<', '&') Reference for error message [▶]: ❙ DRCA002

Buttons

Submit	This function enables you to create a new certificate distinguished name according to the information entered in the fields. Next screen: ❙ *Certificate distinguished name – new* screen References for error messages: [▶] ❙ DRCA001 ❙ DRCA002
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ❙ *Certificate distinguished name – new* screen
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ❙ *Certificate distinguished names – search/list* screen [▶]

2.3.3.3 Grant/Revoke System Privileges – Search Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data,

you can search for privileges granted to a role. You can proceed further by clicking on the buttons below. This function is available in U2A mode only.

Screen Access

❚ Common >> Access Rights Management >> Grant/Revoke System privileges

Privileges

To use this screen, you need the following privilege [▶]:

❚ Privilege query

References

User Instructions Part

This screen is part of the following business scenarios:

❚ Assign a role to a party [▶]

❚ Grant privileges to a role [▶]

Screenshot

Common / Access Rights Management / Grant/Revoke System Privileges / Search

SYSTEM PRIVILEGES

search criteria for System Privileges

Role name

Choose Role...

Q Search   ⬜ Display
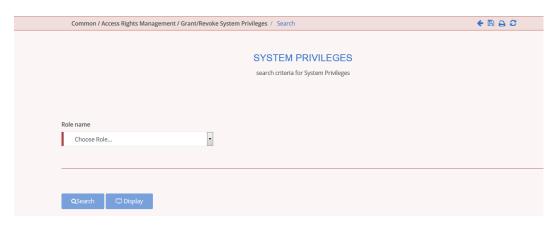
Illustration 42: Grant/revoke System Privileges – search screen

Field Description

Grant/Revoke Privileges – Search Criteria	
Role name	Select the name of the role.
	Required format is: max. 35 characters (SWIFT-x), input sensitive

Buttons

Search	This function enables you to start a search according to the criteria entered. Next screen: ❚ Grant/revoke system privilege – new/edit screen [▶]
Display	This function enables you to start a search according to the criteria entered accessing the grant/revoke system privilege – details screen. Next screen: ❚ Grant/revoke system privilege – details screen [▶]

2.3.3.4 Grant/Revoke Roles – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for:

❚ Parties and users the role is granted to

❚ Roles granted to the selected party

❚ Roles granted to the selected user.

There is no usage restriction for this screen.

Screen Access

❚ Common >> Access Rights Management >> Grant/Revoke Roles

Privileges

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

❚ Granted roles list query

❚ Grant/revoke role

References

User Instructions Part

This screen is part of the following business scenarios:

❚ Assign a role to a user [▶]

❚ Assign a role to a party [▶]

Screenshot

Common / Access Rights Management / Grant/Revoke Roles / Search

GRANT/REVOKE ROLES

search criteria for Roles

Role name — Choose Role...

Parent BIC: — Choose BIC — Party BIC: — Choose BIC

Login name — Choose User...

Q Search   Display
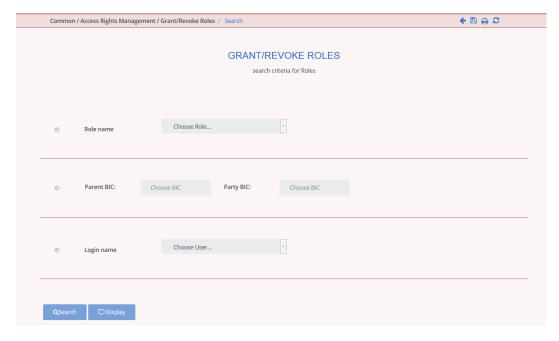
Illustration 43: Grant/Revoke roles – search screen
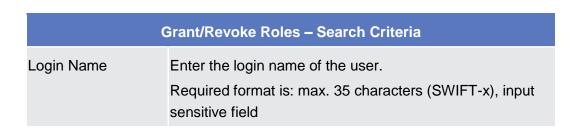
Field Description

Grant/Revoke Roles – Search Criteria	
Role	
Role Name	Select the name of the role. Required format is: max. 35 characters (SWIFT-x), input sensitive field. If the corresponding option is selected, the field is enabled and mandatory, otherwise it is not available.
Parties	
Parent BIC	Enter the parent BIC of the party. Required format is: max. 11 characters (SWIFT-x), input sensitive field. If the corresponding option is selected, the field is enabled and mandatory, otherwise it is not available.
Party BIC	Enter the BIC of the party. Required format is: max. 11 characters (SWIFT-x), input sensitive field. If the corresponding option is selected, the field is enabled and mandatory, otherwise it is not available.
User	

Grant/Revoke Roles – Search Criteria	
Login Name	Enter the login name of the user. Required format is: max. 35 characters (SWIFT-x), input sensitive field

Buttons

Search	The function enables you to start a search according to the criteria entered accessing the *grant/revoke role – new/edit* screen. Next screen: ▌ *Grant/revoke role – new/edit* screen [▶]
Display	The function enables you to start a search according to the criteria entered accessing the *grant/revoke role – details* screen. Next screen: ▌ *Grant/revoke role – details* screen [ ]

2.3.3.5 Grant/Revoke Role – Details Screen

Context of Usage
This screen displays detailed information on users and parties that are granted a specific role. You can check the data. There is no usage restriction for this screen.

Screen Access
▌ Common >> Access Rights Management >> Grant/Revoke Roles >> *Grant/Revoke Roles – search/list* screen >> Click on the *display* button

Privileges
To use this screen, you need the following privilege [▶]:
▌ Granted roles list query

References
User Instructions Part

This screen is part of the following business scenarios:
▌ Assign a role to a user [▶]
▌ Assign a role to a party [▶]

Screenshot

Common / Access Rights Management / Grant/Revoke Roles / Search / Details

ROLES DETAILS

Role 000000000Elisa07

Parties		Users
Parent BIC	Party BIC	Filter....
Filter....	Filter....	
SYSENTT2SX1	SYSENTT2SX1	No Rows To Show
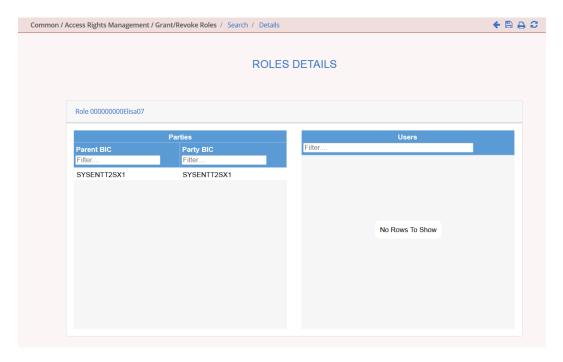
Illustration 44: Grant/revoke role – details screen (role mode)

Common / Access Rights Management / Grant/Revoke Roles / Search / Grant/Revoke

GRANT/REVOKE ROLES

Party SYSENTT2SX1 - NCBKICR0001

Roles	Current Granted Roles
Filter....	Filter....
☐ TEST	
☐ TEST GSP 2	
☐ TEST GSP 3	
☐ TEST GSP 4	
☐ TIP_AdjustCMBLimit	
☐ TIP_InstantPayment	
☐ TIP_LiquidityTransfer	No Rows To Show
☐ TIP_ModifyAllBlocking	
☐ TIP_ModifyCMBBlocking	
☐ TIP_QueryAll	
☐ TIP_QueryReachable	
☐ Test 23 02 2015	
☐ Test115A	
☐ TestLasoAndDDE	

Illustration 45: Grant/revoke role – details screen (party roles mode)
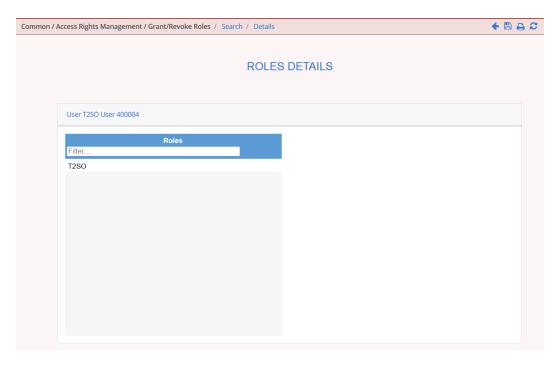
Illustration 46: Grant/revoke role – details screen (user roles mode)

Field Description		Role <Role Name> OR Party <Parent BIC + BIC> OR User <User Login Name>	
	Filter Parent BIC	Enter the parent BIC of the party to filter the 'Parties' and the 'Current Granted Parties' lists. Required format is: max. 11 characters (SWIFT-x) This field is only available in the 'Role' mode.	
	Filter BIC	Enter the BIC of the party to filter the 'Parties' and the 'Current Granted Parties' lists. Required format is: max. 11 characters (SWIFT-x) This field is only available in the 'Role' mode.	
	Current Granted Parties		
	Parent BIC	Shows the parent BIC of the party. This field is only available in the 'Role' mode.	
	Party BIC	Shows the BIC of the party. This field is only available in the 'Role' mode.	

Role <Role Name> OR Party <Parent BIC + BIC> OR User <User Login Name>	
Filter User	Enter the login name of the user to filter the current granted users list. Required format is: max. 35 characters (SWIFT-x) This field is only available in the 'Role' mode.
Users	Shows the login name of the user the role is granted to. This field is only available in the 'Role' mode.
Filter Role	Enter the name of the role to filter the current granted roles list. Required format is: max. 35 characters (SWIFT-x) This field is only available in the 'Party Roles' and 'User Roles' mode.
Roles	Shows the name of the granted role. This field is only available in the 'Party Roles' and 'User Roles' mode.

2.3.3.6 Grant/Revoke Role – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding roles. You can grant new roles to users or parties or revoke those that have been previously granted. You can use this screen either in 2-eyes or in 4-eyes mode.

Screen Access

❙ Common >> Access Rights Management >> Grant/Revoke Roles >> *Grant/Revoke roles – search* screen >> Click on the *search* button

❙ Common >> Access Rights Management >> Roles >> *Roles – search/list* screen >> Click on the *grant/revoke role* button

Privileges

To use this screen, you need the following privilege [▶]:

❙ Grant/revoke role

References

User Instructions Part

This screen is part of the following business scenarios:

❚ Assign a role to a user [▶]

❚ Assign a role to a party [▶]

Screenshot

Common / Access Rights Management / Grant/Revoke Roles / Search / Grant/Revoke

GRANT/REVOKE ROLES

Party SYSENTT2SX1 - BITAITMMXXX

Roles		Current Granted Roles
Filter....		Filter....
☐ 000000000Elisa04		☐ ROLEOBJ2
☐ 000000000Elisa07		
☐ 000000000Elisa08		
☐ 000000000Elisa09		
☐ 000000000Elisa10		
☐ 000000000Praga		
☐ 000000000Vienna		
☐ Avorio		
☐ Avorio		
☐ Bianco		
☐ Blue		
☐ Brown		
☐ Brown		
☐ CB		
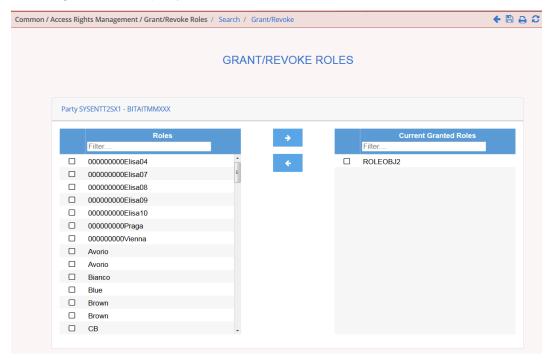
Illustration 47: Grant/revoke role – edit screen

Field Description

Role <Role Name> OR Party <Parent BIC + BIC> OR User <User Login Name>	
Filter Parent BIC	Enter the parent BIC of the party to filter the 'Parties' and the 'Current Granted Parties' lists. Required format is: max. 11 characters (SWIFT-x) This field is only available in the 'Role' mode.
Filter BIC	Enter the BIC of the party to filter the 'Parties' and the 'Current Granted Parties' lists. Required format is: max. 11 characters (SWIFT-x) This field is only available in the 'Role' mode.
Parties	
Parent BIC	Shows the parent BIC of the party.

	Role <Role Name> OR Party <Parent BIC + BIC> OR User <User Login Name>
	References for error messages [ ]: ▌ DRGR002 ▌ DRGR005 This field is only available in the 'Role' mode.
Party BIC	Shows the BIC of the party. References for error messages [ ]: ▌ DRGR002 ▌ DRGR005 This field is only available in the 'Role' mode.
Current Granted Parties	
Parent BIC	Shows the parent BICs of the parties which are currently granted the role. This field is only available in the 'Role' mode.
Party BIC	Shows the BICs of the parties which are currently granted the role. This field is only available in the 'Role' mode.
Filter User	Enter the login name of the user to filter the 'Users' and 'Current Granted Users' lists. Required format is: max. 35 characters (SWIFT-x) This field is only available in the 'Role' mode.
Users	Shows the login name of the user. References for error messages [ ]: ▌ DRGR002 ▌ DRGR005 This field is only available in the 'Role' mode.
Current Granted Users	Shows the names of the users which are currently granted the role.

	Role <Role Name> OR Party <Parent BIC + BIC> OR User <User Login Name>	
	This field is only available in the 'Role' mode.	
Filter Role	Enter the name of the role to filter the 'Roles' and 'Current Granted Roles' lists. Required format is: max. 35 characters (SWIFT-x) This field is only available in the 'Party Roles' and 'User Roles' mode.	
Roles	Shows the name of the role. References for error messages [ ]: ▌ DRGR001 ▌ DRGR003 ▌ DRGR007 This field is only available in the 'Party Roles' and 'User Roles' mode.	
Current Granted Roles	Shows the name of the roles which are currently granted to the user or party. Reference for error message [ ]: ▌ DRGR004 This field is only available in the 'Party Roles' and 'User Roles' mode.	

Buttons

Grant →	This function enables you to grant the selected role to the party or the user by moving the selected items from the 'Not Granted' list to the 'Granted' list. Upon clicking on the *grant* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❚ *Grant/revoke role – new/edit* screen References for error messages [ ]: ❚ DRGR001 ❚ DRGR002 ❚ DRGR003 ❚ DRGR005 ❚ DRGR007 ❚ DRGR008
Revoke ←	This function enables you to revoke the selected role from the party or the user by moving the selected items from the 'Granted' list to the 'Not Granted' list. Upon clicking on the *revoke* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❚ *Grant/revoke role – new/edit* screen References for error messages [ ]: ❚ DRGR001 ❚ DRGR002 ❚ DRGR004 ❚ DRGR005

2.3.3.7 Grant/Revoke System Privilege – Details Screen

Context of Usage

This screen displays detailed information on all roles that are granted a specific system privilege. You can check the data and proceed further by clicking on the buttons below.

This screen is not relevant for payment bank users.

Screen Access

Privileges

▌ Common >> Access Rights Management >> Grant/Revoke System Privileges >> *Grant/Revoke System Privileges – search* screen >> Click on the *display* button

To use this screen, you need the following privilege [▶]:

▌ Granted system privileges list query

Screenshot
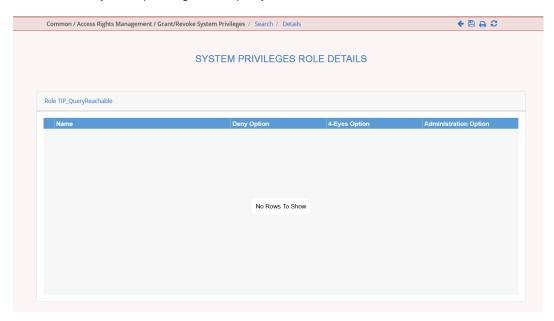
Illustration 48: Grant/revoke system privilege – details screen

Field Description

Role <Role Name>	
Name	Shows the privileges related to the selected group.
Deny Option	Shows whether the system privilege is explicitly denied from the possible values: ❚ Y (for yes) ❚ N (for no)
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the system privilege or not from the possible values: ❚ Y (for yes) ❚ N (for no)
Administration Option	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. 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. The possible values are: ❚ Y (for yes) ❚ N (for no)

2.3.3.8 Grant/Revoke System Privilege – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding system privileges. You can grant new system privileges to roles or revoke those that have been previously granted. Afterwards you can proceed further by clicking on the buttons below. This screen is not relevant for payment bank users. You can use this screen either in 2-eyes or in 4-eyes mode.

Screen Access

❚ Common >> Access Rights Management >> Grant/Revoke System Privileges >> *Grant/Revoke System Privileges – search* screen >> Click on the *search* button

❚ Common >> Access Rights Management >> Roles >> *Roles – search/list* screen >> Click on the *grant/revoke privilege* button

Privileges

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

❚ Grant privilege

❚ Revoke Privilege

❚ Granted System Privileges List Query

References

User Instructions Part

This screen is part of the following business scenario:

❚ Grant privileges to a role [▶]

Screenshot
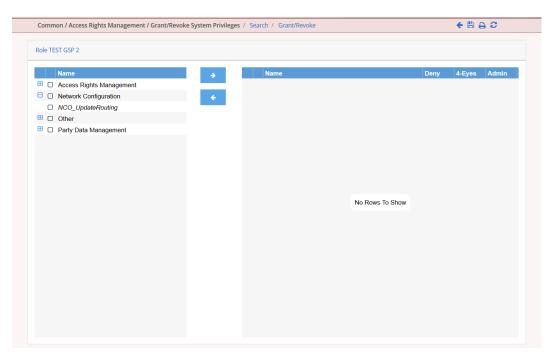
Illustration 49: Grant/revoke system privilege – new/edit screen

Field Description

Role <Role Name>	
Group Name	Shows the full list of all group names.
Privilege Name	Shows the privileges related to the selected group.
	References for error messages [🔊]:
	▎ DRGP001
	▎ DRGP002
	▎ DRRP001
	If the privilege type is set to 'Object', the privilege name and the field are highlighted.
Current Granted Privileges	
Group Name	Shows the full list of all group names related to the currently granted privileges.
Privilege Name	Shows the names of the currently granted privileges.
	If the privilege type is 'Object', the privilege name and the field are highlighted.
Deny Option	Shows whether the system privilege is explicitly denied from the possible values:
	▎ Y (for yes)
	▎ N (for no)
4-Eyes Option	Shows whether the 4-eyes mode is required in order to perform the activity linked to the system privilege or not from the possible values:
	▎ Y (for yes)
	▎ N (for no)
Administration option	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.
	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.

Role <Role Name>
The possible values are: ▌ Y (for yes) ▌ N (for no)

Input Additional Data (data input prompt)	
Deny Option	Select if the system privilege is explicitly denied. Reference for error message [ ]: ▌ DRGP017
4-Eyes Option	Select if the 4-eyes mode is required to perform the activity linked to the system privilege. Reference for error message [ ]: ▌ DRGP018

Buttons

Grant →	This function enables you to grant the selected privileges to the role. Next screen: ▌ *Grant/revoke system privilege – new/edit* screen The function opens the 'Input Additional Data' prompt to specify additional information.
Revoke ←	This function enables you to revoke the selected privileges from the role by moving them from the 'Granted' list to the 'Not Granted' list. Next screen: ▌ *Grant/revoke system privilege – new/edit* screen References for error messages [ ]: ▌ DRRP001 ▌ DRRP003 ▌ DRRP004 ▌ DRRP005 ▌ DRRP006

Submit	This function enables you to move the selected privileges from the 'Not Granted' list to the 'Granted' list inserting the additional information to privileges. Upon clicking on the submit button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the actor.
	Next screen:
	▌ *Grant/revoke system privilege – new/edit* screen
	References for error messages [▶]:
	▌ DRGP001
	▌ DRGP002
	▌ DRGP004
	▌ DRGP005
	▌ DRGP007
	▌ DRGP008
	▌ DRGP012
	▌ DRGP013
	▌ DRGP014
	▌ DRGP016
	▌ DRGP017
	▌ DRGP018
	▌ DRGP019
	▌ DRGP020
	▌ DRRP001
	▌ DRRP004
	▌ DRRP005
	▌ DRRP006
	▌ DRRP007

2.3.3.9 Roles – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for roles. The search results will be displayed in a list, which is sorted by the values of the 'Role Name' column in ascending order (default

setting). After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access	❚ Common >> Access Rights Management >> Roles
Privileges	To use this screen, you need the following privileges [▶]:
	❚ Role list query
	❚ Delete role
References	**User Instructions Part**
	This screen is part of the following business scenario:
	❚ Create a new role [▶]
Screenshot	
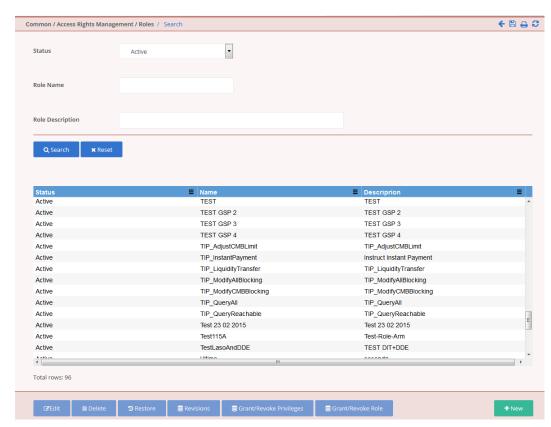
Illustration 50: Roles – search/list screen

Field Description

Roles – Search Criteria	
Status	Select the status of the role from the possible values: ❙ All ❙ Active (default value) ❙ Deleted References for error messages [▶]: ❙ DRD6003 ❙ DRD6044
Role Name	Enter the name of the role. Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ❙ DRD6002
Role Description	Enter the description of the role. Required format is: max. 127 characters (SWIFT-x)

Roles – List	
Status	Shows the status of the role from the possible values: ❙ Active ❙ Deleted If the status is set to 'Deleted', the selected role cannot be edited. If the status is set to 'Active', the selected role cannot be restored. References for error messages [▶]: ❙ DRD6003 ❙ DRD6044
Name	Shows the name of the role. Reference for error message [ ]: ❙ DRD6002
Description	Shows the description of the role.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. Next screen: ❙ *Roles – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❙ *Roles – search/list* screen
New	This function enables you to create a new role. Next screen: ❙ *Role – new* screen [▶]
Edit	This function enables you to edit the details of the selected role. Next screen: ❙ *Role – edit* screen [▶] If the status of the selected role is already set to 'Deleted', this function is not available.
Restore	This function enables you to restore a previously deleted role. Upon clicking on the *restore* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❙ *Roles – search/list* screen If the status of the selected role is already set to 'Active', this function is not available. References for error messages [▶]: ❙ DRD6001 ❙ DRD6002 ❙ DRD6044
Revisions	This function enables you to display the revisions of the selected role.

	Next screen:
	▌ *Revisions/audit trail – list* screen [▶]
Delete	This function enables you to delete the selected role, after confirmation. Upon clicking on the *delete* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor.
	Next screen:
	▌ *Roles – search/list* screen
	If the status of the selected role is already set to 'Deleted', this function is not available.
	References for error messages [▶]:
	▌ DRD6001
	▌ DRD6003
	▌ DRD6050
Grant/Revoke Privileges	This function enables you to grant and/or revoke privileges for the selected role, depending on your access rights.
	Next screens:
	▌ *Grant/revoke system privileges – new/edit* screen [▶]
	▌ *Grant/revoke system privileges – details* screen [▶]
	If you have the 'Grant privileges' or 'Revoke privileges' privilege assigned, the *grant/revoke system privileges – new/edit* screen [▶ 57] is displayed.
	If you have the 'Privileges Query' privilege assigned, the *grant/revoke system privileges – details* screen [ ] is displayed.
Grant/Revoke Role	This function enables you to grant and/or revoke the selected role, depending on your access rights.
	Next screen:
	▌ *Grant/revoke roles – new/edit* screen [▶]
	If you have a 'Grant role' or 'Revoke role' privilege assigned, the *grant/revoke role – new/edit* screen [▶] is displayed.

2.3.3.10 Role – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding roles. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. You can use this screen either in 2-eyes or in 4-eyes mode.

This screen is not relevant for payment bank users.

Screen Access

❚ Common >> Access Rights Management >> Roles >> *Roles – search/list* screen >> Click on the *new* or *edit* button

Privileges

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

❚ Create role

❚ Update role

References

User Instructions Part

This screen is part of the following business scenario:

❚ Create a new role [▶]

Screenshot

Common / Access Rights Management / Roles / Search / New

ROLE NEW

Role Name: FDECCDMIN

Role Description: FDECCDMIN Description

Submit   Reset   Cancel
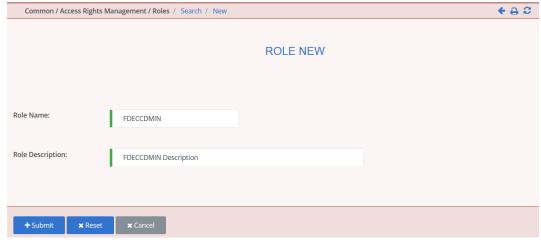
Illustration 51: Role – new screen

Field Description

Role	
Role Name	Enter the name of the role. Required format is: max. 35 characters (SWIFT-x) References for error messages [▶]: ❚ DRC6006 ❚ DRU6006
Role Description	Enter the description of the role. Required format is: max. 127 characters (SWIFT-x)

Buttons

Submit	This function enables you to create or edit a role. Upon clicking on the *submit* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❙ *Role – new/edit* screen References for error messages [▶]: ❙ DRC6001 ❙ DRC6006 ❙ DRU6001 ❙ DRU6003 ❙ DRU6006
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ❙ *Roles – search/list* screen [▶]
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ❙ *Role – new/edit* screen

2.3.3.11 Users – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for users. The search results will be displayed in a list, which is sorted by the values of the 'Login Name' column in ascending order (default setting). After selecting an entry, you can proceed further by clicking on the buttons below.

When exporting the content of this screen, you receive the list and the corresponding details for each data record.

Screen Access ❙ Common >> Access Rights Management >> Users

Privileges To use this screen, you need the following privileges [▶]:

I System user query

I Delete user

References

User Instructions Part

This screen is part of the following business scenario:

I Create a new user [▶]

Screenshot
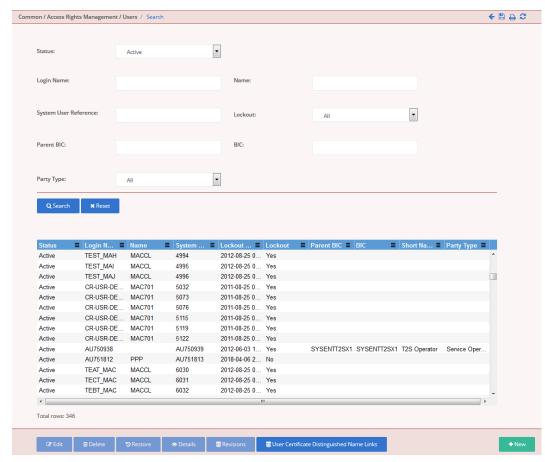
*Illustration 52: Users – search/list* screen

Field Description

Users – Search Criteria	
Status	Select the status of the user from the possible values: I All I Active (default value) I Deleted References for error messages [▶]: I DRD7003 I DRD7004
Login Name	Enter the login name of the user.

Users – Search Criteria	
	Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ❚ DRD7002
Name	Enter the name of the user. Required format is: max. 127 characters (SWIFT-x)
System User Reference	Enter the system user reference associated to the user. Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ❚ DRD7005
Lockout Status	Select the lockout status of the user from the possible values: ❚ All (default value) ❚ Yes ❚ No
Parent BIC	Select the parent BIC of the party related to the user from the drop-down menu or search via the *magnifier* icon. Required format is: max. 11 characters (SWIFT-x) Reference for error messages [ ]: ❚ DRD7007
Party BIC	Select the BIC of the party related to the user from the drop-down menu or search via the *magnifier* icon. Required format is: max. 11 characters (SWIFT-x) Reference for error messages [ ]: ❚ DRD7007
Party Type	Select the type of party related to the user from the possible values: ❚ All (Default value) ❚ Service operator ❚ Payment bank ❚ National Central Bank (NCB)

Users – List	
Status	Shows the status of the user from the possible values: ❙ Active ❙ Deleted If the status is set to 'Deleted', the selected user cannot be edited or deleted. If the status is set to 'Active', the selected user cannot be restored. References for error messages [▶]: ❙ DRD7003 ❙ DRD7004
Login Name	Shows the login name of the user. Reference for error message [ ]: ❙ DRD7002
Name	Shows the name of the user.
System User Reference	Shows the system user reference associated to the user. Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ❙ DRD7005
Lockout Status since	Shows the date and time from which the user is locked out of the system or the date and time from which the user is locked in again. Displayed format is: YYYY-MM-DD hh:mm
Lockout Status	Shows the lockout status of the user from the possible values: ❙ Yes ❙ No
Parent BIC	Shows the parent BIC of the party related to the user. Reference for error message [▶]: ❙ DRD7007

Users – List	
Party BIC	Shows the BIC of the party related to the user. Reference for error messages [ ]: ▌ DRD7007
Party Short Name	Shows the short name of the party related to the user.
Party Type	Shows the party type of the party related to the user.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. If the search retrieves a single record, the *details* screen is displayed directly. Next screens: ▌ *Users – search/list* screen ▌ *User – details* screen [ ]
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ▌ *Users – search/list* screen
New	This function enables you to create a new system user. Next screen: ▌ *User – new* screen [ ]
Edit	This function enables you to edit the details of the selected system user. Next screen: ▌ *User – edit* screen [ ] If the status of the selected user is already set to 'Deleted', this function is not available.
Delete	This function enables you to delete the selected system user, after confirmation. Upon clicking on the *delete* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by

	the CRDM actor. Next screen: ❚ *Users – search/list* screen If the status of the selected user is already set to 'Deleted', this function is not available. References for error messages [▶]: ❚ DRD7001 ❚ DRD7003 ❚ DRD7008
Details	This function enables you to display the details of the selected system user. Next screen: ❚ *User – details* screen [▶]
Restore	This function enables you to restore a previously deleted system user. Upon clicking on the *restore* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❚ *Users – search/list* screen If the status of the selected user is already set to 'Active', this function is not available. References for error messages [▶]: ❚ DRD7001 ❚ DRD7002 ❚ DRD7004 ❚ DRD7005 ❚ DRD7007
User Certificate Distinguished Name Links	This function enables you to access the *User certificate distinguished name links* screen for the selected user. Next screen: ❚ *User certificate distinguished name links – search/list* screen [▶]

2.3.3.12 User – Details Screen

Context of Usage   This screen displays detailed information on the selected user. You can check the data and proceed further by clicking on the buttons below.

Screen Access   ❙ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *search* and/or *details* button

Privileges   To use this screen you, need the following privileges [▶]:

❙ System user query

❙ Delete user

References   **User Instructions Part**

This screen is not part of a business scenario.

Screenshot

Common / Access Rights Management / Users / Search / Details

USER DETAILS

Status:	Active	Login Name:	TEST_USER_LANDI 7
Name:	TEST_USER_LANDI	System User Reference:	7
Lockout From:	9999-12-31 00:00	Lockout:	
Parent BIC:		Party BIC:	
Party Type:		Party Short Name:	

Edit · Delete · Restore · Revisions · New

User Certificate Distinguished Name Links
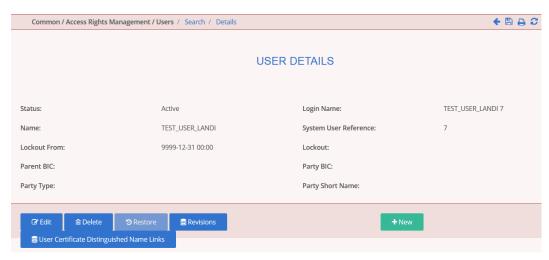
Illustration 53: User – details screen

Field Description

User	
Status	Shows the status of the user from the possible values: ❙ Active ❙ Deleted If the status is set to 'Deleted', the selected user cannot be edited or deleted. If the status is set to 'Active', the selected user cannot be restored. References for error messages [▶]: ❙ DRD7003 ❙ DRD7004
Login Name	Shows the login name of the user. Reference for error message [ ]: ❙ DRD7002
User Name	Shows the name of the user.
System User Reference	Shows the system user reference associated to the user. Reference for error message [ ]: ❙ DRD7005
Lockout Status since	Shows the date and time from which the user is locked out from the system or the date and time from which the user is locked in again according to the lockout status shown in the 'Lockout Status' field. Displayed format is: YYYY-MM-DD hh:mm
Lockout Status	Shows the lockout status of the user from the possible values: ❙ Yes ❙ No
Parent BIC	Shows the parent BIC of the party related to the user. Reference for error message [▶]: ❙ DRD7007

User	
Party BIC	Shows the BIC of the party related to the user. Reference for error message [ ]: ▌ DRD7007
Party Short Name	Shows the short name of the party related to the user.
Party Type	Shows the party type of the party related to the user from the possible values: ▌ Service operator ▌ Payment bank ▌ National Central Bank (NCB)

Buttons

Edit	This function enables you to edit the details of the selected system user. Next screen: ▌ *User – edit* screen [▶] If the status of the selected user is already set to 'Deleted', this function is not available.
Delete	This function enables you to delete the selected system user, after confirmation. Upon clicking on the *delete* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ▌ *Users – search/list* screen [▶] If the status of the selected user is already set to 'Deleted', this function is not available. References for error messages [ ]: ▌ DRD7001 ▌ DRU7003

Revisions	This function enables you to display the revisions of the selected CRDM user. Next screen: ❚ *Revisions/audit trail – list* screen [▶]
Restore	This function enables you to restore a previously deleted user. Upon clicking on the *restore* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❚ *Users – search/list* screen [▶] If the status of the selected user is already set to 'Active', this function is not available. References for error messages [▶]: ❚ DRD7001 ❚ DRD7002 ❚ DRD7004 ❚ DRD7005 ❚ DRD7007 ❚ DRD7008
User Certificate Distinguished Name Links	This function enables you to access the *User certificate distinguished name links* screen for the selected CRDM user. Next screen: ❚ *User certificate distinguished name links – search/list* screen [▶]

2.3.3.13 User – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding users. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. This screen enables lockouts to be applied to and removed from users in order to prevent or allow them to enter the system. User data can be maintained by CB and Payment Bank users.

You can use this screen either in 2-eyes or in 4-eyes mode.

Screen Access

❚ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *new* or *edit* button

❚ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *search and/or details* button >> *User – details* screen >> Click on the *edit* button

Privileges

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

❚ Create user

❚ Update user

References

User Instructions Part

This screen is part of the following business scenario:

❚ Create a new user [▶]

Screenshot
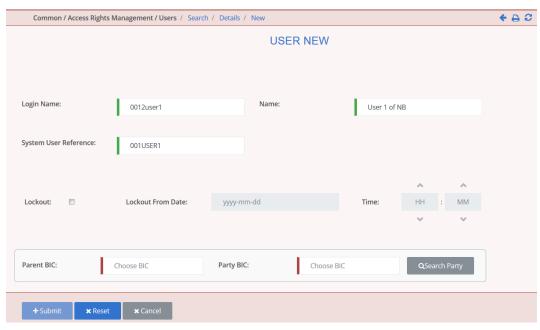
Illustration 54: User – new screen

Field Description

User	
Login Name	Enter the login name of the user. Required format is: max. 35 characters (SWIFT-x) References for error messages [▶]: ❚ DRC7006 ❚ DRU7008
Name	Enter the name of the user. Required format is: max. 127 characters (SWIFT-x)

User

System User Reference	Enter the unique system user reference associated to the user. Required format is: max. 35 characters (SWIFT-x). References for error messages [▶]: ❚ DRC7007 ❚ DRU7005
Lockout Status since	Shows the date and time from which the user is locked out of the system. Displayed format is: YYYY-MM-DD hh:mm
	If the 'Lockout Status Since' field is selected, this field is a mandatory enter field in the *new* screen. You can enter or edit the lockout date and time. Required format is: YYYY-MM-DD hh:mm The default value is the current date. If the 'Lockout Status' field is deselected this field is read-only and empty.
Lockout Status	Select the lockout status. When the select field is selected the user cannot log into the system as from the date specified in the 'Lockout Status since' field.
Parent BIC	Shows the parent BIC of the party related to the user.
	This field is a mandatory enter field in the *new* screen. Required format is: max. 11 characters (SWIFT-x) Reference for error message [ ]: ❚ DRC7005
Party BIC	Shows the BIC of the party related to the user.
	This field is a mandatory enter field in the *new* screen. Required format is: max. 11 characters (SWIFT-x) Reference for error message [▶]: ❚ DRC7005

Buttons

Submit	This function enables you to create or edit a system user according to the information entered in the fields. Upon clicking on the *submit* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ▮ *User – details* screen [▸] References for error messages [▸]: ▮ DRC7001 ▮ DRC7005 ▮ DRC7006 ▮ DRC7007 ▮ DRU7001 ▮ DRU7003 ▮ DRU7005 ▮ DRU7008
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ▮ *Users – search/list* screen [▸]
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ▮ *User – new/edit* screen

2.3.3.14 User Certificate Distinguished Name Links – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for user certificate distinguished name links. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

There is no usage restriction for this screen.

Screen Access

❙ Common >> Access Rights Management >> User Certificate Distinguished Name Links

❙ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *user certificate distinguished name links* button

❙ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *search* and/or the *details* button >> *User – details* screen >> Click on the *user certificate distinguished name links* button

❙ Common >> Access Rights Management >> Certificate Distinguished Names >> *Certificate distinguished names – search/list* screen >> Click on the *user certificate distinguished name links* button

Privileges

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

❙ Delete user certificate distinguish name link

❙ System user link query

References

User Instructions Part

This screen is part of the following business scenario:

❙ Create a new user certificate distinguished name link [▶]

Screenshot
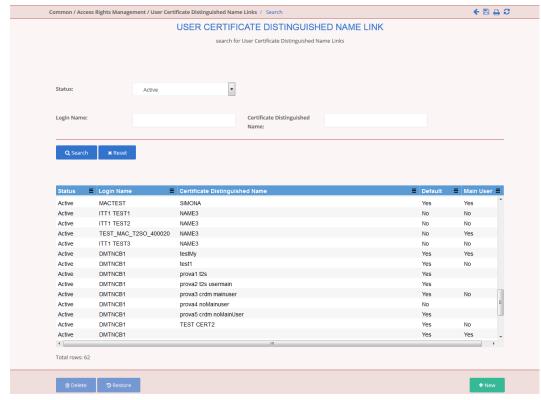
Illustration 55: User certificate distinguished name links – search/list screen

Field Description

User Certificate Distinguished Name Links – Search Criteria	
Status	Select the status of the user certificate distinguished name link from the possible values: ▌ All ▌ Active (default value) ▌ Deleted References for error messages [▶]: ▌ DRD0002 ▌ DRD0007
Login Name	Enter the login name of the user. Required format is: max. 35 characters (SWIFT-x) If you have accessed this screen via the *users – search/list* or *user – details* screen, this field is already filled in. References for error messages [▶]: ▌ DRD0003 ▌ DRD0005
Certificate Distinguished Name	Enter the distinguished name of the certificate. Required format is: max. 256 characters (UTF-8 except '>', '<', '&') If you have accessed this screen via the *certificate distinguished names – search/list* screen, this field is already filled in. References for error messages [▶]: ▌ DRD0004 ▌ DRD0005

User Certificate Distinguished Name Links – List	
Status	Shows the status of the user certificate distinguished name link from the possible values: ❚ Active ❚ Deleted If the status is set to 'Deleted', the selected user certificate distinguished name link cannot be deleted. If the status is set to 'Active', the selected user certificate distinguished name link cannot be restored. References for error messages [ ]: ❚ DRD0002 ❚ DRD0007
Login Name	Shows the login name of the user. References for error messages [ ]: ❚ DRD0003 ❚ DRD0005
Certificate Distinguished Name	Shows the distinguished name of the certificate linked to the user. References for error messages [ ]: ❚ DRD0004 ❚ DRD0005
Default	Shows whether the displayed certificate is the default certificate for the user. Reference for error message [ ]: ❚ DRD0006
Main User	❚ Shows the main certificate for the TIPS User Reference for error message [ ]: ❚ DRD0008

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. Next screen: **I** *User certificate distinguished name links – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: **I** *User certificate distinguished name links – search/list* screen
New	This function enables you to create a new link between an existing user and an existing certificate distinguished name. Next screen: **I** *User certificate distinguished name link – new* screen [▶]

Restore	This function enables you to restore a previously deleted user certificate distinguished name link. Upon clicking on the *restore* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❙ *User certificate distinguished name links – search/list* screen If the status of the selected user certificate distinguished name link is already set to 'Active', this function is not available. References for error messages [▶]: ❙ DRD0001 ❙ DRD0003 ❙ DRD0004 ❙ DRD0005 ❙ DRD0006 ❙ DRD0007 ❙ DRD0008
Revisions	This function enables you to display the revisions of the selected user certificate distinguished name link. Next screen: ❙ *Revisions/audit trail – list* screen [▶]
Delete	This function enables you to delete the selected user certificate distinguished name link, after confirmation. Upon clicking on the *delete* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: ❙ *User certificate distinguished name links – search/list* screen If the status of the selected user certificate distinguished name link is already set to 'Active', this function is not available.

	References for error messages [ ]: ❙ DRD0001 ❙ DRD0002

2.3.3.15 User Certificate Distinguished Name Link – New Screen

Context of Usage   This screen contains a number of fields regarding user certificate distinguished name links. You can enter new data. Afterwards you can proceed further by clicking on the buttons below. You can use this screen either in 2-eyes or in 4-eyes mode.

There is no usage restriction for this screen.

Screen Access   ❙ Common >> Access Rights Management >> User Certificate Distinguished Name Links >> *User certificate distinguished name links search/list* screen >> Click on the *new* button

❙ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *user certificate distinguished name links* button >> *User certificate distinguished name links – search/list* screen >> Click on the *new* button

❙ Common >> Access Rights Management >> Users >> *Users – search/list* screen >> Click on the *search* and/or the *details* button >> *User – details* screen >> Click on the *user certificate distinguished name links* button >> *User certificate distinguished name links – search/list* screen >> Click on the *new* button

❙ Common >> Access Rights Management >> Certificate Distinguished Names >> *Certificate distinguished names – search/list* screen >> Click on the *user certificate distinguished name links* button >> *User certificate distinguished name links – search/list* screen >> Click on the *new* button

Privileges   To use this screen, you need the following privilege [ ]:

❙ Create user certificate distinguish name link

References   **User Instructions Part**

This screen is part of the following business scenario:

❙ Create a new user certificate distinguished name link [ ]

Screenshot

Common / Access Rights Management / User Certificate Distinguished Name Links / Search / New

CERTIFICATE DISTINGUISHED NAME NEW

Login Name: Choose Login name...   Certificate Distinguished Name: Choose Certificate DN...

Default: ☐   Main User: ☐

+ Submit   ✕ Reset   ✕ Cancel
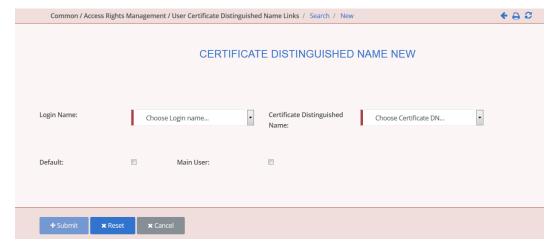
Illustration 56: User certificate distinguished name link – new screen

Field Description

User Certificate Distinguished Name Links	
Login Name	Select the login name of the user that you want to link to the certificate from the drop-down menu. References for error messages [▶]: ▌ DRC0002 ▌ DRC0003 ▌ DRC0005
Certificate Distinguished Name	Select the distinguished name of the certificate that you want to link to the user from the drop-down menu. References for error messages [▶]: ▌ DRC0004 ▌ DRC0005
Default	Select whether this should be the default certificate for the selected user. Reference for error message [▶]: ▌ DRC0006
Main User	Select whether this should be the main certificate for the TIPS User. Reference for error message [ ]: ▌ DRC0007

Buttons

Submit	This function enables you to create a new user certificate distinguished name link. Upon clicking on the *submit* button you will be asked to enter your PIN for digital signature purposes (NRO). With the entry of the PIN, CRDM attaches a digital signature to the instruction entered by the CRDM actor. Next screen: **▌** *User certificate distinguished name link – new* screen References for error messages [▶]: **▌** DRC0001 **▌** DRC0002 **▌** DRC0003 **▌** DRC0004 **▌** DRC0005 **▌** DRC0006 **▌** DRC0007
Reset	This function enables you to set all fields to default value and it blanks out all optional fields. Next screen: **▌** *User certificate distinguished name link – new* screen
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: **▌** *User certificate distinguished name links – search/list* screen [▶]

2.3.4 Message and Reports

2.3.4.1 Message Subscription Rule Sets – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for message subscription rule sets. The search results will be displayed in a list, which is sorted by the values of the 'Rule Set Identification' column in ascending order (default setting). After selecting an entry, you can proceed further by clicking on the buttons below.

There is no usage restriction for this screen.

Screen Access

❙ Common >> Messages and Reports >> Message Subscription Rule Sets

Privileges

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

❙ Message subscription rule set list query

❙ Message subscription rule set details query

❙ Delete message subscription rule set

❙ Delete message subscription rule

References

User Instructions Part

This screen is part of the following business scenario:

❙ Create a new message subscription rule set [▶]

Screenshot

Illustration 57: Message subscription rule sets – search/list screen

Field Description

Message Subscription Rule Sets – Search Criteria	
Status	Select the status of the message subscription rule set from the possible values: ▮ All ▮ Active (default value) ▮ Deleted References for error messages [▶]: ▮ DRDE003 ▮ DRDE044
Name	Enter the name of the rule set. Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ▮ DRDE200
Valid From – from	Enter the lower bound of the search range for the date from which the message subscription rule set is valid or use the *calendar* icon. Required format is: YYYY-MM-DD
Valid From – to	Enter the upper bound of the search range for the date from which the message subscription rule set is valid or use the *calendar* icon. Required format is: YYYY-MM-DD
Valid To – from	Enter the lower bound of the search range for the date until which the message subscription rule set is valid or use the *calendar* icon. Required format is: YYYY-MM-DD
Valid To – to	Enter the upper bound of the search range for the date until which the message subscription rule set is valid or use the *calendar* icon. Required format is: YYYY-MM-DD

Message Subscription Rule Sets – Search Criteria	
Positive/Negative Parameter Set	Select in which way the message subscription rule set must be used from the possible values: ❚ All (default value) ❚ Positive ❚ Negative
Parent BIC	Enter the parent BIC of the interested party. Required format is: max. 11 characters (SWIFT-x) Reference for error message [ ]: ❚ DRDE002
Party BIC	Enter the BIC of the interested party. Required format is: max. 11 characters (SWIFT-x) Reference for error message [ ]: ❚ DRDE002

Message Subscription Rule Sets – List	
Status	Shows the status of the message subscription rule set from the possible values: ❚ Active ❚ Deleted If the status is set to 'Deleted', the selected message subscription rule set cannot be edited or deleted and the related message subscription rules cannot be shown. If the status is set to 'Active', the selected message subscription rule set cannot be restored. References for error messages [ ]: ❚ DRDE003 ❚ DRDE044
Rule Set Identification	Shows the technical identification of the message subscription rule set.
Name	Shows the name of the rule set. Reference for error message [ ]:

Message Subscription Rule Sets – List
▌ DRDE200

Valid from	Shows the date from which the message subscription rule set is valid. Displayed format is: YYYY-MM-DD References for error messages [▶]: ▌ DRDE003 ▌ DRDE006
Valid to	Shows the date until which the message subscription rule set is valid. Displayed format is: YYYY-MM-DD References for error messages [▶]: ▌ DRDE003 ▌ DRDE006
Positive/Negative	Shows in which way the message subscription rule set must be used from the possible values: ▌ Positive ▌ Negative
Creator Party Parent BIC	Shows the parent BIC of the creator party.
Creator Party Party BIC	Shows the BIC of the creator party.
Interested Party: Parent BIC	Shows the parent BIC of the interested party. Reference for error message [▶]: ▌ DRDE002
Interested Party: BIC	Shows the BIC of the interested party. Reference for error message [ ]: ▌ DRDE002

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed in a list on the same screen. If the search retrieves a single record, the *details* screen is displayed directly. Next screens: ❚ *Message subscription rule sets – search/list* screen [▶] ❚ *Message subscription rule set – details* screen [▶]
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Message subscription rule sets – search/list* screen [▶]
Edit	This function enables you to edit the details of the selected message subscription rule set. Next screen: ❚ *Message subscription rule set – edit* screen [▶] If the status of the selected message subscription rule set is already set to 'Deleted', this function is not available.
Delete	This function enables you to delete the selected message subscription rule set, after confirmation. Next screen: ❚ *Message subscription rule sets – search/list* screen [▶] If the status of the selected message subscription rule set is already set to 'Deleted', this function is not available. References for error messages [▷]: ❚ DRDE001 ❚ DRDE003 ❚ DRDE040
Restore	This function enables you to restore a previously deleted message subscription rule set. Next screen: ❚ *Message subscription rule sets – search/list* screen If the status of the selected message subscription rule set

	is already set to 'Active', this function is not available. References for error messages [▶]: ▍ DRDE001 ▍ DRDE002 ▍ DRDE006 ▍ DRDE044 ▍ DRDE200
Details	This function enables you to display the details of the selected message subscription rule set. Next screen: ▍ *Message subscription rule set – details* screen [▶]
Revisions	This function enables you to display the revisions of the selected message subscription rule set. Next screen: ▍ *Revisions/audit trail – list* screen [▶]
New	This function enables you to create a new message subscription rule set. Next screen: ▍ *Message subscription rule set – new* screen [▶]

2.3.4.2 Message Subscription Rule Set – Details Screen

Context of Usage This screen displays detailed information on the selected message subscription rule. It also contains a number of fields regarding message subscription rules, for which you can enter new data or edit existing data. You can check the data and proceed further by clicking on the buttons below. There is no usage restriction for this screen.

Screen Access Common >> Messages and Reports >> Message Subscription Rule Set >> *Message Subscription Rule Set -* s*earch/list* screen >> Click on the *search* and/or *details* button

Privileges

To use this screen you need the following privilege [▶]:

▍ Message Subscription Rule Set Details Query

▍ Delete Message Subscription Rule Set

References

User Instructions Part

This screen is not part of a business scenario

Screenshot
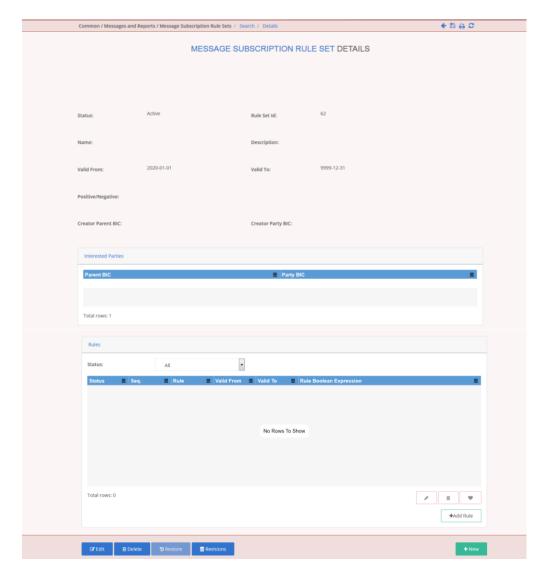
Illustration 58: Message subscription rule set – details screen

Field Description

Message Subscription Rule Set	
Status	Shows the status of the message subscription rule set from the possible values: ▌ Active ▌ Deleted
Rule Set Id	Shows the technical identification of the message subscription rule set.
Name	Shows the name of the message subscription rule set.
Description	Shows the description of the message subscription rule set.
Valid From	Shows the date from which the message subscription rule set is valid. Displayed format is: YYYY-MM-DD References for error messages [▶]: ▌ DRDE003 ▌ DRDE006
Valid To	Shows the date until which the message subscription rule set is valid. Displayed format is: YYYY-MM-DD References for error messages [▶]: ▌ DRDE003 ▌ DRDE006
Positive/Negative	Shows the way in which the message subscription rule set must be used from the possible values: ▌ Positive ▌ Negative
Creator Parent BIC	Shows the parent BIC of the interested party.
Creator Party BIC	Shows the BIC of the interested party.

Interested Parties

Parent BIC	Shows the parent BIC of the interested party.
	Reference for error message [ ]: ❚ DRDE002
Party BIC	Shows the BIC of the interested party.
	Reference for error message [ ]: ❚ DRDE002

Rules	
Status	Select the status of the Message subscription rule from the possible values: ❚ All (default value) ❚ Active ❚ Deleted
Seq.	Enter the sequence related to the message subscription rule. Required format is: Integer References for error messages [ ]: ❚ DRCF003 ❚ DRUF005
Rule	Shows the technical identification of the message subscription rule.
Valid From	Enter the date from which the message subscription rule is valid or use the calendar icon. Required format is: YYYY-MM-DD If the date is in the past, this field is read-only. References for error messages [ ]: ❚ DRCF006 ❚ DRUF006
Valid To	Enter the date until which the message subscription rule is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages []: ❚ DRCF007 ❚ DRUF007
Rule Boolean Expression	Shows the parameters applicable to the rule. The values are Message type, Cash Account and Currency.

Buttons		
Options	Information on functions (icons) can be found in Common Buttons and Icons.	
Add Rule	This function enables the user to add the Message Subscription Rule related to the selected rule set.	
Edit	This function enables the user to update the details of the selected Message Subscription Rule Set. This button is not visible in case of the deletion status of the shown item is "Deleted". Next screen: ❙ *Message subscription rule set – edit* screen [ ]	
Delete	This function enables you to delete the selected message subscription rule set, after confirmation. If the status of the selected message subscription rule set is already set to 'Deleted', this function is not available. References for error messages [ ]: ❙ DRDE001 ❙ DRDE003 ❙ DRDE040	
Restore	This function enables the user to restore a previously deleted item. This button is not visible in case of the deletion status of the shown item is "Active". Next screen: ❙ *Message subscription rule sets – search/list* screen [ ] References for error messages [ ]: ❙ DRDE001 ❙ DRDE002 ❙ DRDE006 ❙ DRDE044	
Revisions	This function enables you to display the revisions of the selected Message Subscription Rule Set.	
New	This function enables you to create a new message subscription rule set.	

Rules
Next screen:
▎ *Message subscription rule set – new* screen [ ]

2.3.4.3 Message Subscription Rule – New Screen

Context of Usage

This screen contains a number of fields regarding message subscription rules. You can enter new data. There is no usage restriction for this screen.

Screen Access

▎ Common >> Messages and Reports >> Message Subscription Rule Set >> *Message Subscription Rule Set - search/list* screen >> Click on the *search* button >> Click on the *details* button >> Click on the *add rule* button

Privileges

To use this screen you need the following privilege [▶]:

▎ Create message subscription rule set

▎ Update message subscription rule set

References

User Instructions Part

This screen is part of the following business scenario:

▎ Create a new message subscription rule [▶]

Screenshot
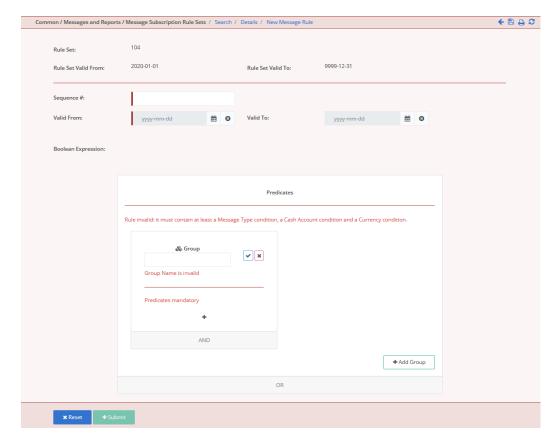
Illustration 59: Message subscription rule – new screen

Field Description

Message Subscription Rule	
Rule Set	Shows the technical identification of the message subscription rule set. References for error messages [▶]: ▮ DRCF001 ▮ DRCF003 ▮ DRCF005
Rule Set Valid From	Shows the date from which the message subscription rule is valid. Displayed format is: YYYY-MM-DD References for error messages [ ]: ▮ DRCF006 ▮ DRUF006
Rule Set Valid To	Shows the date until which the message subscription rule is valid. Required format is: YYYY-MM-DD References for error messages [▶]: ▮ DRCF007 ▮ DRUF007
Sequence #	Enter the sequence related to the message subscription rule. Required format is: Integer References for error messages [ ]: ▮ DRCF003 ▮ DRUF005
Valid From	Enter the date from which the message subscription rule is valid or use the calendar icon. Required format is: YYYY-MM-DD If the date is in the past, this field is read-only. References for error messages [▶]: ▮ DRCF006

Message Subscription Rule	
	▍ DRUF006
Valid To	Enter the date until which the message subscription rule is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages [ ]: ▍ DRCF007 ▍ DRUF007
Group	Enter the group of parameters related to a message subscription rule. You cannot insert an already used group name. References for error messages [ ]: ▍ DRCF300 ▍ DRUF300 This field is also available as a show field for existing records.

Buttons

Add Group	This function enables you to add the Message Type, the Currency and the Cash Account associated with the Message Subscription Rule
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ▍ *Message subscription rule set – new/edit* screen
Submit	This function enables you to create or edit a message subscription rule. References for error messages [ ]: ▍ DRCF001 ▍ DRCF002 ▍ DRCF005 ▍ DRCF006 ▍ DRCF007 ▍ DRCF300

Message Subscription Rule
❙ DRUF001
❙ DRUF003
❙ DRUF004
❙ DRUF005
❙ DRUF006
❙ DRUF007
❙ DRUF050
❙ DRUF300

2.3.4.4 Message Subscription Rule Set – New/Edit Screen

Context of Usage
This screen contains a number of fields regarding message subscription rule sets. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. You can use this screen either in 2-eyes or in 4-eyes mode. There is no usage restriction for this screen.

Screen Access
❙ Common >> Messages and Reports >> Message Subscription Rule Set >> *Message Subscription Rule Set - s*earch/list screen >> Click on the *new* or *edit* button

Privileges
To use this screen you need the following privilege [▶]:

❙ Create Message Subscription Rule

❙ Update Message Subscription Rule

References
User Instructions Part

This screen is part of the following business scenario:

❙ Create a new message subscription rule set [▶]

Screenshot
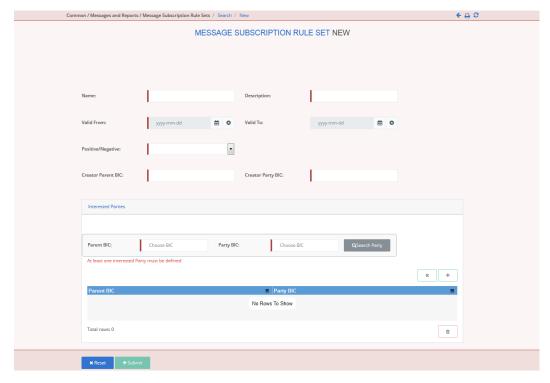
Illustration 60: Message subscription rule set – new screen

Field Description

Message Subscription Rule Set	
Name	Enter the name assigned to the message subscription rule set. Required format is: max. 35 characters (SWIFT-x) References for error messages [▶]: ❚ DRCE200 ❚ DRUE200
Description	Enter the description assigned to the message subscription rule set. Required format is: max. 350 characters (SWIFT-x)
Valid from	Enter the date from which the message subscription rule set is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages [▶]: ❚ DRCE009 ❚ DRCE010 ❚ DRUE205 ❚ DRUE206 ❚ DRUE207 If the date is in the past, this field is read-only.
Valid to	Enter the date until which the message subscription rule set is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages [▶]: ❚ DRCE010 ❚ DRUE206 ❚ DRUE207
Positive/Negative	Select the way in which the message subscription rule set must be used from the possible values: ❚ Positive ❚ Negative
Creator Parent BIC	Shows the parent BIC of the creator party.

Message Subscription Rule Set	
	This field only available if you are the Service operator or a CB. Reference for error message [ ]: ❚ DRCE006 If the user is Service Operator, the field is enabled. If the user is NCB user, this field contains the parent BIC of the party the user is performing the operation belongs to. Required format is: max. 11 characters (SWIFT-x)
Creator Party BIC	Shows the BIC of the creator party. This field is only available if you are the Service operator or a CB user. Reference for error message [▶]: ❚ DRCE006 This field is mandatory in the new screen. You can choose to either enter the BIC of the creator party or to select it from the suggested items in the drop-down menu. Required format is: max. 11 characters (SWIFT-x)
Interested Parties	
Parent BIC	Enter the Parent BIC of the Interested Party. Required format is: max. 11 characters (SWIFT-x) References for error messages [▶]: ❚ DRCE001 ❚ DRCE002 ❚ DRCE005 ❚ DRUE004 ❚ DRUE005 ❚ DRUE007 ❚ DRUE010
Party BIC	Enter the Parent BIC of the Interested Party. Required format is: max. 11 characters (SWIFT-x) References for error messages [ ]:

Message Subscription Rule Set
▌ DRCE001
▌ DRCE002
▌ DRCE005
▌ DRUE004
▌ DRUE005
▌ DRUE007
▌ DRUE010

Buttons

Search Party	This function enables the user to activate "Parties – Select/List" screen and perform a search of "Parent BIC" and "Party BIC".
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ▌ *Message subscription rule set – new/edit* screen
Submit	This function enables you to create or edit a message subscription rule set. Next screen: ▌ *Message subscription rule set – details* screen [▷] References for error messages [▷]: ▌ DRCE001 ▌ DRCE002 ▌ DRCE005 ▌ DRCE009 ▌ DRCE010 ▌ DRCE100 ▌ DRCE200 ▌ DRUE001 ▌ DRUE003 ▌ DRUE004 ▌ DRUE005 ▌ DRUE006 ▌ DRUE007

Message Subscription Rule Set
❚ DRUE008
❚ DRUE010
❚ DRUE200
❚ DRUE205
❚ DRUE206
❚ DRUE207

2.3.4.5 Report Configurations – Search/List Screen

Context of Usage

This screen contains a number of search fields. By inputting the relevant data, you can search for report configurations. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below. There is no usage restriction for this screen.

Screen Access

❚ Common >> Messages and Reports >> Report Configurations

To use this screen you need the following privilege [▶]:

Privileges

❚ Report Configuration List Query

❚ Delete Report Configuration

References

User Instructions Part

This screen is part of the following business scenario:

❚ Create a new Report configuration [▶]

Screenshot
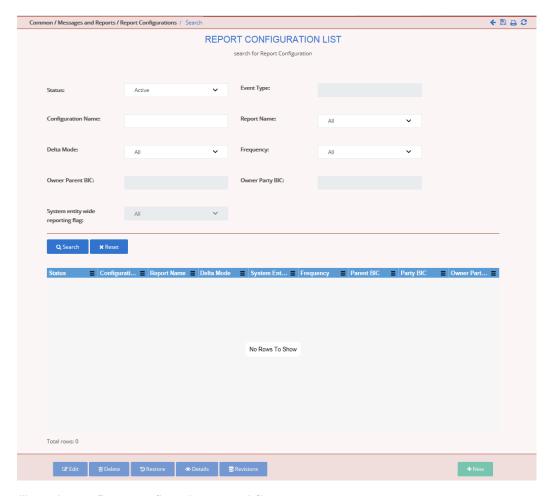
Illustration 61: Report configuration – search/list screen

Field Description

Report configuration – Search criteria	
Status	Select the status of the Report from the possible values: ▌ All (default value) ▌ Active ▌ Deleted
Event type	Enter the code of the event type that triggers the report. This field is not relevant for TIPS and therefore disabled.
Configuration Name	Enter the name of the report configuration. Required format is: max. 35 characters (SWIFT-x) Reference for error message [ ]: ▌ DRDV008
Report Name	Select the name of the report type from the possible values: ▌ All (default value)

Report configuration – Search criteria	
	▌ TIPS Statement of Account Turnover ▌ TIPS Statement of Accounts ▌ TIPS Directory ▌ TIPS Directory Update
Delta mode	Select whether the recipient receives the relevant report in delta mode or in full mode from the possible values: ▌ All (default value) ▌ Yes ▌ No
Frequency	Select the frequency (expressed in hours) with which the report is generated. Possible values are: ▌ All (default value) ▌ 3 ▌ 6 ▌ 12
Owner Parent BIC	Select the BIC of the party which owns the report configuration from the drop-down menu. This field is not relevant for TIPS and therefore disabled.
Owner Party BIC	Select the BIC of the party which owns the report configuration from the drop-down menu. This field is not relevant for TIPS and therefore disabled.
System Entity Wide reporting flag	Select whether the report should include information about the entire system entity. This field is not relevant for TIPS and therefore disabled.

Report configuration – List	
Status	Shows the status of the Report configuration from the possible values: ▌ Active ▌ Deleted If the status is set to 'Deleted', the selected Report

	configuration cannot be deleted or edited. If the status is set to 'Active', the selected Report configuration cannot be restored.
Configuration Name	Shows the name of the report configuration. Reference for error message [ ]:
	▌ DRDV008
Report Name	Shows the name of the report type from the possible values:
	▌ TIPS Statement of Account Turnover
	▌ TIPS Statement of Accounts
	▌ TIPS Directory
Delta Mode	Shows whether the recipient gets the relevant report in delta mode or in full mode.
System entity wide reporting flag	Shows whether the report should include information about the entire system entity.
Frequency	Shows the frequency with which the report is generated.
Parent BIC	Shows the parent BIC of the party which owns the report configuration. References for error messages [ ]:
	▌ DRDV004
	▌ DRDV005
Party BIC	Shows the BIC of the party which owns the report configuration. References for error messages [ ]:
	▌ DRDV004
	▌ DRDV005
Owner Party Short Name	Shows the short name of the party which owns the report configuration.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. Next screens: ❚ *Report Configurations – search/list* screen ❚ *Report configuration – details* screen []
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❚ *Report Configurations – search/list* screen

Edit	This function enables you to edit the details of the selected report configuration. Next screen: ❚ *Report configuration – edit* screen [◌] If the status is already set to 'Deleted', this function is not available.
Delete	This function enables you to delete the selected report configuration, after confirmation. Next screen: ❚ *Report configurations – search/list* screen If the status is already set to 'Deleted', this function is not available. References for error messages [ ]: ❚ DRDV001 ❚ DRDV020 ❚ DRDV060
Restore	This function enables you to restore a previously deleted report configuration. Next screen: ❚ *Report configurations – search/list* screen If the status is already set to 'Active', this function is not available. References for error messages [◌]: ❚ DRDV001 ❚ DRDV004 ❚ DRDV005 ❚ DRDV008 ❚ DRDV030 ❚ DRDV050 ❚ DRDV110
Details	This function enables you to display the details of the selected

	report configuration. Next screen: ❚ *Report configuration – details* screen [ ]
Revisions	This function enables you to display the revisions of the selected report configuration. Next screen: ❚ *Revisions/audit trail – list* screen [▶]
New	This function enables you to create a new report configuration. Next screen: ❚ *Report configuration – new* screen [▶]

2.3.4.6 Report Configuration – Details Screen

Context of Usage This screen displays detailed information on the selected report configuration. You can check the data and proceed further by clicking on the buttons below.

There is no usage restriction for this screen.

Screen Access ❚ Common >> Messages and Reports >> Report Configurations >> *Report Configurations - search/list* screen >> Click on the *search* and/or *details* button

Privileges To use this screen, you need the following privileges [▶]:

❚ Report Configuration Details Query

❚ Delete Report Configuration

Screenshot

Common / Messages and Reports / Report Configurations / Search / Details

REPORT CONFIGURATION DETAILS

Status:	Active	Owner Parent BIC:	NCBXFIRR001
Owner Party BIC:	PBBKFIRR102	Owner Party Short Name:	NCBXFI PBR102
Configuration Name:	NCBXFI PBR102 SOAT	Configuration Description:	NCBXFI PBR102 SOAT
Delta Mode:	No	Report Name:	TIPS Statement of Account Turnover
System entity wide reporting flag:	No	Frequency:	0

Report Configuration Party Links

Parent BIC	Party BIC	Party Shor...	Push Mode	Scheduled...	Event Type...	Currency	Valid From	Valid To
NCBXFIRR001	PBBKFIRR102	NCBXFI PBR102	Yes				2018-03-01	9999-12-31

Total rows: 1

Edit   Delete   Restore   Revisions   + New

Illustration 62: Report Configuration – details screen

Field Description

Report configuration	
Report configuration	
Status	Shows the status from the possible values: ❚ Active ❚ Deleted If the status is set to 'Deleted', the selected report configuration cannot be deleted or edited. If the status is set to 'Active', the selected report configuration cannot be restored. References for error messages [ ]: ❚ DRDV020 ❚ DRDV030
Parent BIC	Shows the parent BIC of the party which owns the report configuration. Reference for error message [ ]: ❚ DRDV004
Party BIC	Shows the BIC of the party which owns the report configuration. Reference for error message [ ]: ❚ DRDV004
Party Short Name	Shows the short name of the party which owns the report configuration.
Configuration Name	Shows the name of the report configuration. Reference for error message [ ]: ❚ DRDV008
Configuration Description	Shows the description of the report configuration.
Delta Mode	Shows whether the recipient receives the relevant report in delta mode or in full mode.
Report name	Shows the name of the report from the possible values: ❚ TIPS Statement of Account Turnover

Report configuration	
	▎ TIPS Statement of Accounts ▎ TIPS Directory
Frequency	Shows the frequency with which the recipient gets the report
System entity wide reporting flag	Shows whether the report should include information about the entire system entity.
Report Configuration Party Links	
Parent BIC	Shows the parent BIC of the party entitled to receive the report. Reference for error message [▸]: ▎ DRDV005
Party BIC	Shows the BIC of the party entitled to receive the report. Reference for error message [ ]: ▎ DRDV005
Party Short Name	Shows the short name of the party entitled to receive the report.
Push Mode	Shows whether the party will receive the report in push mode or not.
Execution Time	Shows the time of execution of the report. Displayed format is: hh:mm
Currency Code	Shows the currency code associated to the report configuration and to the event This field is not relevant for TIPS and therefore disabled.
Valid From	Shows the date from which the report configuration is valid. Displayed format is: YYYY-MM-DD References for error messages [▸]: ▎ DRDV050 ▎ DRDV060

Report configuration	
Valid To	Shows the date until which the report configuration is valid. Displayed format is: YYYY-MM-DD References for error messages [ ]: ❙ DRDV050 ❙ DRDV060

Buttons

Edit	This function enables you to edit the details of the selected report configuration. Next screen: ❙ *Report configuration – edit* screen [▶] If the status is already set to 'Deleted', this function is not available.
Delete	This function enables you to delete the displayed report configuration. Next screen: ❙ *Report configurations – search/list* screen [ ] If the status is already set to 'Deleted', this function is not available. References for error messages [ ]: ❙ DRDV001 ❙ DRDV020 ❙ DRDV060
Revisions	This function enables you to display the revisions of the selected report configuration. Next screen: ❙ *Revisions/audit trail – list* screen [▶]
Restore	This function enables you to restore a previously deleted report configuration. Next screen: ❙ *Report configurations – search/list* screen [ ]

	If the status is already set to 'Active', this function is not available.
	References for error messages [ ]:
	▌ DRDV001
	▌ DRDV004
	▌ DRDV005
	▌ DRDV008
	▌ DRDV030
	▌ DRDV050

2.3.4.7 Report Configuration – New/Edit Screen

Context of Usage

This screen contains a number of fields regarding report configurations. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below.

Screen Access

▌ Common >> Messages and Reports >> Report Configurations >> *Report Configurations – search/list* screen >> Click on the *new* or *edit* button

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

Privileges

▌ Create Report Configuration

▌ Update Report Configuration

Screenshot

Common / Messages and Reports / Report Configurations / Search / New

REPORT CONFIGURATION NEW

Owner Parent BIC: SYSENTT2SX1	**Owner Party BIC:** SYSENTT2SX1
Configuration Name: Report configurationTEST	**Configuration Description:** Report configurationTEST
Report Name: TIPS Statement of Accounts	**Delta Mode:** ☐
Frequency:	**System Entity Wide Reporting Flag:** ☐

Party Links

Opting Parent BIC: SYSENTT2SX1	**Opting Party BIC:** SYSENTT2SX1
Push Mode: ☑	
Valid From Date: 2018-04-19	**Valid To Date:** yyyy-mm-dd

Opting Paren...	Opting Party ...	Push Mode	Scheduled Ti...	Event Type	Currency	Valid From	Valid To
				No Rows To Show			

Total rows: 0

+ Submit   ✗ Reset   ✗ Cancel

Illustration 63: Report configuration – new/edit screen

Field Description

Report configuration	
Owner Parent BIC	This field is not relevant for TIPS and therefore disabled.
Owner Party BIC	This field is not relevant for TIPS and therefore disabled.
Configuration Name	Shows the name of the report configuration. Reference for error message [⧉]: ❚ DRCV008 This field is a mandatory enter field in the new screen. Required format is: max. 35 characters (SWIFT-x)
Configuration Description	Shows the description of the report configuration. This field is a mandatory enter field in the new screen. Required format is: max. 350 characters (SWIFT-x)
Report Name	Shows the name of the report type from the possible values: ❚ TIPS Statement of Account Turnover ❚ TIPS Statement of Accounts ❚ TIPS Directory Reference for error message [⧉]: ❚ DRCV120
Delta Mode	Shows whether the recipient receives the relevant report in delta mode or in full mode. This field is a select field in the new screen. The option can be selected only in case the linked report name has the delta availability set to true.
Frequency	Select the time slots, from a predefined list, when the report is provided. This field is not enabled when the chosen Report Name is TIPS Directory Possible Values are: ❚ 3 ❚ 6 ❚ 12 References for error message [⧉]: ❚ DRCV130

Report configuration	
	▌ DRUV130
System Entity Wide Reporting Flag	Shows whether the report should include information about the entire system entity. Reference for error message [ ]: ▌ DRCV030 This field is select field in the new screen. This field is not relevant for TIPS and therefore disabled.
Opting Parent BIC	If the linked Report Name is a TIPS Report, the field is filled automatically with the Parent BIC of the Owner Party. References for error messages [ ]: ▌ DRCV005 ▌ DRUV005
Opting Party BIC	If the linked Report Name is a TIPS Report, the field is filled automatically with the Party BIC of the Owner Party. References for error messages [ ]: ▌ DRCV005 ▌ DRUV005
Push Mode	Select whether the party will receive the report in push mode or not. You can add, edit or remove only 10 rows at a maximum. This field is also available as show field for existing records. Reference for error messages [ ]: ▌ DRUV120 If the linked Report Name is a TIPS Report, the field is automatically set to TRUE.
Valid From	Enter the date from which the Report configuration is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages [ ]: ▌ DRCV040

Report configuration

	▌ DRUV020
	▌ DRUV030
	▌ DRUV040
Valid To	Enter the date until which the cash account restriction is valid or use the calendar icon.
	Required format is: YYYY-MM-DD
	References for error messages [▶]:
	▌ DRCV050
	▌ DRUV020
	▌ DRUV040

Buttons

Submit	This function enables you to create or edit a *Report Configuration.*
	Next screen:
	❙ *Report Configuration – details* screen [▶]
	References for error messages [▶]:
	❙ DRCV001
	❙ DRCV004
	❙ DRCV005
	❙ DRCV008
	❙ DRCV020
	❙ DRCV030
	❙ DRCV040
	❙ DRCV050
	❙ DRCV070
	❙ DRCV080
	❙ DRCV110
	❙ DRCV120
	❙ DRCV130
	❙ DRCV140
	❙ DRUV001
	❙ DRUV003
	❙ DRUV005
	❙ DRUV010
	❙ DRUV020
	❙ DRUV030
	❙ DRUV040
	❙ DRUV070
	❙ DRUV110
	❙ DRUV120
	❙ DRUV130
Reset	This function enables you to set all fields to default value and blanks out all optional fields.
	Next screen:

	Report Configuration – new/edit screen
Cancel	This function enables you to cancel the process and return to the previous screen.
	Next screen:
	Report Configuration – search/list screen [▶]

2.3.5 Restriction Type Management

2.3.5.1 Restriction Types – Search/List Screen

Context of Usage   This screen contains a number of search fields. By inputting the relevant data, you can search for restriction types. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below. There is no usage restriction for this screen.

Screen Access   ❙ Common >> Market Specific Configuration >> Restriction Types

Privileges   To use this screen you need the following privilege [▶]:

❙ Market-Specific Restriction List Query

Screenshot
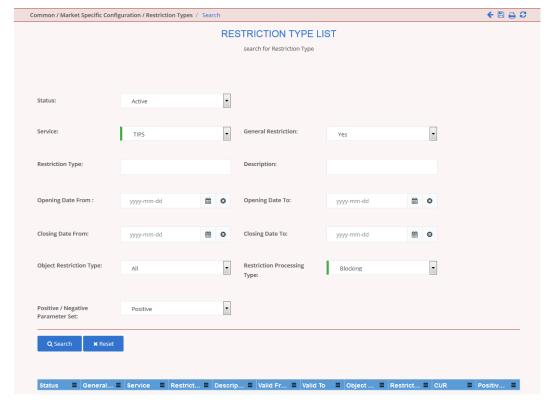
Illustration 64: Restriction Type– search/list screen

Field Description

Restriction Type – Search criteria	
Status	Select the status of the Restriction type from the possible values: ❙ All (default value) ❙ Active ❙ Deleted
Service	Select the list of possible services for which the rule is valid from the drop-down menu. The only available service is TIPS.
General restriction	Select the type of Restriction type to search from the possible values: ❙ All (default value) ❙ Yes ❙ No
Restriction type	Enter the restriction type to search. Required format is: max. 35 characters (SWIFT-x)
Description	Enter the restriction type description. Required format is: max. 350 characters (SWIFT-x)
Opening date from	Enter the lower bound for the opening date of the Restriction type or use the calendar icon. Required format is: YYYY-MM-DD
Opening date to	Enter the upper bound for the opening date of the Restriction type or use the calendar icon. Required format is: YYYY-MM-DD
Closing date from	Enter the lower bound for the closing date of the Restriction type or use the calendar icon. Required format is: YYYY-MM-DD
Closing date to	Enter the upper bound for the closing date of the Restriction type or use the calendar icon. Required format is: YYYY-MM-DD
Object restriction type	Select the Object restriction type from the drop-down menu from the possible values: ❙ All (default value)

Restriction Type – Search criteria	
	▎ Party ▎ Cash Account
Restriction processing type	Select the restriction processing type from the drop-down menu from the possible values: ▎ Blocking
Positive/Negative Parameter set	Select the Positive/Negative parameter set from the drop-down menu from the possible values: ▎ All (default value) ▎ Positive ▎ Negative

Restriction Type – List	
Status	Shows the status of the Report configuration from the possible values: ▎ Active ▎ Deleted
General restriction	Shows if the Restriction Types is created by CRDM Operator and visible to everyone (YES) or if it is created by the specific NCB or CSD (NO).
Service	Shows the service of the restriction. The only possible value is TIPS.
Restriction type	Shows the restriction type code.
Description	Shows the description of the restriction type.
Valid from	Shows the date from which the restriction type is valid. Displayed format: YYYY-MM-DD
Valid to	Shows the date until which the restriction type is valid. Displayed format: YYYY-MM-DD
Object restriction type	Shows the object on which the restriction type can be applied.

Restriction processing type	Shows the restriction processing type from the possible values:
	▍ Blocking
CUR	Shows the currency linked to the restriction type, if available.
Positive/Negative Parameter set	Shows whether the rules of the restriction type represent a positive or negative set of parameters.

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen.
	Next screen:
	▍ *Restriction types – search/list* screen
Reset	This function enables you to set default search criteria and blanks out all optional criteria.
	Next screen:
	▍ *Restriction types – search/list* screen

2.3.6 Network Configuration

2.3.6.1 Distinguished Name-BIC Routing – Search/List Screen

Context of Usage
This screen contains a number of fields regarding the relationship between a Distinguished Name and a BIC for which it is authorised to operate. By inputting the relevant data you can search for DN-BIC relations. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the buttons below.

Screen Access
▍ TIPS >> Common >> Network Configuration>> DN-BIC Routing

To use this screen you need the following privilege [▶]:

Privileges
▍ DN-BIC Routing Query

▍ Delete DN-BIC Routing

References

User Instructions Part

This screen is part of the following business scenario:

❙ Create a DN-BIC Routing configuration [▶]

Screenshot

DN-BIC ROUTING LIST

search for DN-BIC Routing

Status: Active	Distinguished Name:
BIC:	Direction: All
Valid From from: yyyy-mm-dd	Valid From to: yyyy-mm-dd
Valid To from: yyyy-mm-dd	Valid To to: yyyy-mm-dd

Q Search   ✖ Reset

Status	Distinguished Name	BIC	Direction	Valid From	Valid To

No Rows To Show

Total rows: 0

☑ Edit   🗑 Delete   ↻ Restore   📋 Revisions   ➕ New
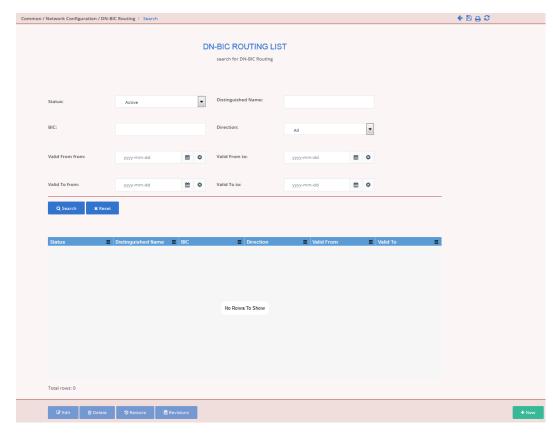
Illustration 65 – DN-BIC Routing – search screen

Field Description

Distinguished Name-BIC Routing – Search criteria	
Status	Select the status of the DN-BIC Routing from the possible values: ❙ All ❙ Active (default value) ❙ Deleted
Distinguished Name	Enter the Distinguished Name which is part of the couple DN-BIC to be searched. Required format is: max. 35 characters (SWIFT-x)
BIC	Enter the BIC which is part of the couple DN-BIC to be searched. Required format is: max. 11 characters (SWIFT-x)

Distinguished Name-BIC Routing – Search criteria	
Direction	Select the direction of the communication for which the DN-BIC Routing to be searched is set from the possible values: ▎ All ▎ Inbound ▎ Outbound
Valid From - from	Enter the lower bound for the Valid from of the DN-BIC routing link or use the calendar icon. Required format is: YYYY-MM-DD
Valid From - to	Enter the upper bound for the Valid from of the DN-BIC routing link or use the calendar icon. Required format is: YYYY-MM-DD The 'Opening Date – to' must be greater than the 'Opening Date – from'.
Valid To - from	Enter the lower bound for the Valid to of the DN-BIC routing link or use the calendar icon. Required format is: YYYY-MM-DD
Valid To - to	Enter the upper bound for the Valid to of the DN-BIC routing link or use the calendar icon. Required format is: YYYY-MM-DD

Distinguished Name-BIC Routing – List	
Status	Shows the status of the DN-BIC routing link from the possible values: ▎ Active ▎ Deleted If the status is set to 'Deleted', the selected DN-BIC routing link cannot be deleted or edited. If the status is set to 'Active', the selected DN-BIC routing link cannot be restored.
Distinguished name	Shows the Distinguished Name which is part of the searched couple DN-BIC.

Distinguished Name-BIC Routing – List	
BIC	Shows the BIC which is part of the searched couple DN-BIC.
Direction	Shows whether the link between the DN and the BIC authorises the DN to act as Originator (inbound routing) or as Beneficiary (outbound routing) for the Party.
Valid from	Shows the Valid from date of the DN-BIC Routing. Format is: YYYY-MM-DD
Valid to	Shows the Valid to date of the DN-BIC Routing. Format is: YYYY-MM-DD

Buttons

Search	This function enables you to start a search according to the criteria entered. The results are displayed on the same screen. Next screen: ❙ Distinguished Name-BIC routing – search/list screen References for error messages: [▶]: ❙ DRD8006 ❙ DRD8007
Reset	This function enables you to set default search criteria and blanks out all optional criteria. Next screen: ❙ Distinguished Name-BIC routing – search/list screen
Edit	This function enables the user to edit the details of the selected DN-BIC Routing.
Delete	This function enables the user to delete the selected DN-BIC Routing References for error messages: [▶] ❙ DRD8001 ❙ DRD8002
Restore	This function enables the user to restore a previously deleted element References for error messages: [▶] ❙ DRD8001 ❙ DRD8003 ❙ DRD8004 ❙ DRD8005
Revisions	This function enables the user to access the Revisions – Select/List screen related to the selected DN-BIC Routing
New	This function enables the user to create a new DN-BIC Routing. Next screen:

I Distinguished Name-BIC routing – New/edit screen

2.3.6.2 Distinguished Name-BIC Routing – New/Edit Screen

Context of Usage   This screen contains a number of fields regarding the Distinguished Name-BIC Routing. You can enter new data or edit existing data. Afterwards you can proceed further by clicking on the buttons below. NCBs can create DN-BIC Routing acting on behalf of their TIPS Participants. Payment Banks can create DN-BIC Routing for the BIC which currently identifies their own Party.

Screen Access   **I** TIPS >> Common >> Network Configuration>> *DN-BIC Routing – search/list* screen >> Click on the *new* or *edit* button

Privileges   To use this screen you need the following privileges [▶]:

I Create DN-BIC Routing

I Update DN-BIC Routing

Screenshot
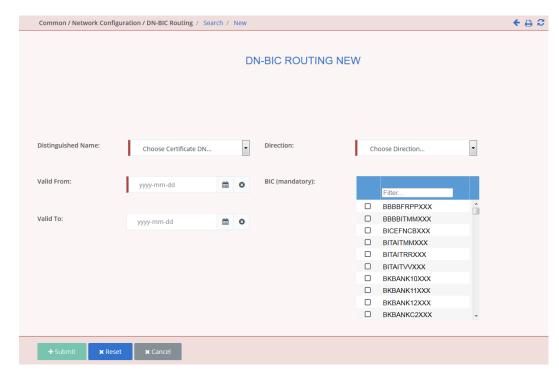
Illustration 66: DN-BIC Routing – new/edit screen

**Field
Description**

Distinguished Name-BIC Routing	
Distinguished Name	Choose the Distinguished Name to link to the BIC from the drop-down menu Reference for error messages [▶]: ❙ DRC8002
Direction	Choose the Direction to specify whether the link between the DN and the BIC authorises the DN to act as Originator (inbound routing) or as Beneficiary (outbound routing) from the drop-down menu References for error messages [▶]: ❙ DRC8006 ❙ DRU8006
Valid From	Enter the date from which the DN-BIC routing link is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages: [▶] ❙ DRC8004 ❙ DRU8003 ❙ DRU8004
Valid To	Enter the date until which the DN-BIC routing link is valid or use the calendar icon. Required format is: YYYY-MM-DD References for error messages: [▶] ❙ DRC8005 ❙ DRU8005
BIC	Enter the BIC to link to the chosen Distinguished Name. Required format is: max. 11 characters (SWIFT-x) References for error messages [▶]: ❙ DRC8003 ❙ DRC8007 ❙ DRU8007

Buttons

Submit	This function enables you to create or edit a DN-BIC routing link. Next screen: ❚ *Distinguished Name-BIC Routing – Search/list* screen [▶] References for error messages [▶]: ❚ DRC8001 ❚ DRC8002 ❚ DRC8003 ❚ DRC8004 ❚ DRC8005 ❚ DRC8006 ❚ DRC8007 ❚ DRU8001 ❚ DRU8002 ❚ DRU8003 ❚ DRU8004 ❚ DRU8005 ❚ DRU8006 ❚ DRU8007
Reset	This function enables you to set all fields to default value and blanks out all optional fields. Next screen: ❚ *Distinguished Name-BIC Routing – new/edit* screen
Cancel	This function enables you to cancel the process and return to the previous screen. Next screen: ❚ *Distinguished Name-BIC Routing – search/list* screen [▶]

2.3.7 Revisions

2.3.7.1 Revisions/Audit Trail – List Screen

Context of Usage

This screen is used to receive an overview of the Revisions and the Audit Trail for a chosen reference data object. The search results will be displayed in a list. After selecting an entry, you can proceed further by clicking on the Details button. There is no usage restriction for this screen. The Revisions / Audit Trail (List Screen) can be reached via every other List or Details Screen, where the user pushes the Revisions Button

Screen Access

❙ Screen name >> Click on the *revisions* button

Privileges
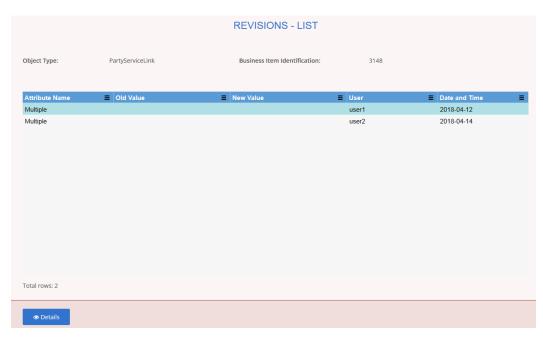
To use this screen you need the following privileges [▶]:

❙ Party Audit Trail Query

❙ Cash Account Audit Trail Query

❙ Residual Static Data Audit Trail Query

References

User Instruction Part

This screen is part of the following business scenario:

❙ View Revisions [▶]

REVISIONS - LIST

| Object Type: | PartyServiceLink | | Business Item Identification: | 3148 |

Attribute Name	Old Value	New Value	User	Date and Time
Multiple			user1	2018-04-12
Multiple			user2	2018-04-14

Total rows: 2

👁 Details

Screenshot   *Illustration 67: Revisions/Audit Trail – list* screen

Field Description

Revisions – List	
Object Type	Shows the type of the selected object.
Business Item Identification	Shows the identification of the respective business object.
Business Item Identification 2	Shows the additional identification of the respective business object. This field is only available in case a second business identification is needed.
Revision/Audit Trail Entry	
Attribute Name	Shows the name of the field which changed.
Old Value	Shows the old value of an attribute which was subject to a change.
New Value	Shows the new value of an attribute after the change.
User	Shows the identification of the user who changed the data.
Date and Time	Shows the date and time at which the user changed the data. Displayed format is: YYYY-MM-DD hh:mm:ss

Buttons

Details	This function enables you to display the details of the selected revisions. Next screen for reference data revisions/audit trail: ❚ *Revisions/audit trail – details* screen [▶]

2.3.7.2 Revisions/Audit Trail – Details Screen

Context of Usage

This screen displays detailed information on a specific revision of a selected object, including the data of this revision as well as the data of the previous revision from the details screen of the object.

Screen Access   ❚ Screen name >> Click on the *revisions* button >> *Revisions/audit trail – list screen* >> Click on the *details* button

Privileges

To use this screen you need (depending on the underlying object) the following privileges [▶]:

- ▌ Party Audit Trail Query
- ▌ Cash Account Audit Trail Query
- ▌ Residual Static Data Audit Trail Query

Screenshot

Revisions - Details

Audit Trail					
Object Type	PartyServiceLink	Business Item 1	3148	Approval Type	NONE
User 1	User Id	PPBKIRC4000	Date and Time	2018-04-12	

New Values			
Attribute Name	Valid From	Value	2018-04-14
Attribute Name	Valid To	Value	2018-05-23

Old Values			
Attribute Name	Valid From	Value	2018-04-04
Attribute Name	Valid To	Value	2018-05-03

Cancel
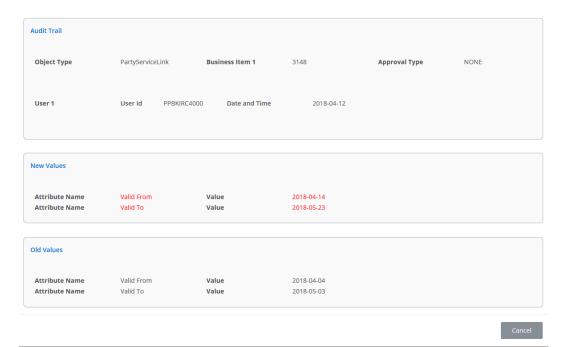
Illustration 68: Revisions/Audit Trail – details screen

Field Description

Revisions – List	
Object Type	Shows the type of object of the selected revisions
Business Item 1	Shows the identification of the business object.
Business Item 2	Shows the additional identification of the respective business object. This field is only available in case a second business identification is needed.
Approval Type	Shows the type of the approval from the possible values: ▌ None (2-eyes mode) ▌ Approval (4-eyes mode)
User 1	Shows the identification of the user who changed the data.
Date and Time	Shows the date and time at which 'User 1' changed the

Revisions – List	
	data. Displayed format is: YYYY-MM-DD hh:mm:ss
User 2	Shows the identification of the user who confirmed the change of data (in case of 4-eyes mode). This field is only available when a second user confirmed the change of data.
Date and Time	Shows the date and time at which 'User 2' confirmed the change of data. Displayed format is: YYYY-MM-DD hh:mm:ss
New Values	
New Values	Shows all elements which are part of the respective details screen. All changed data compared to the previous values are highlighted in red.
Previous Values	
Previous Values	Shows all elements which are part of the respective details screen.

Buttons

Cancel	This function enables you to return to the previous screen. Next screen: ❚ *Revisions/Audit Trail – list* screen [▶]

3 User Instructions Part

3.1 General

The user instructions part comprises scenarios adapted from typical user workflows. They are grouped into related activities, called business packages, which are further grouped into categories.

Furthermore, you can find business scenarios dedicated only to the Service operator are highlighted by the adding 'Service operator only' in the title.

Categories

The categories are a structural element and do not contain any information.

Business Packages

The business packages define an overall task. They include an overview and a list of the business scenarios. In detail, each business package description has the same structure and contains the following elements.

Overview The overview describes the aim and the background of the business package. It also explains the interrelation of the business scenarios.

List of Business Scenarios This section contains a list of all business scenarios belonging to the business package.

The list is unordered if the business scenarios represent alternative ways to achieve the aim of the business package. It is ordered if the business scenarios have to be carried out sequentially. Sequential business scenarios do not necessarily have to be carried out directly after each other. The sequence only implies that one business scenario is a prerequisite for the following ones.

Business Scenarios

Each business scenario represents a single workflow and consists of single action steps, intermediate results and a final result. In detail, each business scenario description has the same structure and contains the following elements.

Context of Usage The context of usage describes the aim of the business scenario and indicates whether this business scenario is mandatory or optional in order to fulfil the overall business package. It also contains the usage restrictions and the pre-requisites (excluding the privileges), if available.

Privileges In this section, all the necessary privileges to access and use the involved screens are listed. First the privileges to access the first screen are mentioned, followed by the privileges necessary to proceed with the business scenario. Afterwards, the privileges for the following screens are mentioned in the same order.

Reference   This section lists all references to the screens involved, in order of their appearance in the business scenario.

Instructions   Each workflow is described from the start to the end, beginning with the access to the starting screen. The instructions involve a number of separate steps which lead you through a series of screens and actions. Each action step is focused on 1 single action. Intermediate results are included and the instructions end with a final result. Possible alternatives and repetitions are highlighted with a notice sign.

⚠ **Example**

1. Action step 1
2. Action step 2
   ⇨ Intermediate result
3. Action step 3
➡ Result

3.2 Access Rights

3.2.1 Configuration of a Role

Overview   This business package describes the configuration of a role.

To configure a role, you first have to create a new role and then to assign privileges or other roles to the created role.

Afterwards you can assign the new role to a user or to a party.

To configure a role, carry out the business scenarios in the predefined order and choose the business scenario relevant to you whenever options are given.

Business Scenarios

1. Create a new role [▶]
2. Grant Privileges to a Role [▶]

❙ Assign a role to a party [▶]

❙ Assign a role to a user [▶]

3.2.1.1 Create a New Role

Context of Usage   This business scenario describes how to create a new role.

A role is a set of privileges, which can be granted to users and parties. You can create a new role for your participant and for yourself.

Creating a new role is mandatory for configuration of a role.

This business scenario is not relevant for payment bank users.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Role list query

❚ Create role

Reference   Further information on screens involved can be found in the screen reference part:

❚ *Roles – search/list* screen [▶]

❚ *Role – new/edit* screen [▶]

Instructions   1. Go to the *roles – search/list* screen:
Common >> Access Rights Management >> Roles

2. Click on the *new* button.

⇨ The *role – new* screen is displayed.

Role	
Role Name * Role Name	Role Description * Role Description

3. Enter all mandatory information about the role you want to create.

🛈   **Alternatives**

To set all fields to default value and blank out all optional fields, click on the *reset* button.

To cancel the process and return to the previous screen, click on the *cancel* button.

4. Click on the *submit* button.

5. Enter your PIN for digital signature purposes (NRO).

➡ The new role has been created.

3.2.1.2 Grant Privileges to a Role

Context of Usage   This business scenario describes how to grant a system privilege to a role. Before you start, make sure that you have already been granted the same privilege and that the role belongs to your system entity.

This business scenario is not relevant for payment bank users.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Grant Privilege

❚ Granted System Privileges List Query

References

Further information on screens involved can be found in the screen reference part:

▌ *Grant/revoke privileges – search* screen [▶]

▌ *Grant/revoke system privileges – new/edit* screen [▶]

Instructions
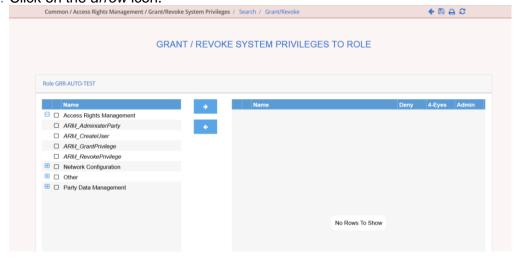
1. Go to the *grant/revoke privileges – search* screen:
   Common >> Access Rights Management >> Grant/Revoke Privileges

2. Select Role and choose the name of the relevant Role from the drop-down menu.

3. Click on the search button.

   ⇨ The *grant/revoke system privilege – new/edit* screen is displayed.

4. Search the relevant category in the 'Privileges' frame, open it by clicking the expand group icon and select the relevant privilege.

   ⇨ If the privilege has been already granted to the role, you can finish the business scenario with this step.

   ⇨ If the privilege has not been granted to the role, proceed with the next step.

5. Select the privilege(s) you want to grant to the Role.

6. Click on the *arrow* icon.

7. Enter your PIN for digital signature purposes (NRO).

➡ The privilege has been granted to the role.

🛈 **Repetition**

To grant more privileges to the role, repeat step 4 and 5 or select all the privileges you want to grant before clicking the *arrow* icon.

3.2.1.3 Assign a Role to a Party

Context of Usage   This business scenario describes how to assign a role to a party. A role is a homogenous group of privileges. To grant a role to a party, you must own that role. You can grant a role to a party not belonging to your system entity only if you are the party administrator of the party that owns the role. This business scenario is not relevant for payment bank users.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Role list query

❚ Grant/revoke role

References   Further information on screens involved can be found in the screen reference part:

❚ *Grant/revoke privileges – search* screen [▶]

❚ *Grant/revoke role – new/edit* screen [▶]

Instructions   1. Go to the *grant/revoke privileges – search* screen:
Common >> Access Rights Management >> Grant/Revoke Roles

2. Select the parent BIC and the BIC of the party you would like to assign the role to.

3. Click on the *search* button.

⇨ The *grant/revoke role – new/edit* screen is displayed.

4. Check if the party has been already granted to the relevant roles in the left column.

⇨ If the party has been already granted to the role, you can finish the business scenario with this step.

⇨ If the party has not been granted to the role, proceed with the next step.

5. Select the role(s) you want to grant to the party in the 'Roles' frame.

6. Click on the *arrow* icon.

7. Enter your PIN for digital signature purposes (NRO).

➡ The role has been granted to the party.

🛈 **Repetition**

To grant more roles to the party, repeat step 4 and 5 or select all the roles you want to grant before clicking the *arrow* icon.

3.2.1.4 Assign a Role to a User

Context of Usage
This business scenario describes how to assign a role to a user. A role is a homogenous group of privileges. To grant a role to a user, you must own that role. You can only grant a role to a user that belongs to your system entity. This business scenario is not relevant for payment bank users.

Privileges
To carry out this business scenario, you need the following privileges:

❚ Role list query

❚ Grant/revoke role

References
Further information on screens involved can be found in the screen reference part:

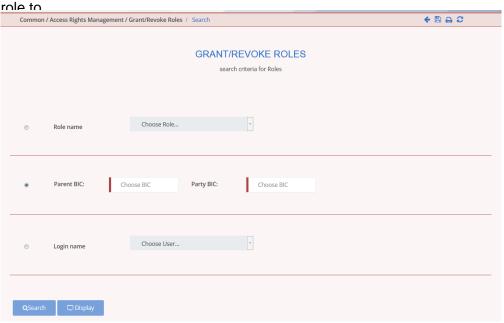❚ *Grant/revoke roles – search* screen [▶]

❚ *Grant/revoke role – new/edit* screen [▶]
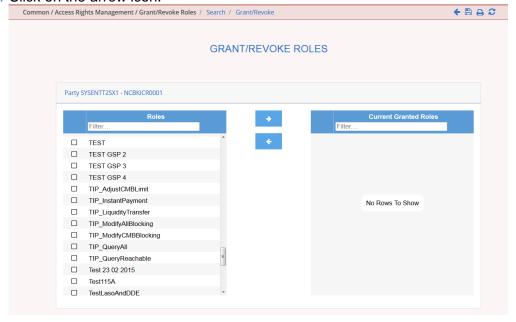
Instructions
1. Go to the *grant/revoke roles – search* screen:
   Common >> Access Rights Management >> Grant/Revoke Roles

2. Enter the login name of the relevant party in the 'User' subframe.

3. Click on the *search* button.

⇨ The *grant/revoke role – new/edit* screen is displayed.

4. Check if the user has been already granted to the relevant roles in the left column.

    ⇨ If the user has been already granted to the role, you can finish the business scenario with this step.

    ⇨ If the user has not been granted to the role, proceed with the next step.

5. Select the role(s) you want to grant to the user in the 'Roles' frame.

6. Click on the *arrow* icon.

Common / Access Rights Management / Grant/Revoke Roles / Search / Grant/Revoke	← 🖫 🖨 🔁

GRANT/REVOKE ROLES

User testtest1

Roles		Current Granted Roles
Filter....		Filter....
☐ 000000000Elisa04	→	
☐ 000000000Elisa07	←	
☐ 000000000Elisa08		
☐ 000000000Elisa09		
☐ 000000000Elisa10		
☐ 000000000Praga		
☐ 000000000Vienna		
☐ Avorio		No Rows To Show
☐ Avorio		
☐ Bianco		
☐ Blue		
☐ Brown		
☐ Brown		
☐ CB		

7. Enter your PIN for digital signature purposes (NRO).

➡ The role has been granted to the user.

🛈 **Repetition**

To grant more roles to the user, repeat step 4 and 5 or select all the roles you want to grant before clicking the *arrow* icon.

3.2.2 Configuration of a User

Overview
This business package describes the configuration of a user. A user is a reference data object that allows an individual or an application to interact with the shared services. The functions that can be triggered depend on the privileges granted to the user. It is possible to grant roles to the new user after its creation. To configure a user, carry out the following business scenarios in the predefined order.

Business Scenarios

1. Create a new user [▶]

2. Create a new user certificate distinguished name link [▶]

3. Assign a role to a user [▶]

3.2.2.1 Create a New User

Context of Usage

This business scenario describes how to create a new user. A user is a reference data object that allows an individual or an application to interact with one or many Eurosystem Market Infrastructure services. The functions that can be triggered within each service depend on the privileges granted to the user.

The user is mainly defined by the 'Login Name' and 'System User Reference' that must be unique in the system. All the users are linked to a specific party and can be created by another authorised user. There is no usage restriction for this business scenario.

Privileges

To carry out this business scenario, you need the following privileges:

❙ System user query

❙ Create user

Reference
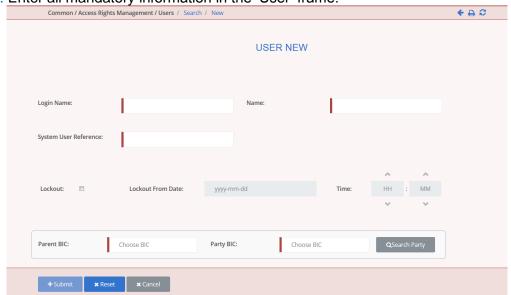
Further information on screens involved can be found in the screen reference part:

❙ *Users – search/list* screen [▶]

❙ *User – new/edit* screen [▶]

Instructions

1. Go to the *users – search/list* screen:

   Common >> Access Rights Management >> Users

2. Click on the *new* button.

   ⇨ The *user – new* screen is displayed.

3. Enter all mandatory information in the 'User' frame.

4. Click on the *submit* button.
5. Enter your PIN for digital signature purposes (NRO).
➡ The new user has been created.

3.2.2.2 Create a New User Certificate Distinguished Name

Context of Usage   This business scenario describes how to create a new user certificate distinguished name.

Privileges   To carry out this business scenario, you need the following privileges:
▌ Certificate query
▌ Create certificate distinguish name
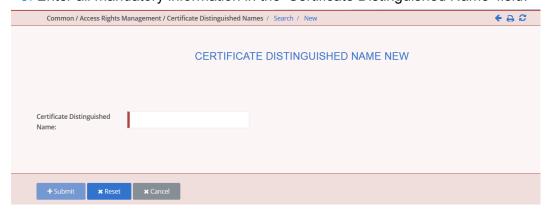
Reference   Further information on screens involved can be found in the screen reference part:
▌ *Certificate distinguished names – search/list* screen [▶]
▌ *Certificate distinguished name – new* screen [▶]

Instructions   1. Go to the *certificate distinguished name – search/list* screen:
Common >> Access Rights Management >> Certificate Distinguished Name
2. Click on the *new* button.
   ⇨ The *certificate distinguished name– new* screen is displayed.
3. Enter all mandatory information in the 'Certificate Distinguished Name' field.

> **Alternative**

To set default criteria and blank out all optional fields, click on the *reset* button. To cancel the process and return to the previous screen, click on the *cancel* button.

4. Click on the *submit* button.

➡ The new certificate distinguished name has been created.

3.2.2.3 Create a New User Certificate Distinguished Name Link

Context of Usage

This business scenario describes how to create a new user certificate distinguished name link.

You need to create a link between a certificate distinguished name and a user login name in order to allow your users or applications to access to the system via the interface.

Before you start please check if a certificate distinguished name has been available and if a link between the selected user and the certificate distinguished name has been already created.

You can link more than one certificate to a single login name and one certificate to more than one user.

Privileges

To carry out this business scenario, you need the following privileges:

❚ Create user certificate distinguish name link

❚ Query user certificate distinguish name link

❚ System user link query

References

Further information on screens involved can be found in the screen reference part:

❚ *User certificate distinguished name links – search/list* screen [▶]

❚ *User certificate distinguished name link – new* screen [▶]

Instructions
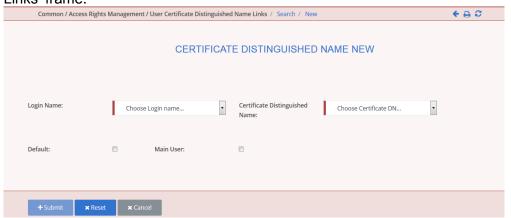
1. Go to the *user certificate distinguished name links – search/list* screen: Common >> Access Rights Management >> User Certificate Distinguished Name Links

2. Click on the *new* button.

   ⇨ The *user certificate distinguished name link – new* screen is displayed.

3. Enter all mandatory information in the 'User Certificate Distinguished Name Links' frame.

Common / Access Rights Management / User Certificate Distinguished Name Links / Search / New				← 🖨 ⟳
		CERTIFICATE DISTINGUISHED NAME NEW		
Login Name:	Choose Login name... ▾	Certificate Distinguished Name:	Choose Certificate DN... ▾	
Default:	☐	Main User:	☐	
✛ Submit	✖ Reset	✖ Cancel		

🛈 **Alternatives**

To set default criteria and blank out all optional fields, click on the *reset* button. To cancel the process and return to the previous screen, click on the *cancel* button.

4. Click on the *submit* button.

5. Enter your PIN for digital signature purposes (NRO).

➡ The new user certificate distinguished name link has been created.

3.2.2.4 Assign a Role to a User

Context of Usage   This business scenario describes how to assign a role to a user. A role is a homogenous group of privileges. To grant a role to a user, you must own that role. You can only grant a role to a user that belongs to your system entity.

This business scenario is not relevant for payment bank users.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Role list query

❚ Grant/revoke role

References   Further information on screens involved can be found in the screen reference part:

❚ *Grant/revoke roles – search* screen [▶]

❚ *Grant/revoke role – new/edit* screen [▶]

Instructions   1. Go to the *grant/revoke roles – search* screen:
Common >> Access Rights Management >> Grant/Revoke Roles

2. Enter the login name of the relevant party in the 'User' subframe.

3. Click on the *search* button.

   ⇨ The *grant/revoke role – new/edit* screen is displayed.

4. Check if the user has been already granted to the relevant roles in the left column.

   ⇨ If the user has been already granted to the role, you can finish the business scenario with this step.

   ⇨ If the user has not been granted to the role, proceed with the next step.

5. Select the role(s) you want to grant to the user in the 'Roles' frame.

6. Click on the *arrow* icon.

7. Enter your PIN for digital signature purposes (NRO).

➡ The role has been granted to the user.

> **ⓘ Repetition**
>
> To grant more roles to the user, repeat step 4 and 5 or select all the roles you want to grant before clicking the *arrow* icon.

3.2.3 Usage of the 4-Eyes Mode

Overview   This business package describes the usage of the 4-eyes mode. The use of the 2-eyes or the 4-eyes mode depends on your access rights configuration.

Business Scenarios   To use the CRDM in 4-eyes mode, carry out the following business scenarios in the predefined order:

❙ Initiate an action in 4-eyes mode [▶]

❙ Approve an action in 4-eyes mode [▶]

3.2.3.1 Initiate an Action in 4-Eyes Mode

Context of Usage   This Business scenario describes how to initiate an action via an enter (new/edit) screen, which has to be approved by a second user. Whether your actions in CRDM (new/edit/delete) have to be approved by a second user depends on your access right configuration. Initiating an action in 4-eyes mode is mandatory for the usage of the 4-eyes mode.

Privileges   To carry out this business scenario, you need the privileges necessary for the action you want to initiate.

Reference   Further information on screens involved can be found in the screen reference part (see business scenario or screen description of the underlying action).

Instructions
1. Go to the relevant *edit* or *new* screen:
2. Enter all mandatory information in the *enter* screen on which you want to initiate an action or delete a request by clicking on the *delete* button.
3. Click on the *submit* button.
   ⇨ A success message is displayed on the screen indicating that the request was sent in 4-eyes mode and showing the 4-eyes principle ID assigned by CRDM.
   ⇨ An alert icon is displayed on the active CRDM screen of all users eligible for approving actions in 4-eyes mode.
   ⇨ You have initiated an action carrying the 'Awaiting approval' status.

3.2.3.2 Approve an Action in 4-Eyes Mode

Context of Usage

This Business scenario describes how to approve an action, which has been initiated by a different user in 4-eyes mode. The use of 2-eyes or 4-eyes mode depends on your access rights configuration.

Approving an action is mandatory for the usage of the 4-eyes mode.

Before you start, the action has to be initiated by a different user.

Privileges

To carry out this business scenario, you need the following privileges:

❙ Data changes of a business object list query

❙ Data changes of a business object details query

Reference

Further information on screens involved can be found in the screen reference part:

❙ Data changes – search/list screen [▶]

❙ Data Change – details screen [▶]

Instructions

1. Go to the *Data changes – search/list* screen.

2. Enter the search criteria known to you (e.g. user reference of the change) about the action waiting for your approval. Ask the first user for the 4-eyes principle ID submitted in the success message to identify the action easily.

3. In the *status* field, select the status 'Awaiting approval'.

4. Click on the *search* button.

   ⇨ The search results are displayed in a list on the same screen.

   ⇨ If the search retrieves only one data change waiting for your approval, the *data change – details screen* is displayed directly. Proceed with step 7.

5. *Select the action you would like to approve by clicking on an entry in the list.*

6. Click on the details button.

   ⇨ The *data change – details screen* is displayed.

7. Check the data. If everything is correct, click on the *approve* button.

➡ The action has been approved and is submitted for execution. The *data changes – search/list* screen is displayed with the updated result of the previously selected criteria.

3.3 Rule Sets

3.3.1 Configuration of a New Message Subscription Rule Set

Overview   This business package describes how to configure a new message subscription rule set.

You can only create a new message subscription rule set, if you have the relevant privilege. You can configure the specific set of messages (or copies of messages) you want to receive from TIPS for yourself and for your directly connected parties based on a set of rules.

Each Actor can have many active rule sets at any given point in time. Each rule set can include many rules. Each rule can include many groups of parameters. The maximum overall number of groups of parameters for the active rule sets is 1,500. Each rule can include many parameters. Within each rule, each parameter can be linked to many distinct values. The maximum overall number of distinct values for the active rule sets is 50.

To configure a new message subscription rule set, carry out the following business scenario:

Business Scenario   ❙ Create a new message subscription rule set [▶]

3.3.2 Create a New Message Subscription Rule Set

Context of Usage   This Business scenario describes how to create new message subscription rule sets, which are used by the CRDM application for each outgoing message. These rules determine to which interested party or parties the given message has to be sent or copied.

Creating a new message subscription rule set is mandatory for the creation of a new message subscription rule set.

The creation of a message subscription rule set can be performed by all parties owning the relevant privilege.

Privileges   To carry out this business scenario, you need the following privileges:

❙ Create message subscription rule set

❙ Message subscription rule set list query

❙ Message subscription rule list query

❙ Create message subscription rule

Reference   Further information on screens involved can be found in the screen reference part:

❙ *Message subscription rule sets – search/list* screen [▶]
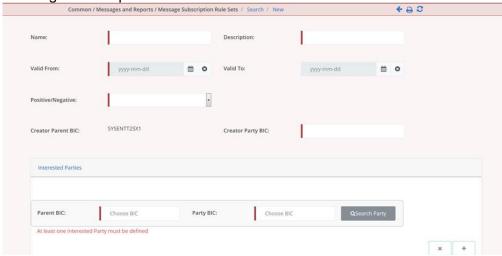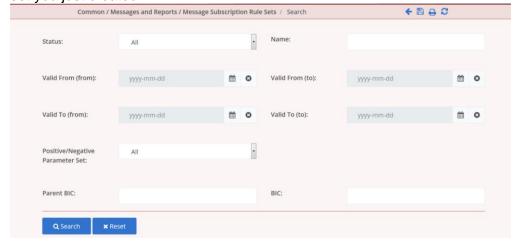
| *Message subscription rule set – new/edit* screen [▶]

Instructions

1. Go to the *message subscription rule sets – search/list* screen:
   Common >> Messages and Reports >> Message Subscription Rule Set

2. Click on the *new* button.

   ⇨ The *message subscription rule set – new* screen is displayed.

3. Enter all mandatory information about the rule set you want to create in the 'Message Subscription Rule Set' and 'Interested Parties' frames.

4. Click on the *submit* button.

   ⇨ The new message subscription rule set has been created without any rule attached.

5. Go to the *message subscription rule sets – search/list* screen:
   Common >> Messages and Reports >> Message Subscription Rule Set

6. Enter all search criteria known to you about the message subscription rule set you just created.

7. Click on the *search* button.

   ⇨ A list containing the search results is displayed on the screen.

8. Select the message subscription rule set you just created by clicking on an entry in the list.

9. Click on the *details* button.

   ⇨ The *message subscription rule set – details* screen is displayed.

10. Click on the *Add Rule* button.

11. Enter all mandatory information about the rule you want to create in the 'Message Subscription Rules' frame.

12. Click on the *Ok* icon.

13. Click on the *submit* button. At least one rule should be present in the rule set.

➡ The new message subscription rule has been created.

3.4 Party Management

3.4.1 Administration of Participants

Overview　　This business package describes all activities a CB can perform for the administration of its participants during their lifecycle. The administration of participants has the aim of making sure that all parties are registered in CRDM and that their reference data are always up to date.

After the initial creation of participants, a party administrator has to edit the previously entered reference data whenever a change takes place. The Central Bank party administrator can also decide to close a party, imposing a new closing date. If a party ceases to exist, the party administrator has to delete it in CRDM.

To administer your participants, carry out the following business scenarios in the predefined order:

Business Scenario

❙ Create a new participant [▶]

❙ Edit an existing participant [▶]

❙ Delete an existing participant [▶]

3.4.1.1 Create a New Participant

Context of Usage

This business scenario describes how to create a new participant. Each CB is responsible for the creation of the party reference data for their payment banks.

Creating a new participant is mandatory for the administration of participants. It is optional for the configuration for a central bank.

Before you start, check whether the participant has not already been created by someone else. Also, make sure that the party BIC you want to use for the new participant has been created in the BIC directory.

Privileges

To carry out this business scenario, you need the following privileges:

❚ Party list query

❚ Create party

Reference

Further information on screens involved can be found in the screen reference part:

❚ *Parties – search/list* screen [▶]

❚ *Parties – new/edit* screen [▶]

Instructions

1. Go to the *Parties – search/list* screen:
   Common >> Parties >> Parties

2. Click on the *new* button.

   ⇨ The *parties – new* screen is displayed.

3. Enter all mandatory information in the 'Party' and 'Address' frames.

4. To add a technical address or restriction, enter all mandatory information in the 'Technical Addresses' and 'Restrictions' frames. At least one technical address has to be defined.

   ⇨ A new technical address or restriction has been added to the list.

5. Click on the submit button.

➡ The new participant has been created.

3.4.1.2 Edit an Existing Participant

Context of Usage

This business scenario describes how to edit the reference data of an existing participant. Each national central bank is responsible for maintaining the reference data for their payment banks.

Editing an existing participant is optional for the administration of participants.

If you want to close a party, verify that all the reference data of all objects linked to that party have a closing date equal to or earlier than the party closing date or have been deleted.

Privileges

To carry out this business scenario, you need the following privileges:

❚ Party list query

❚ Party reference data query

❚ Update party

Reference

Further information on the involved screens can be found in the screen reference part:

❚ *Parties – search/list* screen [▶]

❚ *Party – details* screen [▶]

❚ *Party – new/edit* screen [▶]

Instructions

1. Go to the *parties – search/list* screen:

   Common >> Parties >> Parties
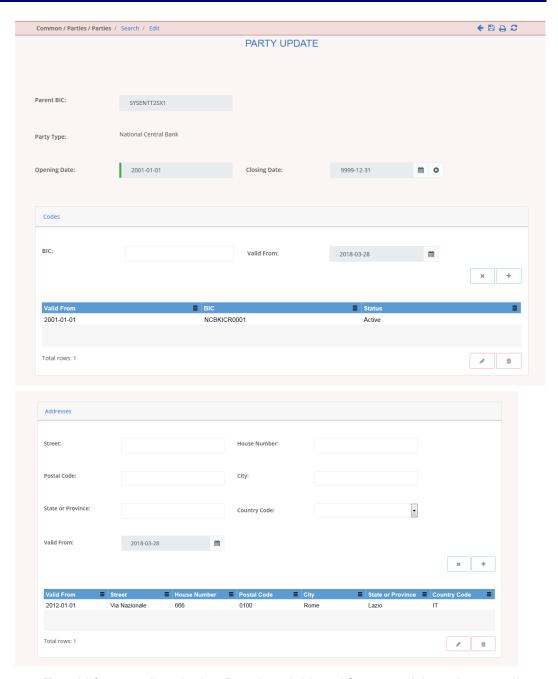
2. Enter all search criteria known to you about the party you want to edit.

3. Click on the *search* button.

   ⇨ A list containing the search results is displayed on the screen.

   ⇨ If the search retrieves a single party, the *party – details* screen is displayed directly. Proceed with step 6.

4. Select the relevant party from the search results by clicking on an entry in the list.

5. Click on the *details* button.

   ⇨ The *party – details* screen is displayed.

6. Click on the *edit* button.

   ⇨ The *party – edit* screen is displayed.

7. To add or change current values in the 'Party' or 'Address' frames, enter the new values in the respective fields.

Common / Parties / Parties / Search / Edit

PARTY UPDATE

Parent BIC: SYSENTT2SX1

Party Type: National Central Bank

Opening Date: 2001-01-01   Closing Date: 9999-12-31

Codes

BIC: _____   Valid From: 2018-03-28

Valid From	BIC	Status
2001-01-01	NCBKICR0001	Active

Total rows: 1

Addresses

Street: _____   House Number: _____

Postal Code: _____   City: _____

State or Province: _____   Country Code: _____

Valid From: 2018-03-28

Valid From	Street	House Number	Postal Code	City	State or Province	Country Code
2012-01-01	Via Nazionale	666	0100	Rome	Lazio	IT

Total rows: 1

8. To add future values in the 'Party' or 'Address' frames, click on the *pencil* icon in the lower right-hand corner of the frame.

   ⇨ Empty fields are displayed.

   ⇨ Changes in the current values are reset.

9. Enter all mandatory information in the newly displayed fields.
   The 'Valid From' date must be later than today.

10. To delete existing values in the 'Party' or 'Address' frames, clear the content and leave the respective fields blank.

11. To add new technical addresses or restrictions, enter new data in the 'Add/Update Technical Address' or 'Restrictions' sub-frames.

12. Click on the *add row* icon.

   ⇨ A technical address or restriction has been added to the list.

13. To change technical addresses or restrictions, select the relevant entry from the list.

14. Enter the new data in the 'Add/Update Technical Address' or 'Restrictions' sub-frames.

15. Click on the *submit changes* icon.

   ⇨ The data of the technical address or restriction are changed in the list.

16. To delete a technical address or restriction, select the relevant line in the list.

17. Click on the *cancel changes* icon in the 'Options' column.

   ⇨ The technical address or restriction has been deleted from the list.

🛈 **Repetition**

Repeat steps 11 and 12 to add more technical addresses or restrictions.

Repeat steps 13 to 15 to edit more technical addresses or restrictions.

Repeat steps 16 and 17 to delete more technical addresses or restrictions.

You can add, edit or delete up to 10 technical addresses or restrictions.

🛈 **Alternatives**

To set all fields to default value and blank out all optional fields, click on the *reset* button.

To cancel the process and return to the previous screen, click on the *cancel* button.

18. Click on the *submit* button.

➡ The edited party reference data are stored.

3.4.1.3 Create a Distinguished Name-BIC routing configuration

Context of Usage
Each participant is responsible for maintaining the reference data for their DN-BIC routing links. For Inbound communication, different DNs can be linked to different BICs and vice versa. In the outbound case, the same BIC can only be linked to a single DN. However different BICs can still be linked to the same DN.

Privileges
To carry out this business scenario, you need the following privilege:

❚ Delete DN-BIC Routing

Reference
Further information on the involved screens can be found in the screen reference part:

❚ *Distinguished Name-BIC routing – search/list* screen [▶]

❚ *Distinguished Name-BIC routing – new/edit* screen [▶]

Instructions
1. Go to the *Distinguished Name-BIC routing – search/list* screen:
   TIPS >> Cash >> *Distinguished Name-BIC routing*
2. Click on the *new* button.
   ⇨ The *Distinguished Name-BIC routing – new screen* is displayed.
3. Enter all mandatory information.
4. Click on the *submit* button.
➡ The new *Distinguished Name-BIC routing* has been created.

3.4.1.4 Delete an Existing Participant

Context of Usage
Each central bank is responsible for maintaining the reference data for their payment banks. If a party ceases to exist, the party administrator has to delete it in CRDM.

Deleting an existing participant is an optional step for the administration of participants.

Before you delete a participant, check the opening and closing date of the participant. A participant can only be deleted if the closing date has passed or if the opening date has not yet been reached (future opening date). If the closing

date is equal to the current date, you have to wait for the new business day to delete the participant. In addition, make sure that all the linked instances in a higher position within the deletion hierarchy (i.e. Cash account) have been deleted.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Party list query

❚ Party reference data query

❚ Delete party

Reference   Further information on the involved screens can be found in the screen reference part:

❚ *Parties – search/list* screen [▶]

❚ *Party – details* screen [▶]

Instructions   1. Go to the *parties – search/list* screen:
Common >> Parties >> Parties

2. Enter all search criteria known to you about the party you want to delete.

3. Click on the *search* button.

   ⇨ A list containing the search results is displayed on the screen.

   ⇨ If the search retrieves a single party, the *party – details* screen is displayed directly. Proceed with step 6.

4. Select the relevant party from the search results by clicking on an entry in the list.

5. Click on the *details* button.

   ⇨ The *party – details* screen is displayed.

6. Click on the *delete* button if the opening date is not reached and/or the closing date is later than the current date.

   ⇨ A confirmation prompt is displayed.

7. Click on *yes* if you really want to delete the party reference data.

➡ The party reference data are deleted.

3.5 Reports

3.5.1 Report Management

3.5.1.1 Create a New Report Configuration

Context of Usage
This business scenario describes how to create a new report to receive specific information about dynamic or reference data through a predefined report. Each report is periodically created.

You can check the created report via the CRDM graphical user interface.

You can configure a report only in U2A mode.

Privileges
To carry out this business scenario, you need the following privileges:

❚ Report configuration list query

❚ Create report configuration
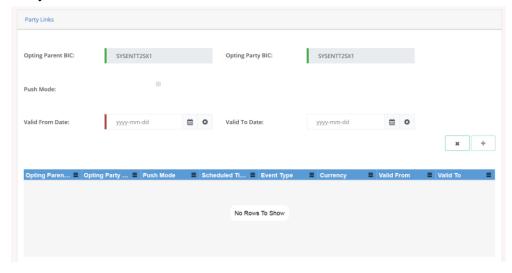
References
Further information on screens involved can be found in the screen reference part:

❚ *Report configuration – search/list* screen [▶]

❚ *Report configuration – new/edit* screen [▶]

Instructions
1. Go to the *report configuration – search/list* screen:
   Common >> Messages and Reports >> Report Configurations

2. Click on the *new* button.
   ⇨ The *report configuration – new* screen is displayed.

3. Enter all mandatory information about the report configuration you want to create.

4. Enter all mandatory information about the addressee of the report in the 'Party Links' frame.

5. Click on the *submit changes* icon.

    ⇨ The report configuration party link has been added.

6. Click on the *submit* button.

➡ A new report configuration has been created.

3.6 Revisions

3.6.1 Monitoring of Revisions

Overview   This business package describes the monitoring of revisions. It enables you to view the historical status and historical data of a dataset in order to monitor revisions.

Business scenario   To monitor revisions, carry out the following business scenario:

❚ View revisions [▶]

3.6.1.1 View Revisions

Context of Usage   This business scenario describes how to view the historical status of a dataset and the history of attribute values, the identification of the user who created/edited/deleted the dataset as well as the timestamp when this action happened, since every creation/modification/deletion of a dataset is stored within CRDM.

In case of the 4-eyes mode any action of the first and confirming user including

the timestamp is displayed. Viewing revisions is mandatory for the monitoring of revisions.

Privileges   To carry out this business scenario, you need (depending on the underlying object) the following privileges:

❚ Party audit trail query

❚ Cash Account audit trail query

References   Further information on screens involved can be found in the screen reference part:

❚ *Revisions/audit trail – list* screen [▶]

❚ *Revisions/audit trail – details* screen [▶]

Instructions   1. Go to the relevant *search/list* or *details* screen.

2. Click on the *revisions* button.

3. Select the item you want to view by clicking on an entry in the list.

4. Click on the *details* button.

➡ The *revisions/audit trail – details* screen is displayed.

3.7 Account Management

3.7.1 Administration of Cash Accounts

3.7.1.1 Create a New Cash Account

Context of Usage
This business scenario describes how to create a new cash account. Each central bank is responsible for opening cash accounts for itself and its payment banks, in order to settle Instant Payment transactions.

You have to link each of your cash accounts to a specific settlement currency. This business scenario is mandatory for the administration of cash accounts, for the configuration for a central bank.

Privileges
To carry out this business scenario, you need the following privileges:

❙ Create cash account

❙ Cash account list query

**References**
Further information on screens involved can be found in the screen reference part:

❙ *Cash Account – search/list* screen [▶]

❙ *Cash Account – new/edit* screen [▶]

Instructions
1. Go to the *cash accounts – search/list* screen:
   TIPS >> Cash >> Cash Accounts

2. Click on the *new* button.

   ⇨ The c*ash account – new* screen is displayed.

3. Enter all mandatory information in the 'Cash Account' frame.

4. To add a restriction, click on *add row* icon under the "restriction" frame.

5. Enter all mandatory information in the available fields of the "Restrictions" frame.

6. Click on the *submit changes* icon.

    ⇨ A new restriction has been added to the list.

7. Click on the *submit* button.

➡ The new cash account has been created.

3.7.1.2 Edit an Existing Cash Account

Context of Usage   This business scenario describes how to edit an existing cash account. Each CB is responsible to maintain the reference data for the cash account of their participants. This business scenario is not relevant for Payment Bank users.

Privileges   To carry out this business scenario, you need the following privileges:

❚ Cash account list query

❚ Update cash account

❚ Delete cash account

References   Further information on screens involved can be found in the screen reference part:

❚ *Cash Account – search/list* screen [▶]

❚ *Cash Account – new/edit* screen [▶]

❚ *Cash Account – details* screen [▶]

Instructions
1. Go to the *cash accounts – search/list* screen:
   TIPS >> Cash >> Cash Accounts

2. Enter the search criteria known to you about the cash account you want to edit.

3. Click on the *search* button.

    ⇨ A list containing the search results is displayed on the screen.

    ⇨ If the search retrieves a single cash account, the *cash account – details* screen is displayed directly. Proceed with step 5.

4. Select the relevant cash account by clicking on an entry in the list.

5. Click on the *edit* button.

    ⇨ The *cash account – edit* screen is displayed

6. To add or edit current values of the cash account reference data, enter all mandatory information in the "cash account" frame.

7. To add a restriction click on the *add row* in the frame "restrictions".

8. Enter all mandatory information in the available fields in the "Restrictions" frame.

9. Click on the *submit changes* button

10. To edit a restriction, select the relevant entry from the list by clicking on it.

11. Click on the *copy row* icon

12. Update the data.

13. Click on the *submit changes* icon.

⇨ The *data* of the restriction has been changed in the list.

14. To delete a restriction, select the relevant entry from the list.

15. Click on the *cancel changes* icon in the 'Options' column.

⇨ The *restriction* has been deleted from the list.

16. Click on the *submit* button.

➡ The edited cash account reference data is stored.

3.7.1.3 Delete an Existing Cash Account

Context of Usage

This business scenario describes how to delete an existing cash account. Each CB is responsible to delete the cash account of their participants. Deleting an existing cash account is an optional step in the administration of a cash account.

The request to delete a TIPS account must refer to an existing and active cash account. Before you delete the cash account, check the opening and closing day: a cash account can be deleted if the closing date is earlier than or equal to the

current business date or if the opening date is earlier than the current business date. In case of the deletion of a future RTGS dedicated transit account, check that no active cash account with the same currency exists. This business scenario is not relevant for Payment Bank users.

Privileges   To carry out this business scenario, you need the following privileges:
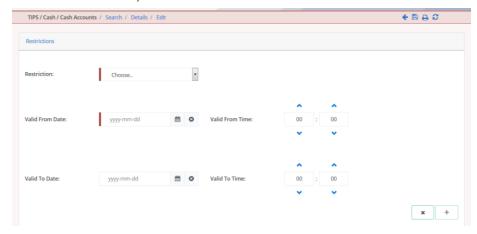
❚ Cash account list query

❚ Cash account reference data query

❚ Delete cash account

References   Further information on screens involved can be found in the screen reference part:

❚ *Cash Account – search/list* screen [▶]

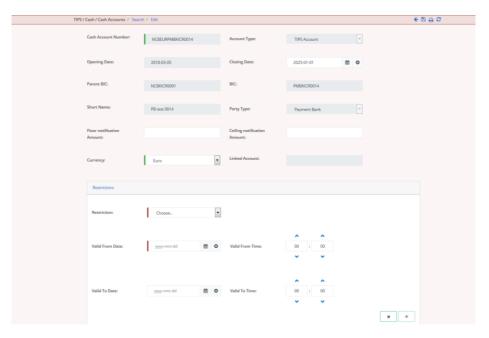❚ *Cash Account – details* screen [▶]

Instructions   1. Go to the *cash accounts – search/list* screen:
TIPS >> Cash >> Cash Accounts

2. Enter the search criteria known to you about the cash account you want to delete.

3. Click on the *search* button.

⇨ A list containing the search results is displayed on the screen.

⇨ If the search retrieves a single cash account, the *cash account – details* screen is displayed directly. Proceed with step 6.

4. Select the relevant cash account by clicking on an entry in the list.

5. Click on the *details* button.

⇨ The *cash account – details* screen is displayed.

6. Click on the *delete* button if the opening date is not reached and/or the closing date is equal or greater than the current date.

➡ The cash account has been deleted.

3.7.1.4 Create an Authorised Account User

Context of Usage   This business scenario describes how to create an authorised account user in order to connect a BIC11 to a specific cash account. This connection allows the BIC11 to use the cash account for its settlement purposes.

The same cash account can be assigned to more than one BIC11 but only one cash account can be linked to the same BIC11.

Before you start, check whether the BIC11 and the cash account exist in CRDM.

Privileges   To carry out this business scenario, you need the following privilege:
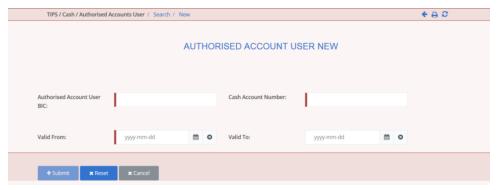
❙ Create Authorised Account User

Reference   Further information on screens involved can be found in the screen reference part:

❙ *Authorised Account User – search/list* screen [▶]

❙ *Authorised Account User – new/edit* screen [▶]

Instructions   1. Go to the *Authorised Account User – search/list* screen:
TIPS >> Cash >> Authorised Account Users

2. Click on the *new* button.

3. Enter all the mandatory information in the 'Authorised account user new' frame.

4. Click on the *submit* button.

➡ A new Authorised account user has been created.

3.7.1.5 Edit an Authorised Account User

Context of Usage   This business scenario describes how to edit an authorised account user in order to modify the validity dates of the connection between the BIC11 and the cash account for settlement purposes.

Privileges   To carry out this business scenario, you need the following privilege:

❙ Update Authorised Account User

Reference   Further information on screens involved can be found in the screen reference part:

❙ *Authorised Account User – search/list* screen [▶]

❙ *Authorised Account User – new/edit* screen [▶]
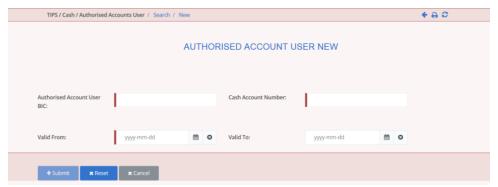
Instructions   1. Go to the *Authorised Account User – search/list* screen:
TIPS >> Cash >> Authorised Account Users

2. Click on the *edit* button.

3. Modify the information on the validity dates of the selected Authorised Account User.

4. Click on the *submit* button.

➡ The Authorised account user has been modified.

3.7.1.6 Delete an Authorised Account User

Context of Usage

This business scenario describes how to delete an authorised account user. The authorised account user can be deleted only if the Valid from value is in the future or the Valid to value is in the past.

Privileges

To carry out this business scenario, you need the following privilege:

❚ Delete Authorised Account User

Reference

Further information on screens involved can be found in the screen reference part:

❚ *Authorised Account User – search/list* screen [▶]

❚ *Authorised Account User – new/edit* screen [▶]

Instructions

1. Go to the *Authorised Account User – search/list* screen:
   TIPS >> Cash >> Authorised Account Users

2. Click on the *search* button.

⇨ A list containing the search results is displayed on the screen.

3. Select the relevant Authorised account user by clicking on an entry in the list.

4. Click on the *delete* button.

➡ The Authorised account user has been deleted.

3.8 Technical Addresses

3.8.1 Configuration of a Technical Address

Overview

This business package describes the configuration of a technical address. The technical address is used by the shared services to exchange data with the party.

A complete configuration foresees the specification of a technical address connected to a network service via a technical address service link.

To configure a technical address, carry out the following business scenarios in the predefined order:

Business Scenarios

1. Add a new technical address to a party [▶]

2. Create a new technical address service link [▶]

3.8.1.1 Add a new Technical Address to a Party

Context of Usage

This business scenario describes how to add a new technical address to a party. Each Central Bank is responsible for defining all the required technical addresses for its parties as a first step to have a complete routing configuration. Adding a new technical address to a party is mandatory for the configuration of a technical address. Before you add a technical address to yourself or one of your participants, check whether the technical address exists in CRDM.

You have to add at least one technical address for each of your participants.

This business scenario is not relevant for payment bank users.

Privileges

To carry out this business scenario, you need the following privileges:

❚ Party list query

❚ Party reference data query

❚ Technical address network service link details query

❚ Update party

Reference

Further information on screens involved can be found in the screen reference part:

❚ *Parties – search/list* screen [▶]

❚ *Party – details* screen [▶]

❚ *Party – new/edit* screen [▶]

Instructions

1. Go to the *parties – search/list* screen:
   Common >> Parties >> Parties
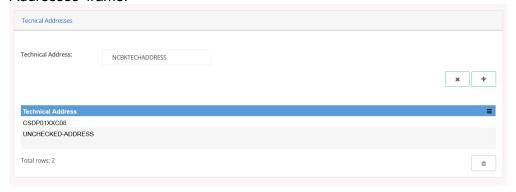
2. Enter all search criteria known to you about the party to which you want to add the technical address.

3. Click on the *search* button.

   ⇨ A list containing the search results is displayed on the screen.

   ⇨ If the search retrieves only one party, the *party – details* screen is displayed directly. Proceed with step 5.

4. Select the relevant party by clicking on an entry in the list.

5. Click on the *edit* button.
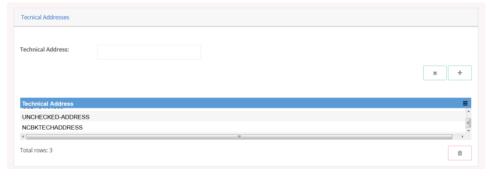
⇨ The *party – edit* screen is displayed.

6. To add a technical address, click on the *add row* icon in the 'Technical Addresses' frame.

Tecnical Addresses		
Technical Address:	NCBKTECHADDRESS	
		✕ +
Technical Address		☰
CSDP01XXC08		
UNCHECKED-ADDRESS		
Total rows: 2		🗑

7. Enter the name of the technical address.

8. Click on the *submit changes* icon.

⇨ The technical address has been added to the list.

Tecnical Addresses		
Technical Address:		
		✕ +
Technical Address		☰
UNCHECKED-ADDRESS		
NCBKTECHADDRESS		
Total rows: 3		🗑

🛈 **Repetition**

To add more technical addresses, repeat steps from 6 to 8.

You can add up to 10 technical addresses.

🛈 **Alternatives**

To set all fields to default value and blank out all optional fields, click on the *reset* button.

To cancel the process and return to the previous screen, click on the *cancel* button.

9. Click on the *submit* button.

➡ The new technical address has been created.

3.8.1.2 Create a New Technical Address Service Link

Context of Usage

This business scenario describes how to create a new technical address in order to connect a party technical address to a specific network service. This connection allows the shared services to route outbound communication.

You can assign the same network service to more than one technical address of the same party and you can also assign more than one network service to the same technical address.

Before you start, check whether the network service and the technical address exist in CRDM.

This business scenario is not relevant for payment bank users.

Privileges

To carry out this business scenario, you need the following privileges:

❙ Party list query

❙ Party reference data query

❙ Update party

❙ Create technical address network service link

Reference

Further information on screens involved can be found in the screen reference part:

❙ *Parties – search/list* screen [▶]

❙ *Party – details* screen [▶]

❙ *Party – new/edit* screen [▶]

❙ *Technical addresses network services link – new/edit* screen [▶]

Instructions
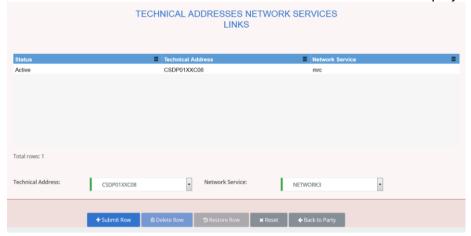
1. Go to the *parties – search/list* screen:
   Common >> Parties >> Parties

2. Enter all search criteria known to you about the party, for which you want to create a new technical address service link.

3. Click on the *search* button.

   ⇨ A list containing the search results is displayed on the screen.

   ⇨ If the search retrieves only one party, the *party – details* screen is displayed directly. Proceed with step 6.

4. Select the relevant party by clicking on an entry in the list.

5. Click on the *details* button.

   ⇨ The *party – details* screen is displayed.

6. Click on the *edit* button

   ⇨ The *party – edit* screen is displayed.

7. Click on the *technical addresses network services links* button.

⇨ The *technical addresses network services link – edit* screen is displayed.

8. Enter all mandatory information in the 'Add Tech. Address Network Service Link' frame.

9. Click on the *submit row* button.

🛈 Repetition

To add more technical addresses network services links, repeat steps 8 and 9.

You can add up to 10 technical addresses network services links.

---

10. Click on the *back to party* button.

⇨ The *party – edit* screen is displayed.

11. Click on the *submit* button.

➡ A new technical address network service link has been created.

4 Annex

4.1 Sitemap
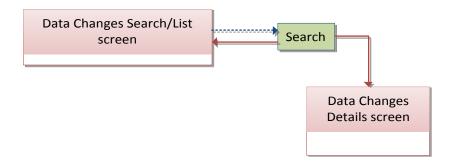
In the following sub-sections the reader may find the hierarchical, structured illustration of all the CRDM screens and their interrelations.

You can find below the legend which explains the meaning of each object, i.e. screen, button, dotted (blue) arrow, solid (red) arrow illustrated in the following diagrams.

Object in the diagram	Description
Data Changes Search/List screen	The object represents a screen.
- - - - - - - ▶	When a button is displayed on the screen, a dotted blue arrow is shown as a link between the screen and the corresponding button.
Search	The object represents a button which is shown in the relevant screen.
◀ ————	After a button is pressed, the result can be displayed either on the same screen or in a different screen (e.g. the details screen).

Illustration 68: Legend of the sitemap

4.1.1 Data Changes
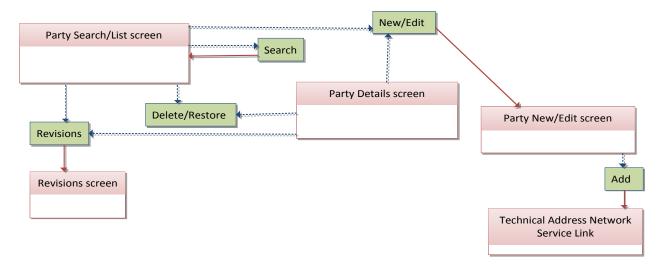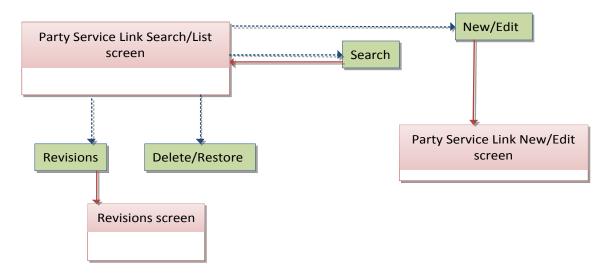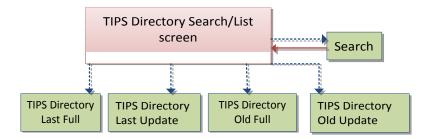
.
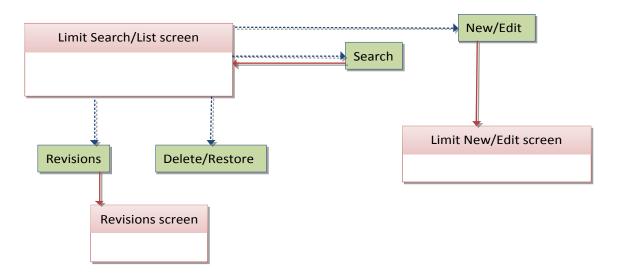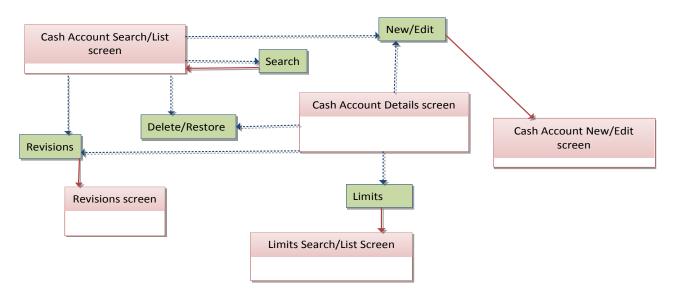
4.1.5 Limits

4.1.6 Cash Account
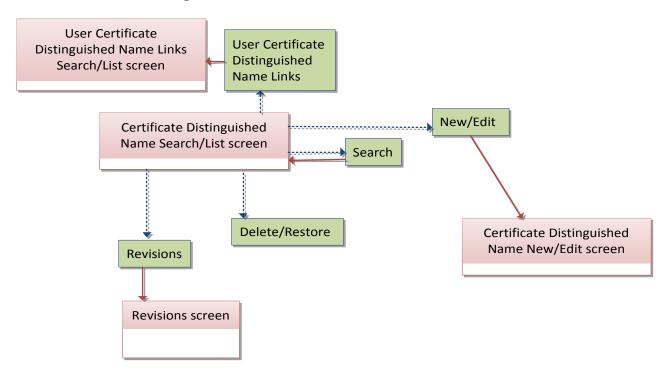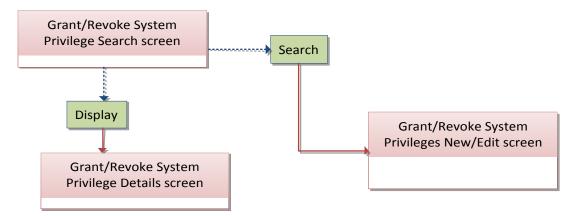
4.1.7 Certificate Distinguished Name

4.1.8 Grant/Revoke Privilege
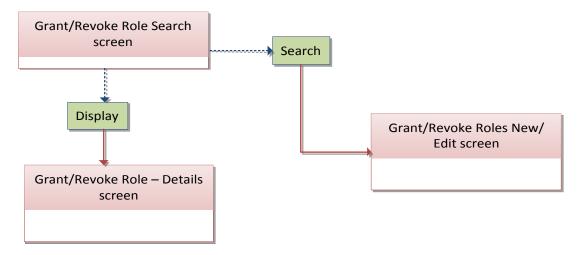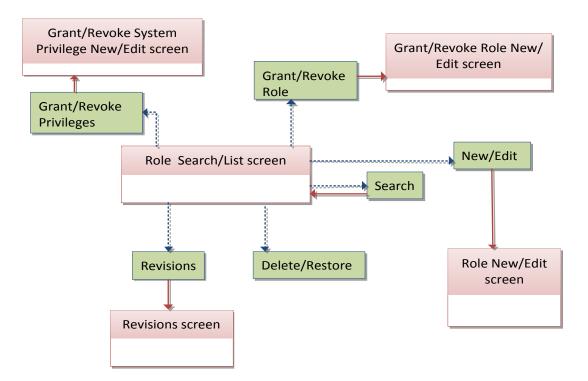
4.1.9 Grant/Revoke Role

4.1.10 Role
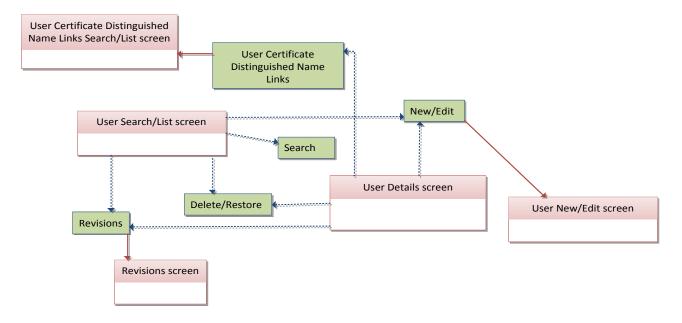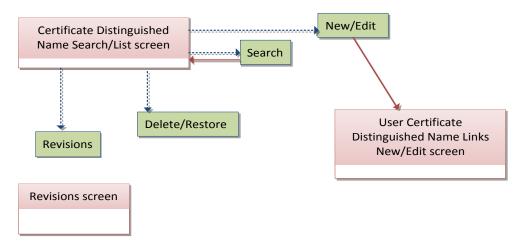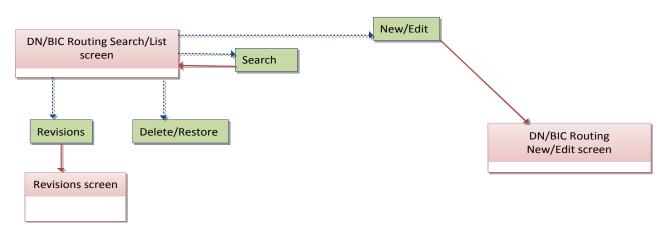
4.1.11 User

4.1.12 User Certificate Distinguished Name Link

4.1.13 Distinguished Name-BIC Routing
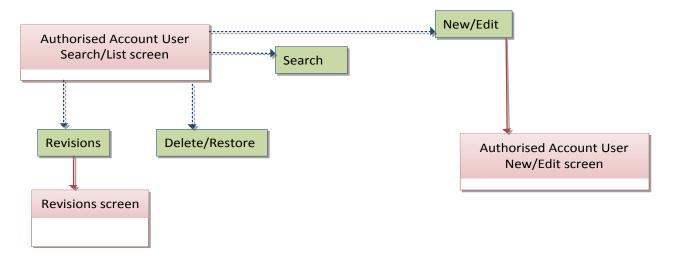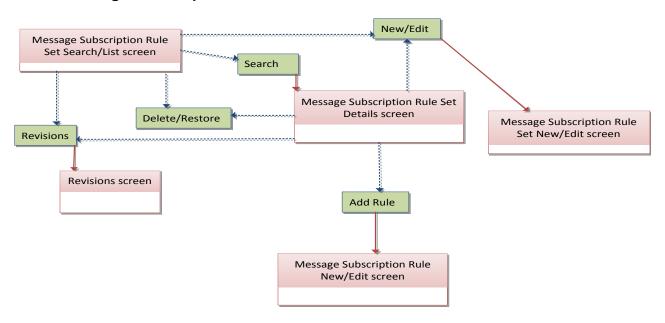
4.1.14 Authorised Account User

4.1.15 Message Subscription Rule Set
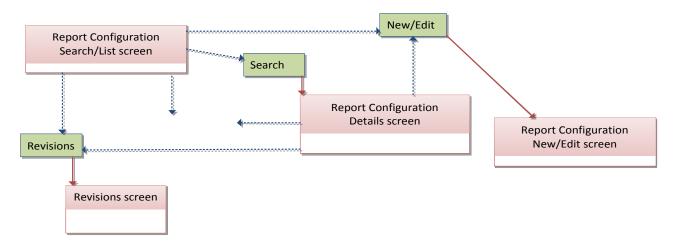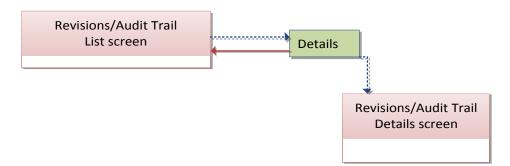
4.1.16 Report Configuration

4.1.17 Restriction Types

4.1.18 Revisions/Audit Trail

4.2 List of Privileges

4.2.1 Reader's Guide

Reader's guide The list of privileges is structured in accordance with the alphabetical screen order and provides detailed information on privilege code, privilege type, object type and screen criteria related to each privilege.

All rights reserved.

4.2.2 Privileges for GUI Screens

4.2.2.1 Authorised Account User – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Delete Authorised Account User	DCA_Delete AuthorisedAccountUser	*Delete* button
Authorised Account User Query	DCQ_Authorised AccountUserListQuery	n/a

4.2.2.2 Authorised Account User – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Authorised Account User	DCA_CreateAuthorised AccountUser	New mode
Update Authorised Account User	DCA_UpdateAuthorised AccountUser	Edit mode

4.2.2.3 Cash Account – Details Screen

Privilege	Privilege Code	Screen Criteria
Cash Account Reference Data Query	DCQ_T2SDedicCashAccReferDataQuery	n/a
Delete Cash Account	DCA_DeleteT2SDedicatedCashAccount	*Delete* button

4.2.2.4 Cash Account – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Cash Account	DCA_CreateT2SDedicatedCashAccount	New mode
Update Cash Account	DCA_UpdateT2SDedicatedCashAccount	Edit mode

4.2.2.5 Cash Account – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Cash Account List Query	DCQ_T2SDedicatedCashAccListQuery	n/a
Delete Cash Account	DCA_DeleteT2SDedicatedCashAccount	*Delete* button
Cash Account Reference	DCQ_T2SDedicCashAccReferDataQuery	*Details* button

Privilege	Privilege Code	Screen Criteria
Data Query		

4.2.2.6 Certificate Distinguished Name – New Screen

Privilege	Privilege Code	Screen Criteria
Create Certificate Distinguish Name	ARM_CreateCertificateDN	New mode

4.2.2.7 Certificate Distinguished Name – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Certificate Query	ARQ_CertificateDNQuery	n/a
Delete Certificate Distinguish Name	ARM_DeleteCertificateDN	Delete Button

4.2.2.8 Data Change – Details Screen

Privilege	Privilege Code	Screen Criteria
Data Changes of a Business Object Details Query	DDQ_DataChan-BusinessObjDetailQuery	n/a

4.2.2.9 Data Changes – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Queued Data Changes Query	SDQ_QueuedDataChangesQuery	n/a

4.2.2.10 Distinguished Name/BIC Routing – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Delete DN-BIC Routing	ARM_DeleteDNBIC	n/a

4.2.2.11 Distinguished Name/BIC Routing – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create DN-BIC Routing	ARM_CreateDNBIC	New Mode
Update DN-BIC Routing	ARM_UpdateDNBIC	Edit Mode

4.2.2.12 Grant/Revoke Privileges – Search Screen

Privilege	Privilege Code	Screen Criteria
Privilege Query	ARQ_PrivilegeQuery	n/a

4.2.2.13 Grant/Revoke Role – Details Screen

Privilege	Privilege Code	Screen Criteria
Granted Roles List Query	ARQ_GrantedRolesListQuery	n/a

4.2.2.14 Grant/Revoke Role – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Grant/Revoke Role	ARM_GrantRole	n/a

4.2.2.15 Grant/Revoke System Privilege – Details Screen

Privilege	Privilege Code	Screen Criteria
Granted System Privileges List Query	ARQ_GrantedSysPrivilegesListQuery	n/a

4.2.2.16 Grant/Revoke System Privilege – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Grant Privilege	ARM_GrantPrivilege	n/a
Revoke Privilege	ARM_RevokePrivilege	n/a
Granted System Privileges List Query	ARQ_GrantedSysPrivilegesListQuery	n/a

4.2.2.17 Grant/Revoke Roles – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Granted Roles List Query	ARQ_GrantedRolesListQuery	n/a
Grant/Revoke Role	ARM_GrantRole	n/a

4.2.2.18 Limit – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Limit	DCA_CreateLimit	New Mode
Update Limit	DCA_UpdateLimit	Edit Mode

4.2.2.19 Limits – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Delete Limit	DCA_DeleteLimit	*Delete* button
Limit Query	DCQ_LimitQuery	n/a

4.2.2.20 Message Subscription Rule – New Screen

Privilege	Privilege Code	Screen Criteria
Create Message Subscription Rule Set	MSU_CreateMessSubsRuleSet	New Mode
Update Message Subscription Rule Set	MSU_UpdateMessSubscriptionRuleSet	Edit Mode

4.2.2.21 Message Subscription Rule Set – Details Screen

Privilege	Privilege Code	Screen Criteria
Message Subscription Rule Set Details Query	MSQ_MessSubscrRuleSetDetailQuery	n/a
Delete Message Subscription Rule Set	MSU_DeleteMessSubscriptionRuleSet	*Delete* button

4.2.2.22 Message Subscription Rule Set – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Message Subscription Rule	MSU_CreateMessageSubscriptionRule	New Mode
Update Message Subscription Rule	MSU_UpdateMessageSubscriptionRule	Edit Mode

4.2.2.23 Message Subscription Rule Sets – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Message Subscription Rule Set List Query	MSQ_MessSubscrRuleSetListQuery	n/a
Message Subscription Rule Sets Details Query	MSQ_MessSubscrRuleSetDetailQuery	n/a
Delete Message Subscription Rule Set	MSU_DeleteMessSubscriptionRuleSet	*Delete* button
Delete Message Subscription Rule	MSU_DeleteMessSubscriptionRule	*Delete* button

4.2.2.24 Parties – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Party List Query	PDQ_PartyListQuery	n/a
Delete Party	PDM_DeleteParty	*Delete* button

4.2.2.25 Party – Details Screen

Privilege	Privilege Code	Screen Criteria
Party Reference Data Query	PDQ_PartyReferDataQuery	n/a
Delete Party	PDM_DeleteParty	*Delete* button
Technical Address Network Service Link Details Query	NCQ_DisplayTechAddressNetSerLink	Technical address network services link button

4.2.2.26 Party – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Party	PDM_CreateParty	n/a
Update Party	PDM_UpdateParty	*Delete* button
Create Technical Address Network Service Link	NCO_CreateTechnAddressNetServLink	Technical address network services link button

4.2.2.27 Party Service Link – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Delete Party-Service Link	PDM_DeletePartyServiceLink	*Delete* button
Party-Service Link List Query	PDQ_PartyServiceLinkListQuery	n/a

4.2.2.28 Party Service Link – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Party-Service Link	PDM_CreatePartyServiceLink	New mode
Update Party-Service Link	PDM_UpdatePartyServiceLink	Edit mode

4.2.2.29 Privileges – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Privilege Query	ARQ_PrivilegeQuery	n/a

4.2.2.30 Report Configuration – Details Screen

Privilege	Privilege Code	Screen Criteria
Report Configuration Details Query	RCO_ReportConfigDetailQuery	n/a
Delete Report Configuration	RCO_DeleteReportConfiguration	*Delete* button

4.2.2.31 Report Configuration – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Report Configuration	RCO_CreateReportConfiguration	New mode
Update Report Configuration	RCO_UpdateReportConfiguration	Edit mode

4.2.2.32 Report Configuration – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Report Configuration List Query	RCO_ReportConfigListQuery	n/a
Delete Report Configuration	RCO_DeleteReportConfiguration	*Delete* button

4.2.2.33 Restriction Type – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Market-specific Restriction List Query	MSA_Market-SpecRestrictListQuery	n/a

4.2.2.34 Restriction Type Rule – Details Screen

Privilege	Privilege Code	Screen Criteria
Market-Specific Restriction Type Rule Detail Query	MSA_Market-SpecRestrictDetailQuery	n/a
Market-Specific Restriction Type Rule Parameter Details Query	MSA_MarkSpecRestrTypeRuleParamDetQ	n/a

4.2.2.35 Revisions/Audit Trail – Details Screen

Privilege	Privilege Code	Screen Criteria
Party Audit Trail Query	PDQ_PartyAudTrailQuery	n/a
Cash Account Audit Trail Query	DCQ_T2SDedicCashAccAudTrailQuery	n/a
Residual Static Data Audit Trail Query	SDQ_ResidualStaticDataAudTrailQuery	n/a

4.2.2.36 Revisions/Audit Trail – List Screen

Privilege	Privilege Code	Screen Criteria
Party Audit Trail Query	PDQ_PartyAudTrailQuery	n/a
Cash Account Audit Trail Query	DCQ_T2SDedicCashAccAudTrailQuery	n/a
Residual Static Data Audit Trail Query	SDQ_ResidualStaticDataAudTrailQuery	n/a

4.2.2.37 Role – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Role	ARM_CreateRole	New mode
Update Role	ARM_UpdateRole	Edit mode

4.2.2.38 Roles – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Role List Query	ARQ_RoleListQuery	n/a
Delete Role	ARM_DeleteRole	n/a

4.2.2.39 Technical Addresses Network Service Link – Details Screen

Privilege	Privilege Code	Screen Criteria
Technical Address Network Service Link Details Query	NCQ_DisplayTechAddressNetSerLink	n/a

4.2.2.40 Technical Addresses Network Service Link – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create Technical Address Network Service Link	NCO_CreateTechnAddressNetServLink	New mode
Delete Technical Address Network Service Link	NCO_DeleteTechnAddressNetServLink	*Delete* button

4.2.2.41 TIPS Directory – Search/List screen

Privilege	Privilege Code	Screen Criteria
TIPS Directory Query	SDQ_TIPSDirectoryQuery	n/a

4.2.2.42 User – Details Screen

Privilege	Privilege Code	Screen Criteria
System User Query (T2S Actor Query)	ARQ_T2SSysUserQueryT2SActorQuery	n/a
Delete User	ARM_DeleteUser	*Delete* button

4.2.2.43 User – New/Edit Screen

Privilege	Privilege Code	Screen Criteria
Create User	ARM_CreateUser	New mode
Update User	ARM_UpdateUser	Edit mode

4.2.2.44 User Certificate Distinguished Name Link – New Screen

Privilege	Privilege Code	Screen Criteria
Create User Certificate Distinguish Name Link	ARM_CreateUserCertificDNLink	New mode

4.2.2.45 User Certificate Distinguished Name Link – Search/List Screen

Privilege	Privilege Code	Screen Criteria
Delete User Certificate Distinguish Name Link	ARM_DeleteUserCertificDNLink	*Delete* button
System User Link Query	ARQ_UserCertifDNLinkQuery	n/a

4.2.2.46 Users – Search/List Screen

Privilege	Privilege Code	Screen Criteria
System User Query (T2S Actor Query)	ARQ_T2SSysUserQueryT2SActorQuery	n/a
Delete User	ARM_DeleteUser	*Delete* button

4.3 List of References for Error Messages

4.3.1 Reader's Guide

Reader's Guide

This section includes a list of references for error messages for all screens. The list of references for error messages consists of a general section, which lists overall error codes that apply to all GUI screens, and a section listing all error codes relevant for using the 4-eyes mode in GUI screens. For all sections, these are followed by specific sections for individual screens, which are organised in alphabetical screen order and specify the respective error codes applicable for each screen. Each error code table entry includes the error text and the description.

Please bear in mind that the Error Message description may make references to T2S reference data objects since the underlying Business Rules may be used for the creation of reference data for T2S when CRDM may be used for T2S also.

4.3.2 References for error messages for GUI screens

4.3.2.1 All

Reference for error message	Field or Button	Error Text	Description
DXAA007		Only one instance may become effective in the future	Each historical entity may have no more than one future instance.

4.3.2.2 All screens which allow the initiation of a second user

Reference for error message	Field or Button	Error Text	Description
DXAA002		Data awaiting for approval cannot be modified	It is not allowed to perform a maintenance request, neither in 2-eyes nor in 4-eyes first step mode, that refers to an instance already awaiting for approval.
DXAA011		Invalid approval requestor (must be different from the first requestor)	In case of approval request (4-eyes second step), the requestor must be different from the requestor of the first step. It can be equal only in case of revocation (confirmation = 'NO')
DXAA035		Request to be approved not found	In case of approval request (4-eyes second step), the request must refer to an existing instruction and the related entity(ies) must be in status 'Awaiting approval'.

4.3.2.3 Authorised Account User – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DCD2001	❙ Delete button	Requestor not allowed	Authorised Account Users can be deleted or restored only by the Service Operator, NCBs or Payment Banks. NCBs can delete or restore Authorised Account Users within their own System Entities. Payment Banks can delete or restore Authorised Account Users for Cash Accounts owned by them.
DCD2002	❙ Delete button	Unknown, deleted or open	Deletion requests must refer to existing, active and closed Authorised Account

		Authorised Account User	Users.
DCD2003	❙ Restore button	Unknown, active or open Authorised Account User	Restore requests must refer to existing, deleted and non-open Authorised Account Users.
DCD2004	❙ Restore button	Unknown, deleted, closed or invalid Cash Account	In a restore request, the Cash Account Identifier must refer to an existing, active and non-closed Cash Account with Account Type 'TIPS Account' or 'TIPS Credit Memorandum Balance'.
DCD2005	❙ Restore button	Unknown or deleted BIC	In a restore request, the BIC Mnemonic must refer to an existing and active BIC.
DCD2006	❙ Restore button	Authorised Account user already defined for this BIC	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.
DCD2007	❙ Restore button	Authorised Account User already defined for this TIPS CMB	At any given point in time, there cannot be more than one Authorised Account User for each TIPS Credit Memorandum Balance.
DCD2008	❙ Delete button	Deletion not allowed due to a priority constraint	In a delete request, there cannot be any DN-BIC Routing instances referencing the same BIC as the Authorised Account User.

4.3.2.4 Authorised Account User – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DCC2001	❙ Submit button	Requestor not allowed	Authorised Account Users can be created only by the Service Operator, NCBs or Payment Banks. NCBs can create Authorised Account Users for Cash Accounts within their own System Entities. Payment Banks can create Authorised Account users for TIPS Accounts owned by them and for the TIPS CMBs linked to them.
DCC2002	❙ Cash Account Number field ❙ Submit button	Unknown or invalid Cash Account	The Cash Account Identifier must refer to an existing, active and non-closed Cash Account with Account Type 'TIPS Account' or 'TIPS Credit Memorandum Balance'.
DCC2003	❙ Authorised Account User BIC field ❙ Submit button	Unknown or invalid BIC	The BIC Mnemonic must refer to an existing and active BIC.
DCC2004	❙ Valid From field	Valid From cannot be set to a past	The Valid From must be equal to or greater than the current business date.

		date	
DCC2005	❚ Valid To field ❚ Submit button	Valid To cannot be set to a past date or to a date before Valid From	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.
DCC2006	❚ Submit button	Authorised Account user already defined for this BIC in the related Cash Account Currency	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.
DCC2007	❚ Submit button	Authorised Account User already defined for this TIPS CMB	At any given point in time, there cannot be more than one Authorised Account User for each TIPS Credit Memorandum Balance.
DCU2001	❚ Submit button	Requestor not allowed	Authorised Account Users can be updated only by the Service Operator, NCBs or Payment Banks. NCBs can update Authorised Account Users within their own System Entities. Payment Banks can update Authorised Account users for TIPS Accounts owned by them and for the TIPS CMBs linked to them.
DCU2002	❚ Cash Account Number field ❚ Submit button	Unknown or invalid Authorised Account User	The Authorised Account User to be updated must refer to an existing, active and non-closed instance.
DCU2003	❚ Valid From field ❚ Submit button	Valid From cannot be modified	The Valid From can be updated only if the current value is later than the current business date.
DCU2004	❚ Valid From field ❚ Submit button	Valid From cannot be set to a past date or later than existing DN-BIC Routing Valid From	The modified Valid From must be equal to or later than the current business date and equal to or earlier than the Valid From of all DN-BIC Routing instances referencing the same BIC as the Authorised Account User.
DCU2005	❚ Valid To field ❚ Submit button	Valid To cannot be set to a past date, to a date before Valid From or earlier than existing DN-BIC Routing Valid To	The Valid To must be equal to or later than the current business date, equal to or later than the Valid From and equal to or later than the Valid To of all DN-BIC Routing instances referencing the same BIC as the Authorised Account User.
DCU2006	❚ Submit button	Authorised Account user already defined for this BIC in the related Cash Account Currency	At any given point in time, there cannot be more than one Authorised Account User for each BIC in any given Currency.
DCU2007	❚ Submit button	Authorised Account User	At any given point in time, there cannot be more than one Authorised Account User for

		already defined for this TIPS CMB	each TIPS Credit Memorandum Balance.

4.3.2.5 Cash Account – Details Screen

Reference for error message	Field or Button	Error Text	Description
DCD1001	❙ Delete button	Requestor not allowed	When performing a Cash Account delete or restore request, the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only delete or restore Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only delete or restore TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the relevant Party holding the account.
DCD1003	❙ Opening Date field ❙ Closing Date field ❙ Delete button	Unknown Cash Account. The account must be closed or have Opening Date greater than the current date.	The delete requests of Cash Accounts must refer to an existing and active instance. The account to be deleted must be already closed or must have Opening Date greater than the current date.
DCD1012	❙ Opening Date field ❙ Closing Date field ❙ Restore button	Cash Account cannot be restored	When performing a Cash Account restore request it must refer to an existing and deleted Cash Account. The account to be restored must have Closing date equal to or earlier than the Current Business date or Opening date equal to or later than the Current Business date; in addition, the Opening date must be equal to or later than the Account Holder Opening Date and the Closing Date must be equal to or earlier than the Account Holder Closing Date.
DCD1013	❙ Account Type field ❙ Restore button	Transit account already existing for this currency	When performing a Cash Account restore request, when restoring an RTGS Dedicated Transit Account or a TIPS Transit Account, no other Transit Account must be already associated to the relevant currency in the same validity period.
DCD1014	❙ Account Type field	Deletion not allowed due to	When performing a Cash Account delete request, in case of deletion of a future

	▌ Delete button	open Cash Accounts related to this Transit Account	RTGS Dedicated Transit Account or TIPS Transit Account, no active Cash Accounts with the same currency for T2S or TIPS respectively must exist in T2S.
DCD1030	▌ Delete button	The deletion/close is not allowed due to a deletion priority constraint	A Cash Account cannot be deleted if there still are valid instances of the following entities linked to it: Liquidity Transfer Order, Liquidity Transfer Order Link Set, Credit Memorandum Balance, TIPS Credit Memorandum Balance-type Cash Account.
DCD1082	▌ Currency field ▌ Restore button	Unknown currency code	When performing a Cash Account restore request the currency code of the Cash Account to be restored must refer to an existing currency code in CRDM with Settlement Currency set to True or a Currency-Service Link in place with the relevant Service.
DCD1083	▌ Party Parent BIC field ▌ Party BIC field ▌ Restore button	Unknown Party	When performing a Cash Account restore request the account holder must be an existing and active Party in CRDM with Party Type equal to NCB or Payment Bank.
DCD1084	▌ Type field ▌ Restore button	Invalid restriction type	When performing a Cash Account restore request, all restrictions associated to the Cash Account to be restored must refer to existing Restriction Types whose Object Restriction Type is Cash Account.
DCD1085	▌ External RTGS Account field ▌ Restore button	Unknown External RTGS Account	When performing a Cash Account restore request the Linked Account of the Cash Account, T2S Central Bank Account or RTGS Dedicated Transit Account to be restored must refer to an existing External RTGS Account in T2S.
DCD1086	▌ Restore button	Unknown linked Cash Account	When performing a Cash Account restore request the Linked Account of the TIPS Credit Memorandum Balance to be restored must refer to an existing and open TIPS Account in CRDM.
DCD1207	▌ External RTGS Account field ▌ Currency field ▌ Restore button	Invalid External RTGS Account Currency Code	When performing a Cash Account restore request, if the Cash Account to be restored is linked to an External RTGS Account, they must have the same currency code.
DCD1532	▌ Restore button	Transit Account not found or not valid	When performing a Cash Account restore request, the validity period of a TIPS Account, Cash Account or T2S Central Bank Account must be consistent with the validity period of the relevant Transit Account.
DCD1555	▌ Account Type field ▌ Party Type field ▌ Restore button	Invalid relations between account type and party type	When performing a Cash Account restore request the relation between the Account Type to be restored and the Party Type of the account holder is checked.

4.3.2.6 Cash Account – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DCC1001	∎ Parent BIC field ∎ Party BIC field ∎ Submit button	Requestor not allowed	When performing a Cash Account create request, the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only create Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only create TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rules are represented by any user that is granted the appropriate privilege(s) on the specific Party to be linked to the account.
DCC1024	∎ Restriction field ∎ Submit button	Invalid restriction type	When performing a Cash Account create request, the Restriction Type must refer to an existing Restriction Type with Object Restriction Type equal to Cash Account and belonging to the same system entity of the Cash Account or of the Service Operator.
DCC1025	∎ Valid From field ∎ Submit button	"Valid From" invalid	When performing a Cash Account create request, the Valid From specified in the Cash Account Restriction section must be equal to or greater than the current timestamp.
DCC1100	∎ Issue Currency field ∎ Submit button	Currency Code not found	When performing a Cash Account create request the Currency Code must refer to an existing instance in CRDM with Settlement Currency set to True or a Currency-Service Link in place with the relevant Service.
DCC1101	∎ Floor Notification field ∎ Ceiling Notification field ∎ Submit button ∎ Parent BIC field	Invalid Floor Notification Amount/Ceiling Notification Amount	When performing a Cash Account create request the Floor Notification Amount specified must be less than the Ceiling Notification Amount.
DCC1103	∎ Submit button ∎ Cash Account Number field	Cash Account Number already assigned	When performing a Cash Account create request, the Cash Account Number must be compliant with ISO 20022 standards and it must not be already assigned to any other Cash Account in CRDM.

DCC1205	❙ Opening Date field ❙ Submit button	"Opening Date" invalid	When performing a Cash Account create request the Opening Date must be equal to or greater than the current date and be equal or greater than the Account Holder Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.
DCC1206	❙ RTGS Account field ❙ Submit button	Invalid External RTGS account	When performing a Cash Account create request to create a Cash Account, RTGS Dedicated Transit Account or T2S Central Bank Account, the Linked Account must refer to an existing and open External RTGS Account instance in CRDM.
DCC1207	❙ RTGS Account field ❙ Submit button ❙ Currency field	Invalid Currency code	When performing a Cash Account create request, if the Linked Account references an External RTGS Account it must have the same currency code of the Cash Account.
DCC1208	❙ Valid from field ❙ Submit button	"Valid From" invalid	When performing a Cash Account create request, in case of request of creation of Cash Account Restriction, the Valid From of the Cash Account Restriction must be equal or greater than the Valid From of the Restriction Type entity.
DCC1209	❙ Valid from field ❙ Submit button	"Valid To" invalid	When performing a Cash Account create request, in case of request of creation of Cash Account Restriction, the Valid To of the Cash Account Restriction must be equal or less than the Valid To of the Restriction Type entity.
DCC1210	❙ Closing Date field ❙ Submit button	"Closing Date" invalid	When performing a Cash Account create request the Closing Date specified in the request must be equal to or greater than the Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.
DCC1212	❙ Valid To field ❙ Submit button	"Valid To" invalid	When performing a Cash Account create request, the Valid To specified in the Cash Account Restriction section must be equal to or greater than the Valid From.
DCC1300	❙ Type field ❙ Valid from field ❙ Valid to field ❙ Submit button	Cash Account Restriction overlaps with existing instance	When performing a Cash Account Create request, in case of request for creation of a Cash Account Restriction, the created restriction must not overlap with any other Cash Account Restriction in input having the same Restriction Type.
DCC1524	❙ Parent BIC field ❙ Party BIC field	Invalid Party Mnemonic	When performing a Cash Account create request, the account holding Party must refer to an existing active and open instance in CRDM with Party Type equal to NCB or Payment Bank.
DCC1530	❙ Submit button	Transit account already existing	When performing a Cash Account create request, when creating an RTGS Dedicated

	▌ Currency field	for this currency	Transit Account, no other account of the same type must be already associated to the relevant currency.
DCC1531	▌ Submit button ▌ Account type field ▌ Currency field	Transit account not found for this currency	When performing a Cash Account create request, when creating a Cash Account or a central bank account, there must be an RTGS Dedicated Transit Account related to the relevant currency.
DCC1532	▌ Closing Date field ▌ Account type field ▌ Submit button	Transit account not found for this currency	When performing a Cash Account create request, when creating a TIPS Account, there must be a TIPS Transit Account related to the relevant currency.
DCC1555	▌ Type field ▌ Party Type field ▌ Submit button	Invalid relations between account type and party type	When performing a Cash Account create request check the relation between the Account Type to be created and the Party Type of the account holder.
DCC1601	▌ Submit button		When performing a Cash Account Create request, in case of immediate setup of Cash Account Restriction, the timestamp to be used must take a conventional value which the system will interpret as the current timestamp. Furthermore, no check must be performed on such a conventional value in case of four eyes second step or processing of retrieved queued requests.
DCC1800	▌ Floor Notification Amount field ▌ Ceiling Notification Amount field ▌ Submit button	Invalid number of decimals	When performing a Cash Account Create request, the number of decimals in the values provided for Floor Notification Amount and Ceiling Notification Amount must be compliant with the number of decimals foreseen for the relevant currency.
DCU1001	▌ Parent BIC field ▌ Party BIC field ▌ Submit button	Requestor not allowed	When performing a Cash Account update request the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only update Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Users belonging to Payment Banks can only update TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the relevant Party holding the account.
DCU1003	▌ Account Identifier field ▌ Submit button	Data to be updated not found	The update requests of a Cash Account must refer to an existing and active account. Furthermore, the Closing Date must be equal to or greater than the current date.

DCU1024	❙ Restriction field ❙ Submit button	Invalid restriction type	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Restriction Type must refer to an existing Restriction Type with Object Restriction Type equal to Cash Account and belonging to the same system entity of the Cash Account or of the Service Operator.
DCU1030	❙ Submit button	The account cannot be closed due to a closure priority constraint	A Cash Account cannot be closed if there still are valid instances of the following entities linked to it: Liquidity Transfer Order, Liquidity Transfer Order Link Set.
DCU1040	❙ Submit button	Opening/Closing Date not consistent with linked TIPS CMB	When performing a Cash Account update request, any update of the Opening Date and Closing Date must be consistent with the validity periods of other existing Cash Accounts with type 'TIPS Credit Memorandum Balance' linking to it.
DCU1101	❙ Floor Notification field ❙ Ceiling Notification field ❙ Submit button	Invalid Floor Notification Amount/Ceiling Notification Amount	When performing a Cash Account update request, the Floor Notification Amount must be less than the Ceiling Notification Amount
DCU1204	❙ Submit button	Invalid use of Linked Account	When performing a Cash Account update request, the Linked Account can be specified only for TIPS Credit Memorandum Balances, RTGS Dedicated Transit Accounts, T2S Central Bank Accounts and Cash Accounts.
DCU1206	❙ RTGS Account field ❙ Submit button	Invalid External RTGS account	When performing a Cash Account update request, the Linked Account, when it refers to an External RTGS Cash Account, must refer to an existing and open instance in CRDM.
DCU1207	❙ RTGS Account field ❙ Submit button	Invalid External RTGS account	When performing a Cash Account update request, if the Linked Account references an External RTGS Account it must have the same currency code of the Cash Account.
DCU1210	❙ Closing Date field ❙ Submit button	"Closing Date" Invalid	When performing a Cash Account update request, the Closing Date must be equal to or greater than the current date and equal to or greater than the Cash Account Opening Date. Furthermore it must be equal to or less than the Account Holder Closing Date.
DCU1211	❙ Valid From field ❙ Submit button	"Valid From" invalid	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid From must be equal to or greater than the current timestamp.
DCU1212	❙ Valid To field ❙ Submit button	"Valid To" invalid	When performing a Cash Account update request, in case of request of creation/update of Cash Account

			Restriction, the Valid To specified in the Cash Account Restriction section must be equal to or greater than the current timestamp and must be equal to or greater than the Valid From.
DCU1213	▮ Opening Date field ▮ Submit button	"Opening Date" Invalid	When performing a Cash Account update request, the Opening Date can be updated only if the existing one is greater than the current date and the new one must be equal to or greater than the current date. Furthermore it must be equal to or greater than the Account Holder Opening Date and equal to or less than the Account Holder Closing Date.
DCU1214	▮ Submit button	Invalid linked account	When performing a Cash Account update request on the Linked Account, Opening Date and/or Closing Date of a TIPS Credit Memorandum Balance, the Linked Account must refer to an existing Cash Account instance in CRDM with type "TIPS Cash Account" which is open throughout the specified validity period of the TIPS CMB being updated.
DCU1216	▮ Valid From field ▮ Submit button	Restriction cannot be deleted	When performing a Cash Account update request, in case of request of deletion of Cash Account Restriction, the Valid From must be greater than the current timestamp or the Cash Account Restriction must be closed.
DCU1217	▮ Restriction field ▮ Submit button	Account is not restricted	When performing a Cash Account update request, case of request of update of Cash Account Restriction, it must refer to an existing Cash Account Restriction with a non-past Valid To.
DCU1218	▮ Submit button	Invalid Currency Code	When performing a Cash Account update request, the specified Currency Code must refer to the one already linked to the existing Cash Account.
DCU1219	▮ Valid From field ▮ Submit button	"Valid From" invalid	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid From of the Cash Account Restriction must be equal or greater than the Valid From of the Restriction Type.
DCU1220	▮ Valid to field ▮ Submit button	"Valid To" invalid	When performing a Cash Account update request, in case of request of creation of Cash Account Restriction, the Valid To of the Cash Account Restriction must be equal or less than the Valid To of the Restriction Type.
DCU1300	▮ Type field ▮ Valid from field	Cash Account Restriction	When performing a Cash Account Update request, in case of request for

Reference for error message	Field or Button	Error Text	Description
	❙ Valid to field ❙ Submit button	overlaps with existing instance	creation/update of Cash Account Restriction, the new or updated restriction must not overlap with any other Cash Account Restrictions having the same Restriction Type on the same Cash Account.
DCU1313	❙ Closing date field ❙ Floor Notification Amount field ❙ Submit button	Open Cash Accounts exist related to this Transit Account	When performing a Cash Account update request, in case of update of the Opening or Closing Date of an RTGS Dedicated Transit Account or TIPS Transit Account, no active Cash Account with the same currency for T2S and TIPS respectively must be open outside of the Transit Account validity period.
DCU1532	❙ Submit button	No valid Transit Account found for the specified validity period	When performing a Cash Account Update request, the validity period of the TIPS Account, Cash Account or T2S Central Bank Account must be contained within the validity period of the relevant Transit Account.
DCU1555	❙ Submit button	Party-Service Link for TIPS not found or not valid	When performing a Cash Account Update request, Cash Accounts for TIPS require an existing and active Part-Service Link to be in place between the Owner Party and TIPS for the relevant validity period.
DCU1600	❙ Submit button		When performing a Cash Account Update request, in case of immediate setup or removal of Cash Account Restriction, the timestamp to be used must take a conventional value which the system will interpret as the current timestamp. Furthermore, no check must be performed on such a conventional value in case of four eyes second step or processing of retrieved queued requests.
DCU1800	❙ Floor Notification Amount field ❙ Ceiling Notification Amount field ❙ Submit button	Invalid number of decimals	When performing a Cash Account Update request, the number of decimals in the values provided for Floor Notification Amount and Ceiling Notification Amount must be compliant with the number of decimals foreseen for the relevant currency.

4.3.2.7 Cash Accounts – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DCD1001	❙ Search button ❙ Restore button ❙ Delete button	Requestor not allowed	When performing a Cash Account delete or restore request, the Party Type of the Requestor must be NCB or Payment Bank. Users belonging to NCBs can only delete or

			restore Cash Accounts for Parties that fall under their responsibility according to the Hierarchical Party Model, or TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility.
			Users belonging to Payment Banks can only delete or restore TIPS Credit Memorandum Balances linked to Cash Accounts that fall under their responsibility.
			Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the account or on the relevant Party holding the account.
DCD1003	▌ Status field ▌ Delete button ▌ Closing date field ▌ Opening date field	Unknown Cash Account. The account must be closed or have Opening Date greater than the current date.	The delete requests of Cash Accounts must refer to an existing and active instance. The account to be deleted must be already closed or must have Opening Date greater than the current date.
DCD1012	▌ Status field ▌ Restore button ▌ Closing date field ▌ Opening date field ▌ Delete button	Cash Account cannot be restored	When performing a Cash Account restore request it must refer to an existing and deleted Cash Account. The account to be restored must have Closing date equal to or earlier than the Current Business date or Opening date equal to or later than the Current Business date; in addition, the Opening date must be equal to or later than the Account Holder Opening Date and the Closing Date must be equal to or earlier than the Account Holder Closing Date.
DCD1013	▌ Account Type field ▌ Restore button	Transit account already existing for this currency	When performing a Cash Account restore request, when restoring an RTGS Dedicated Transit Account or a TIPS Transit Account, no other Transit Account must be already associated to the relevant currency in the same validity period.
DCD1014	▌ Account Type field ▌ Delete button	Deletion not allowed due to open Cash Accounts related to this Transit Account	When performing a Cash Account delete request, in case of deletion of a future RTGS Dedicated Transit Account or TIPS Transit Account, no active Cash Accounts with the same currency for T2S or TIPS respectively must exist in T2S.
DCD1030	▌ Delete button	The deletion/close is not allowed due to a deletion priority constraint	A Cash Account cannot be deleted if there still are valid instances of the following entities linked to it: Liquidity Transfer Order, Liquidity Transfer Order Link Set, Credit Memorandum Balance, TIPS Credit Memorandum Balance-type Cash Account.
DCD1082	▌ Restore button ▌ Currency field	Unknown currency code	When performing a Cash Account restore request the currency code of the Cash Account to be restored must refer to an existing currency code in CRDM with

Reference for error message	Field or Button	Error Text	Description
			Settlement Currency set to True or a Currency-Service Link in place with the relevant Service.
DCD1083	❙ Parent BIC field ❙ Party BIC field ❙ Restore button	Unknown Party	When performing a Cash Account restore request the account holder must be an existing and active Party in CRDM with Party Type equal to NCB or Payment Bank.
DCD1084	❙ Type field ❙ Restore button	Invalid restriction type	When performing a Cash Account restore request, all restrictions associated to the Cash Account to be restored must refer to existing Restriction Types whose Object Restriction Type is Cash Account.
DCD1085	❙ RTGS Account Number field ❙ Restore button	Unknown External RTGS Account	When performing a Cash Account restore request the Linked Account of the Cash Account, T2S Central Bank Account or RTGS Dedicated Transit Account to be restored must refer to an existing External RTGS Account in T2S.
DCD1086	❙ Restore button	Unknown linked Cash Account	When performing a Cash Account restore request the Linked Account of the TIPS Credit Memorandum Balance to be restored must refer to an existing and open TIPS Account in CRDM.
DCD1207	❙ RTGS Account Number field ❙ Restore button ❙ Currency field	Invalid External RTGS Account Currency Code	When performing a Cash Account restore request, if the Cash Account to be restored is linked to an External RTGS Account, they must have the same currency code.
DCD1532	❙ Restore button	Transit Account not found or not valid	When performing a Cash Account restore request, the validity period of a TIPS Account, Cash Account or T2S Central Bank Account must be consistent with the validity period of the relevant Transit Account.
DCD1555	❙ Account Type field ❙ Party Type field ❙ Restore button	Invalid relations between account type and party type	When performing a Cash Account restore request the relation between the Account Type to be restored and the Party Type of the account holder is checked.

4.3.2.8 Certificate Distinguished names – Search/List

Reference for error message	Field or Button	Error Text	Description
DRDA001	❙ Restore button ❙ Delete button	Requestor not allowed	A Certificate DN can be deleted or restored only by users with the correct privilege.

DRDA002	❚ Certificate Distinguished Name field ❚ Restore button	Distinguished Name already used	When performing a Certificate DN Restore request, the Distinguished Name must not be already used within active instances in CRDM.
DRDA003	❚ Status field ❚ Delete button	Unknown or not active Certificate DN	When performing a Certificate DN Delete request, it must refer to an existing and active Certificate DN.
DRDA004	❚ Status field ❚ Restore button	Unknown or not deleted Certificate DN	When performing a Certificate DN Restore request, it must refer to an existing and deleted Certificate DN.
DRDA010	❚ Delete button	Certificate DN is linked to a User	When performing a Certificate DN Delete request, it must refer to a Certificate DN not actively linked to any User.

4.3.2.9 Certificate Distinguished names – New Screen

Reference for error message	Field or Button	Error Text	Description
DRCA001	❚ Submit button	Requestor not allowed	A Certificate DN can be created only by users with the correct privilege.
DRCA002	❚ Certificate Distinguished Name field ❚ Submit button	Distinguished Name already used	When performing a Certificate DN Create request, the Distinguished Name must not be already used within active instances in CRDM.

4.3.2.10 Data changes – Details screen

No references for error messages.

4.3.2.11 Data changes – Search/List screen

No references for error messages.

4.3.2.12 Distinguished Name–BIC Routing – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRD8001	❚ Delete button ❚ Restore button	Requestor not allowed	DN-BIC Routing can be deleted or restored only by the Service Operator, NCBs or Payment Banks. NCBs can delete or restore DN-BIC Routings within their own System Entities. Payment Banks can delete or restore DN-BIC Routings that reference DNs linked to

			their own Users and BICs authorised to act on their own accounts.
DRD8002	❚ Delete button	Unknown, deleted or open DN-BIC Routing	Deletion requests must refer to existing, active and closed DN-BIC Routings.
DRD8003	❚ Restore button	Unknown, active or open DN-BIC Routing	Restore requests must refer to existing, deleted and non-open DN-BIC Routings.
DRD8004	❚ Restore button	Unknown, deleted or invalid Distinguished Name	In a restore request, the Distinguished Name Identifier must refer to an existing and active Certificate DN which is linked to at least one User of the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the User to be within the same System Entity.
DRD8005	❚ Restore button	Unknown, deleted or invalid BIC	In a restore request, the BIC Mnemonic must refer to an existing and active BIC which is linked to at least one Authorised Account User referencing an Account owned by the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the Account to be within the same System Entity.
DRD8006	❚ Search button	DN-BIC Routing already defined for this BIC, DN and Direction	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.
DRD8007	❚ Search button	Outbound DN-BIC Routing already defined for this BIC	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic.

4.3.2.13 Distinguished Name–BIC Routing – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRC8001	❚ Submit button	Requestor not allowed	DN-BIC Routing can be created only by the Service Operator, NCBs or Payment Banks. NCBs can create DN-BIC Routing acting on behalf of their TIPS Participants. Payment Banks can create DN-BIC Routing for the BIC which currently identifies their own Party.
DRC8002	❚ Distinguished Name field ❚ Submit button	Unknown or invalid Distinguished Name	The Distinguished Name specified in input must refer to an existing and active Certificate DN which is linked to at least one User of the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the User to be within the same

			System Entity.
DRC8003	▌ BIC field ▌ Submit button	Unknown or invalid BIC	The BIC Mnemonic must refer to an existing and active BIC which is linked in the same validity period to at least one Authorised Account User referencing an Account owned by the Requestor Party. If the Requestor Party is a Central Bank, it is sufficient for the Account to be within the same System Entity.
DRC8004	▌ Valid from field ▌ Submit button	Valid From cannot be set to a past date	The Valid From must be equal to or greater than the current business date.
DRC8005	▌ Valid to field ▌ Submit button	Valid To cannot be set to a past date or to a date before Valid From	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.
DRC8006	▌ Submit button	DN-BIC Routing already defined for this BIC, DN and Direction	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.
DRC8007	▌ Submit button	Outbound DN-BIC Routing already defined for this BIC	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic.
DRU8001	▌ Submit button	Requestor not allowed	DN-BIC Routings can be updated only by the Service Operator, NCBs or Payment Banks. NCBs can update DN-BIC Routings within their own System Entities. Payment Banks can update DN-BIC Routings that reference DNs linked to their own Users and BICs authorised to act on their own accounts.
DRU8002	▌ Submit button	Unknown or invalid DN-BIC Routing	The DN-BIC Routing to be updated must refer to an existing, active and non-closed instance.
DRU8003	▌ Valid from field ▌ Submit button	Valid From cannot be modified	The Valid From can be updated only if the current value is greater than the current business date.
DRU8004	▌ Valid from field ▌ Submit button	Valid From cannot be set to a past date or earlier than the related Authorised Account User	The modified Valid From must be equal to or later than the current business date and equal to or later than the Valid From of the Authorised Account User referencing the BIC.
DRU8005	▌ Valid to field ▌ Submit button	Valid To cannot be set to a past date, to a date before Valid From	The Valid To must be equal to or later than the current business date, equal to or later than the Valid From, and equal to or earlier than the Valid To of the Authorised Account

Reference for error message	Field or Button	Error Text	Description
		or later than the related Authorised Account User	User referencing the BIC.
DRU8006	❙ Direction field ❙ Submit button	DN-BIC Routing already defined for this BIC, DN and Direction	At any given point in time, there cannot be more than one DN-BIC Routing for the same combination of BIC Mnemonic, Distinguished Name and Direction.
DRU8007	❙ BIC field ❙ Submit button	Outbound DN-BIC Routing already defined for this BIC	At any given point in time, there cannot be more than one Outbound DN-BIC Routing for the same BIC Mnemonic

4.3.2.14 Grant/Revoke Privileges – Search screen

No references for error messages.

4.3.2.15 Grant/Revoke Role – Details Screen

No references for error messages.

4.3.2.16 Grant/Revoke Role – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRGR001	❙ Roles field ❙ Grant button ❙ Revoke button	Requestor not allowed	When performing a "Grant/Revoke Role" request, the role to be granted/revoked must be in the data scope of the requestor. This means that at least one of the following conditions has to be fulfilled: o The requestor is the Service Operator; o The requestor is a Party Administrator of a CSD/NCB and the Role to be granted is in the same System Entity as the requestor's Party; o The requestor is a Party Administrator user and the Role is currently granted to their Party

DRGR002	▮ Parent BIC field ▮ BIC field ▮ Users field ▮ Grant button ▮ Revoke button	Requestor not allowed	When performing a "Grant/Revoke Role" request, a role can be granted to/revoked from a user only if the user belongs to the same Party as the requestor. The Service Operator can grant and revoke any Role to/from any User. As an exception to this rule, CSD/NCB Party Administrators can grant/revoke Roles directly to any User within their own System Entity provided the Role does not contain any privileges different from ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.
DRGR003	▮ Roles field ▮ Grant button	Invalid role	When performing a "Grant/Revoke Role" request to grant a role to a party or user, the request must refer to a role that is not already granted to the party or user.
DRGR004	▮ Current Granted Roles field ▮ Revoke button	Invalid role	When performing a "Grant/Revoke Role" request to revoke a role to a party or user, the request must refer to a party or user the role to be revoked is granted to.
DRGR005	▮ BIC field ▮ Parent BIC field ▮ Users field ▮ Grant button ▮ Revoke button	Invalid Grantee User/Party	When performing a "Grant/Revoke Role" request, the request must refer to an existing party or user.
DRGR007	▮ Roles field ▮ Grant button	Invalid role	When performing a "Grant/Revoke Role" request to grant a role to a party or user, the set of privileges connected to the role must not intersect with the set of privileges already granted to the party/user.
DRGR008	▮ Grant button	Requestor not allowed	When performing a "Grant/Revoke Role" request, the Role can be granted to/revoked from a Party as follows: o The Service Operator can grant and revoke any Role to/from any Party; o CSD/NCBs can grant and revoke the Role to/from any Party within their System Entity; o CSD Participants, External CSDs and Payment Banks cannot grant the Role to Parties.

4.3.2.17 Grant/Revoke System Privilege – Details screen

No references for error messages.

4.3.2.18 Grant/Revoke System Privilege – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRGP001	❙ Privilege Name field ❙ Submit button	Requestor not allowed	A Grant Privilege request grants a system privilege and/or an object privilege on a secured element to a user, a role or a party. The grantor user must be granted with the relevant privilege beforehand in order to administer it. If the grantor user is a Party Administrator, the privilege must be granted to the Party the user belongs to. Otherwise, the privilege must be granted directly to the user.
DRGP002	❙ Privilege Name field ❙ Submit button	Invalid system privilege	When performing a Grant Privilege request the privilege to be granted must refer to an existing privilege. A System Privilege cannot be assigned to a Party if this would always result in an empty data scope for that Party type.
DRGP005	❙ Submit button	Invalid grantee party	When performing a Grant Privilege request to grant a system privilege to a Party, the grantee party must be an active one in the default data scope of the grantor.
DRGP007	❙ Submit button	Invalid grantee user	When performing a Grant Privilege request, the User to be granted with a privilege must refer to an existing one belonging to the same party as the grantor, with the following exceptions: o The Service Operator can grant any privilege to any User. o CSD/NCB Party Administrators can grant Party Administrator privileges to any User within their own System Entity. The Party Administrator privileges are ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.
DRGP008	❙ Submit button	Invalid grantee role	When performing a Grant Privilege request, the Role to be granted with a privilege must refer to an existing one in the data scope of the grantor.
DRGP012	❙ Submit button	Invalid privilege type	When performing a Grant Privilege request, the specified privilege type must be consistent with its use. System privileges can only be granted at system level.
DRGP013	❙ Submit button	Privilege already granted	When performing a Grant Privilege request, in order to prevent the possibility to grant contradicting privileges to the same role,

			user or party:
			Each system privilege can be granted to a role, a user or a party only once.
			Each object privilege can be granted to a role, a user or a party on the same object only once.
DRGP014	▌ Submit button	Invalid valid from date	When performing a Grant Privilege request, the valid from date can't be less than the current business date.
DRGP016	▌ Submit button	User does not have Admin rights on the specified privilege	A Party Administrator can grant a Privilege to a Party only if the Privilege is already granted to their Party with Admin flag = TRUE. A Party Administrator can grant a Privilege to a User or Role only if the Privilege is already granted to their Party with Deny Flag = FALSE. Any other user can grant a privilege only to other users of its own Party or Roles and only if the Privilege is already granted to the grantor User with Admin Flag = TRUE.
DRGP017	▌ Deny Option field ▌ Submit button	Deny flag cannot be set to TRUE when granting privilege to a Party	When performing a Grant Privilege request, it is not possible to set the Deny flag to TRUE when the grantee is a Party.
DRGP018	▌ 4-Eyes Option field ▌ Submit button	Four-Eyes flag must be set to TRUE	When performing a Grant Privilege request, if a Privilege is granted to a Party with Four-Eyes flag = TRUE, the responsible Party Administrator can only grant it with Four-Eyes flag = TRUE. If a Privilege is granted to a User with Four-Eyes flag = TRUE and Admin flag = TRUE, the User can only grant it with Four-Eyes flag = TRUE.
DRGP019	▌ Submit button	A Role cannot contain privileges related to multiple Services	When performing a Grant Privilege request, Privileges linked to a certain Service cannot be granted to a Role if the Role already contains Privileges linked to a different Service.
DRGP020	▌ Submit button	TIPS privileges can only be granted to Roles.	When performing a Grant Privilege request, privileges for the TIPS service can only be granted to Roles.
DRRP001	▌ Submit button	Requestor not allowed	A Revoke Privilege request revokes a system privilege from a user, a role or a party and/or revokes an object privilege on a secured element. The requestor user must be a Party Administrator of their own Party or a User granted with the relevant privilege with Admin flag = TRUE.
DRRP004	▌ Submit button	Requestor not allowed	In case of request to revoke a privilege from a party, the requestor user must be a Party Administrator and the privilege to be revoked

Reference	Field or Button	Error Text	Description
			must have been granted by a user belonging to the same party of the requestor. The Service Operator can revoke any privilege from any Party.
DRRP005	▌ Submit button	Requestor not allowed	In case of request to revoke a privilege from a role, the requestor must belong to the Service Operator, or to a CSD, or to an NCB. The Service Operator can revoke any privilege from any Role. CSDs and NCBs can revoke privileges from Roles that have the same system entity as the requestor.
DRRP006	▌ Submit button	Requestor not allowed	In case of request to revoke a privilege from a user, the user must belong to the same party of the requestor, with the following exceptions: o The Service Operator can revoke any privilege from any user; o Party Administrator privileges can be revoked from any user in the requestor's system entity provided the requestor is a Party Administrator of a CSD or NCB Party. The Party Administrator privileges are ARM_AdministerParty, ARM_GrantPrivilege, ARM_GrantRole, ARQ_GrantedSysPrivilegesListQuery, ARQ_GrantObjectPrivilegesListQuery, ARQ_GrantedRolesListQuery.
DRRP007	▌ Submit button		When revoking a privilege from a party, the same privilege is also revoked from all users of the party.

4.3.2.19 Grant/Revoke Roles – Search/List Screen

No references for error messages.

4.3.2.20 Limits – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRD9001	▌ Delete button	Requestor not allowed	When performing a request to delete a Limit, the requestor must be authorised to delete the requested data according to the following: A System Operator user can delete all data A NCB user can delete only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can delete only Limits for non-primary T2S CMBs and TIPS CMBs

			linked to its own Cash Account
DRD9004	▌ Status field ▌ Restore button	Limit to be restored not found	The restore requests of a Limit must refer to an existing and deleted instance.
DRD9065	▌ Restore button	Unknown Credit Memorandum Balance Identifier	When performing a TIPS CMB Limit restore request, the Credit Memorandum Balance Identifier must refer to an existing and active Cash Account instance in CRDM with Account Type equal to TIPS CMB
DRD9205	▌ Restore button	Valid From invalid	When performing a Limit restore request, the Valid From date must be equal to or greater than the current date.

4.3.2.21 Limits – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRC9001	▌ Cash Account Number field ▌ Submit button	Requestor not allowed	When performing a request to create a Limit, the requestor must be authorised to create the requested data according to the following: A Service Operator user can create all data A NCB user can create only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can create only Limits for non-primary T2S CMBs and TIPS CMBs linked to its own Cash Account
DRC9052	▌ Cash Account Number field ▌ Submit button	Unknown Cash Account Identifier	When performing a Limit create request, the Cash Account specified must refer to an existing and active instance in CRDM.
DRC9058	▌ Limit Type field ▌ Submit button	Invalid Cash Account type	When performing a limit create request, if the limit type is TIPS CMB Limit then the Cash Account type must be TIPS CMB; if the limit type is autocollateralisation, external guarantee or unsecured credit the Cash Account type cannot be TIPS Account, TIPS Transit Account or TIPS CMB.
DRC9100	▌ Limit Type field ▌ Limit Amount field ▌ Submit button	Limit already defined	When performing a Limit create request, it must be verified that no Limit has already been defined for the BIC+BIC Branch Code (if present), Cash Account, Valid From and Limit Type provided in input.
DRC9205	▌ Valid From field ▌ Submit button	Valid From invalid	When performing a Limit create request, the Valid From date must be equal to or greater than the current date.

DRC9800	▌ Limit Amount field ▌ Submit button	Invalid number of decimals	When performing a Limit Create request, the number of decimals in the value provided for Limit Amount must be compliant with the number of decimals foreseen for the relevant currency.
DRU9001	▌ Submit button	Requestor not allowed	When performing a request to update a Limit, the requestor must be authorised to update the requested data according to the following: A Service Operator user can update all data A NCB user can update only Limits for CMBs (T2S CMBs and TIPS CMBs) belonging to its own System Entity A Payment Bank user can update only Limits for non-primary T2S CMBs and TIPS CMBs linked to its own Cash Account
DRU9003	▌ Submit button	Data to be updated not found	The update requests of a Limit must refer to an existing and active instance.
DRU9800	▌ Limit Amount field ▌ Submit button	Invalid number of decimals	When performing a Limit Update request, the number of decimals in the value provided for Limit Amount must be compliant with the number of decimals foreseen for the relevant currency.

4.3.2.22 Message Subscription Rule Set – Details Screen

Reference for error message	Field or Button	Error Text	Description
DRDE001	▌ Restore button ▌ Delete button	Requestor not allowed	A user can delete/restore only Message Subscription Rule Sets belonging to its own data scope.
DRDE002	▌ Interested Parent BIC field ▌ Interested Party BIC field ▌ Restore button	Unknown Party	When performing a Message Subscription Rule Set restore request, the Message Subscription Rule Set Party must reference Parties that exist and are active in CRDM.
DRDE003	▌ Status field ▌ Valid from field ▌ Valid to field ▌ Delete button	Data to be deleted/restored not found	When performing a Message Subscription Rule Set delete request it must refer to an existing and active instance of Message Subscription Rule Set with future Valid From or past Valid To.
DRDE006	▌ Valid from field ▌ Valid to field ▌ Restore button	Invalid validity dates	When performing a Message Subscription Rule Set restore request, either the Valid From must be greater than the current date, or the Valid To must be in the past. The Service Operator can skip this check in contingency situations.

DRDE040	▌ Delete button	The deletion/close is not allowed due to a priority constraint	A Message Subscription Rule Set cannot be deleted if there still are valid instances of the following entity linked to it: Message Subscription Rule.
DRDE044	▌ Status field ▌ Restore button	Data to be deleted/restored not found	When performing a Message Subscription Rule Set restore request it must refer to an existing and deleted instance of Message Subscription Rule Set.

4.3.2.23 Message Subscription Rule – New Screen

Reference for error message	Field or Button	Error Text	Description
DRCF001	▌ Submit button	Requestor not allowed	A Message Subscription Rule can be created only by users belonging to Service Operator, CSD, NCB, CSD Participant, Payment Bank and External CSD with the correct privilege. CSD and NCB users can only create Message Subscription Rules within their own system entity. CSD Participant, Payment Bank and External CSD users can only create Message Subscription Rules for their own party.
DRCF002	▌ Submit button	Unknown Message Subscription Rule Set Identifier	When performing a Message Subscription Rule creation request, the Message Subscription Rule Set Identifier specified must exist in CRDM and must belong to the data scope of the requestor.
DRCF003	▌ Rule Set field ▌ Message Subscription Sequence Number field	Rule Sequence already inserted	When performing a Message Subscription Rule creation request, the Rule Sequence specified must not be already existing for the same Message Subscription Rule Set Identifier
DRCF006	▌ Valid from field ▌ Submit button	Invalid 'Valid From'	When performing a Message Subscription Rule creation request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.
DRCF007	▌ Valid to field ▌ Submit button	Invalid "Valid To"	When performing a Message Subscription Rule creation request, the Valid To, if specified, must be equal to or greater than the Valid From, and equal to or less than the related Message Subscription Rule Set Valid To.
DRCF300	▌ Group field ▌ Submit button	Number of maximum active Message Subscription Rule exceeded	When performing a Message Subscription Rule create request, the overall number of group of parameters for the relevant CSD must be compliant with the configuration limit defined in CRDM.

DRUF001	▌ Submit button	Requestor not allowed	A user can only update Message Subscription Rules within its own data scope.
DRUF003	▌ Submit button	Data to be updated not found	When performing a Message Subscription Rule update request it must refer to an existing and active instance of Message Subscription Rule.
DRUF004	▌ Rule Set field ▌ Submit button	Only 'Valid To' can be updated	When performing a Message Subscription Rule update request, if the existing Valid From is equal to or less than the current business date, it is only possible to modify the Valid To field.
DRUF005	▌ Message Subscription Sequence Number field ▌ Submit button	Rule Sequence already inserted	When performing a Message Subscription Rule update request, the Rule Sequence, when specified, must not be already used for the same Message Subscription Rule Set Identifier
DRUF006	▌ Valid from field ▌ Submit button	Invalid 'Valid From'	When performing a Message Subscription Rule update request, the specified Valid From must be equal to or greater than the related Message Subscription Rule Set Valid From and greater to the current business date. The Service Operator can skip this check in contingency situations.
DRUF007	▌ Valid to field ▌ Submit button	Invalid 'Valid To'	When performing a Message Subscription Rule update request, the specified Valid To must be equal to or less than the related Message Subscription Rule Set Valid To and equal to or greater than the Valid From specified in input, if present.
DRUF050	▌ Submit button	Invalid TIPS Account	When performing a Message Subscription Rule update request involving a TIPS Account as Rule Parameter Value, the account must belong to the data scope of the requestor.
DRUF300	▌ Group field ▌ Submit button	Number of maximum active Message Subscription Rules exceeded	When performing a Message Subscription Rule update request, in case of creation of Message Subscription Rule Parameter, the overall number of group of parameters for the relevant CSD must be compliant with the configuration limit defined in CRDM.

4.3.2.24 Message Subscription Rule Set – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRCE001	▌ Parent BIC field ▌ Party BIC field	Requestor not allowed	A Message Subscription Rule Sets can be created only by users belonging to Service Operator, CSD, NCB, CSD Participant,

			Payment Bank and External CSD with the correct privilege. CSD and NCB users can only create Message Subscription Rule Sets within their own system entity. CSD Participant, Payment Bank and External CSD users can only create Message Subscription Rule Sets for their own party.
DRCE002	▌ Parent BIC field ▌ Party BIC field ▌ Submit button	Unknown Party	When performing a Message Subscription Rule Set Party creation request, the Parties specified must exist and be active in CRDM.
DRCE005	▌ Parent BIC field ▌ Party BIC field ▌ Submit button	Invalid Party	When performing a Message Subscription Rule Set Party creation request, the Party Id specified must belong to a Party in the default data scope of the requestor.
DRCE006	▌ Creator Parent BIC field ▌ Creator Party BIC field	Invalid Party	When performing a Message Subscription Rule Set Party creation request, the Creator Party specified must be the same Party as the Requestor or the CSD/NCB specified as System Entity by the Service Operator in case of act on behalf.
DRCE009	▌ Valid from field ▌ Submit button	"Valid From" invalid	When performing a Message Subscription Rule Set creation request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.
DRCE010	▌ Valid from field ▌ Valid to field ▌ Submit button	"Valid To" invalid	When performing a Message Subscription Rule Set creation request, the Valid To must be greater than or equal to the Valid From.
DRCE100	▌ Submit button	Invalid System Entity	When performing a Message Subscription Rule Set create request, the specified System Entity must refer to an existing and active instance in CRDM.
DRCE200	▌ Name field ▌ Submit button	Name already assigned	When performing a Message Subscription Rule Set create request, the specified Name must not be already assigned in CRDM under the same Party.
DRUE001	▌ Submit button	Requestor not allowed	A Message Subscription Rule Sets can be updated only by users belonging to Service Operator, CSD, NCB, CSD Participant, Payment Bank and External CSD with the correct privilege. CSD and NCB users can only update Message Subscription Rule Sets within their own system entity. CSD Participant, Payment Bank and External CSD users can only update Message Subscription Rule Sets for their own party.
DRUE003	▌ Submit button	Data to be updated not found	When performing a Message Subscription Rule Set update request it must refer to an existing and active instance of Message Subscription Rule Set. If the Valid To is in

			the past, only the Valid From can be updated (The Service Operator can skip this check in contingency situations).
DRUE004	❚ Parent BIC field ❚ Party BIC field ❚ Submit button	Party Id already specified	When performing a Message Subscription Rule Set Party create request, the same Party Id cannot be specified twice.
DRUE005	❚ Parent BIC field ❚ Party BIC field ❚ Submit button	Invalid Party Id	When performing a Message Subscription Rule Set Party create request, the Party Id specified must belong to a Party in the default data scope of the requestor.
DRUE006	❚ Submit button	Invalid Creator Party	When performing a Message Subscription Rule Set Party create request, the Creator Party specified must be the same party as the requestor or the CSD/NCB specified as System Entity by the Service Operator in case of act on behalf.
DRUE007	❚ Parent BIC field ❚ Party BIC field ❚ Submit button	Invalid Party Id	When performing a Message Subscription Rule Set Party delete request, the Party Id specified must refer to an existing Message Subscription Rule Set Party instance.
DRUE008	❚ Submit button	Only "Valid To" can be updated	When performing a Message Subscription Rule Set update request if the Valid From is in the past, only a future Valid To can be updated (The Service Operator can skip this check in contingency situations).
DRUE010	❚ Parent BIC field ❚ Party BIC field ❚ Submit button	Unknown Party	When performing a Message Subscription Rule Set update request, the Party Id and Creator Party specified must exist and be active in CRDM.
DRUE200	❚ Name field ❚ Submit button	Name already assigned	When performing a Message Subscription Rule Set update request, the specified Name must not be already assigned in CRDM under the same Party.
DRUE205	❚ Valid from field ❚ Submit button	"Valid From" invalid	When performing a Message Subscription Rule Set update request, the Valid From must be greater than the current date. The Service Operator can skip this check in contingency situations.
DRUE206	❚ Valid from field ❚ Valid to field ❚ Submit button	"Valid To" invalid	When performing a Message Subscription Rule Set update request, the Valid To must be greater than or equal to the current date and greater than or equal to the Valid From.
DRUE207	❚ Valid from field ❚ Valid to field ❚ Submit button	Validity dates not compliant with Message Subscription Rules	When performing a Message Subscription Rule Set update request, the Valid To must be greater than or equal to all the Valid To of the related Message Subscription Rules. The Valid From must be equal to or less than the Valid From of the related Message Subscription Rules.

4.3.2.25 Message Subscription Rule Sets – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRDE001	▌ Restore button ▌ Delete button	Requestor not allowed	A user can delete/restore only Message Subscription Rule Sets belonging to its own data scope.
DRDE002	▌ Interested Parent BIC field ▌ Interested Party BIC field ▌ Restore button	Unknown Party	When performing a Message Subscription Rule Set restore request, the Message Subscription Rule Set Party must reference Parties that exist and are active in CRDM.
DRDE003	▌ Status field ▌ Valid from field ▌ Valid to field ▌ Delete button	Data to be deleted/restored not found	When performing a Message Subscription Rule Set delete request it must refer to an existing and active instance of Message Subscription Rule Set with future Valid From or past Valid To.
DRDE006	▌ Valid from field ▌ Valid to field ▌ Restore button	Invalid validity dates	When performing a Message Subscription Rule Set restore request, either the Valid From must be greater than the current date, or the Valid To must be in the past. The Service Operator can skip this check in contingency situations.
DRDE040	▌ Delete button	The deletion/close is not allowed due to a priority constraint	A Message Subscription Rule Set cannot be deleted if there still are valid instances of the following entity linked to it: Message Subscription Rule.
DRDE044	▌ Status field ▌ Restore button	Data to be deleted/restored not found	When performing a Message Subscription Rule Set restore request it must refer to an existing and deleted instance of Message Subscription Rule Set.
DRDE200	▌ Name field ▌ Restore button	Name already assigned	When performing a Message Subscription Rule Set restore request, the specified Name must not be already assigned in CRDM under the same Party.

4.3.2.26 Parties – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DPD1001	▌ Restore button ▌ Delete button	Requestor not allowed	Party can only be deleted or restored by Service operator or CB. A user belonging to a CB can only delete or restore parties that fall under their responsibility according to the hierarchical party model. Exceptions to the above rule are

DPD1003	▌ Status field ▌ Opening Date – From field ▌ Opening Date – To field ▌ Closing Date – From field ▌ Closing Date – To field ▌ Delete button	Unknown party	represented by any user that is granted the appropriate privilege(s) on the specific party to be maintained. When performing a party delete request, it must refer to an existing, active and closed party or with a future opening date.
DPD1004	▌ Status field ▌ Opening Date – From field ▌ Opening Date – To field ▌ Closing Date – From field ▌ Closing Date – To field ▌ Restore button	Party is not deleted	When performing a party restore request, it must refer to an existing and deleted party already closed or with an Opening date equal to or greater than the current business date.
DPD1005	▌ Type field ▌ Restore button	Only one CSD/ NCB per System Entity allowed	When performing a party restore request, the party type cannot be 'CSD' or 'NCB' if there is already a CSD or CB defined within the system entity.
DPD1013	▌ Parent BIC field ▌ BIC field ▌ Restore button	Party Mnemonic already used	When performing a party restore request, the party mnemonic specified in the party code section must not be already assigned to an active party having the same party type and belonging to the same system entity.
DPD1021	▌ Restore button	Invalid country code	When performing a Party Restore request, the 'Country Code' specified in the Party Address section must refer to an existing Country Code in CRDM.
DPD1024	▌ Restore button	Invalid restriction type	When performing a Party Restore request, the 'Restriction Type' specified in the Party Restriction section must refer to an existing type in CRDM available for the relevant System Entity.
DPD1030	▌ Delete button	The deletion is not allowed due to a deletion priority constraint	In case of request to delete a Party, all the linked instances in a higher position within the deletion hierarchy (i.e. Securities Account, Cash Account, External RTGS Account, Security CSD Link, CSD Account Link and Party) must be deleted.

DPD1040	▐ Restore button	Technical Address not found in BIC directory	When performing a Party Restore request, the 'Technical Address' specified in the Party Technical Address section must exist in the BIC Directory, when its type is BIC.
DPD1180	▐ Parent BIC field ▐ BIC field ▐ Restore button	Party Mnemonic not found in BIC directory	When performing a Party Restore request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.
DPD1207	▐ Restore button	'Valid To' invalid	When performing a party restore request, the party restriction valid to, when specified, must be equal to or less than the valid to of the relevant restriction type entity.
DPD1208	▐ Restore button	'Valid From' invalid	When performing a Party restore request, the Party Restriction 'Valid From", when specified, must be equal to or greater than the Valid From of the relevant Restriction Type entity and equal to or less than the Valid To of the relevant Restriction Type entity.

4.3.2.27 Party – Details Screen

Reference for error message	Field or Button	Error Text	Description
DPD1001	▐ Delete button	Requestor not allowed	Party can only be deleted or restored by Service operator or CB. A user belonging to a CB can only delete or restore parties that fall under their responsibility according to the hierarchical party model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the specific party to be maintained.
DPD1003	▐ Status field ▐ Opening Date field ▐ Delete button	Unknown party	When performing a party delete request, it must refer to an existing, active and closed party or with a future opening date.
DPD1004	▐ Status field ▐ Opening Date field	Party is not deleted	When performing a party restore request, it must refer to an existing and deleted party already closed or with an Opening date equal to or greater than the current business date.
DPD1005	▐ Type field	Only one NCB per System Entity allowed	When performing a party restore request, the party type cannot be 'NCB' if there is already a CB defined within the system entity.
DPD1013	▐ Parent BIC field ▐ BIC field	Party Mnemonic already used	When performing a party restore request, the party mnemonic specified in the party code section must not be already assigned to an active party having the same party

Reference for error	Field or Button	Error Text	Description
			type and belonging to the same system entity.
DPD1021	▌Country Code field	Invalid country code	When performing a Party Restore request, the 'Country Code' specified in the Party Address section must refer to an existing Country Code in CRDM.
DPD1024	▌Type field	Invalid restriction type	When performing a Party Restore request, the 'Restriction Type' specified in the Party Restriction section must refer to an existing type in CRDM available for the relevant System Entity.
DPD1030	▌Delete button	The deletion is not allowed due to a deletion priority constraint	In case of request to delete a Party, all the linked instances in a higher position within the deletion hierarchy (i.e. Securities Account, Cash Account, External RTGS Account, Security CSD Link, CSD Account Link and Party) must be deleted.
DPD1040	▌Technical address field ▌Restore button	Technical Address not found in BIC directory	When performing a Party Restore request, the 'Technical Address' specified in the Party Technical Address section must exist in the BIC Directory, when its type is BIC.
DPD1180	▌Parent BIC field ▌BIC field ▌Restore button	Party Mnemonic not found in BIC directory	When performing a Party Restore request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.
DPD1207	▌Restore button	'Valid To' invalid	When performing a party restore request, the party restriction valid to, when specified, must be equal to or less than the valid to of the relevant restriction type entity.
DPD1208	▌Restore button	'Valid From' invalid	When performing a Party restore request, the Party Restriction 'Valid From", when specified, must be equal to or greater than the Valid From of the relevant Restriction Type entity and equal to or less than the Valid To of the relevant Restriction Type entity.
DPU1001	▌Edit button	Requestor not allowed	Party can only be updated by Service Operator or NCB. A user belonging to an NCB can only update parties that fall under their responsibility according to the hierarchical party model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the specific party to be maintained.

4.3.2.28 Party – New/Edit Screen

Reference for error	Field or Button	Error Text	Description

message			
DPC1001	▌ Parent BIC field ▌ Submit button	Requestor not allowed	A Party can be created only by Service operator, CSD or CB. A user belonging to a CSD or CB can only create parties that fall under their responsibility according to the hierarchical party model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the party responsible for the party to be created.
DPC1002	▌ Party Type field ▌ Submit button	Invalid System Entity Identifier	When performing a party create request, the system entity specified in input must refer to an existing instance in CRDM, and its type must be consistent with the party type specified in input.
DPC1005	▌ Party Type field ▌ Submit button	Only one CSD/ NCB per System Entity allowed	When performing a party create request, the party type cannot be CSD or CB if there is already a CSD or CB defined within the system entity.
DPC1013	▌ BIC field ▌ Submit button	Party Mnemonic already used	When performing a Party Create request, the 'Party Mnemonic' specified in the Party Code section must not be already assigned to another active Party belonging to the same System Entity and having the same Parent BIC.
DPC1021	▌ Country Code field ▌ Submit button	Invalid country code	When performing a party create request, the country code specified in the party address section must refer to an existing country code in CRDM.
DPC1024	▌ Type field ▌ Submit button	Invalid restriction type	When performing a Party Create request, In case of request for creation of Party Restriction, the created restriction type must refer to an existing type in [Restriction Type] entity with Object Restriction Type 'Party'.
DPC1025	▌ Valid from field ▌ Valid to field ▌ Type field ▌ Submit button	Party Restriction overlaps with existing instance	When performing a party create request, in case of a request for the creation of a party restriction, the created restriction type must not overlap with any other party restriction in input having the same restriction type.
DPC1180	▌ BIC field ▌ Submit button	Party Mnemonic not found in BIC directory	When performing a party create request, the party mnemonic specified in the party code section (when its type is BIC) must exist in the BIC directory.
DPC1205	▌ Opening Date field ▌ Submit button	'Opening Date' invalid	When performing a party create request, the party opening date specified in the request must be equal to or greater than the current date.
DPC1206	▌ Closing Date field ▌ Submit button	'Closing Date' invalid	When performing a party create request, the party closing date, if specified, must be equal to or greater than the current date

			and greater than the opening date.
DPC1207	▌ Valid To field ▌ Submit button	'Valid To' invalid	When performing a party create request, the party restriction 'valid to' , when specified, must be equal to or greater than the current timestamp, equal to or greater than the party restriction valid from and equal to or less than the valid to of the relevant restriction type entity.
DPC1208	▌ Valid From field ▌ Submit button	'Valid From' invalid	When performing a Party Create request, the Party Restriction 'Valid From", when specified, must be equal to or greater than the current timestamp and equal to or greater than the Valid From of the relevant Restriction Type entity and equal to or less than the Valid To of the relevant Restriction Type entity.
DPC1300	▌ Valid From field ▌ Submit button	'Valid From' invalid	When performing a party create request, the valid from date specified in the party code section, must be equal to the current business date.
DPC1301	▌ Valid From field ▌ Submit button	'Valid From' invalid	When performing a party create request, the valid from date specified in the party address section must be equal to the current business date.
DPC1302	▌ Valid From field ▌ Submit button	'Valid From' invalid	When performing a Party Create request, the 'Valid From' specified in the Party Name section, must be equal to the current business date.
DPU1001	▌ Parent BIC field ▌ BIC field ▌ Submit button	Requestor not allowed	Party can only be updated by the Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only update parties that fall under their responsibility according to the Hierarchical Party Model. Exceptions to the above rule are represented by any user that is granted the appropriate privilege(s) on the specific Party to be maintained.
DPU1003	▌ Closing Date field ▌ Submit button	Unknown party	When performing a Party Update request, it must refer to an existing and active Party whose Closing Date is equal to or greater than the current business date.
DPU1005	▌ BIC field ▌ Party Long Name ▌ Party Short Name ▌ Street field ▌ House Number field ▌ Postal Code field ▌ City field ▌ State or Province field ▌ Country Code field	Unknown party	When performing a Party Update request, the update request of a "minor" entity (such as Party Name, Party code, Party Address,Market-Specific Attribute, Party Restriction, AutoCollateralisation Rule) must refer to an existing and active instance with a non-past Valid To, where applicable.

	▌ Address Value field ▌ Type field ▌ Valid to field ▌ Submit button		
DPU1006	▌ Address Value field ▌ Submit button	Missing mandatory section/field	Each party must have at least one party technical address.
DPU1007	▌ Address Value field ▌ Submit button	Party Technical address already defined for Party	When performing a Party Update request, in case of request for creation of Party Technical Address, the PTA specified cannot be identical to a PTA already linked to the relevant Party.
DPU1009	▌ Valid From field ▌ Submit button	'Opening Date' or 'Close Date' invalid	When performing a Party Update request, the create request of a historical (i.e. which has the validity date) "minor" entity (such as Party Name Party code, Party Address) cannot have a past validity date.
DPU1010	▌ Valid From field ▌ Submit button	Instance with past validity date cannot be deleted	When performing a Party Update request, the delete request of a historical (i.e. which has the validity date) "minor" entity (such as Party Name, Party Address) cannot refer to an entity having a past validity date. This does not apply to the Party Code, for which only the currently active entity cannot be deleted.
DPU1013	▌ Parent BIC field ▌ BIC field ▌ Submit button	Party Mnemonic already used	When performing a Party Update request, the 'Party Mnemonic' specified in the Party Code section must not be already assigned, as an active instance, to another active Party belonging to the same System Entity and having the same Parent BIC.
DPU1021	▌ Country Code field ▌ Submit button	Invalid country code	When performing a Party Update request, the 'Country Code' specified in the Party Address section must refer to an existing Country Code in CRDM.
DPU1024	▌ Type field ▌ Submit button	Invalid restriction type	When performing a Party Update request, in case of request for creation of Party Restriction, the created restriction type must refer to an existing type in [Restriction Type] entity with Object Restriction Type 'Party'.
DPU1025	▌ Type field ▌ Valid From field ▌ Submit button	Invalid restriction type	When performing a Party Update request, in case of request for deletion of Party Restriction, it must refer to a closed instance or its Valid From must be greater than the current timestamp.
DPU1030	▌ Submit button	The deletion/close is not allowed due to a deletion	When performing a Party Update request, in case of request to close a Party, all the linked instances in a higher position within the deletion hierarchy (i.e. Securities

		priority constraint	Account, Cash Account, External RTGS Account, Security CSD Link and CSD Account link, Party) must be closed or deleted.
DPU1180	▌ BIC field ▌ Submit button	Party Mnemonic not found in BIC directory	When performing a Party Update request, the 'Party Mnemonic' specified in the Party Code section (when its type is BIC) must exist in the BIC Directory.
DPU1205	▌ Closing Date field ▌ Submit button	"Opening Date" or "Close Date" invalid	When performing a Party Update request, in case of Closing of [Party], the specified 'Closing Date' must be equal to or greater than the current business date.
DPU1206	▌ Opening Date field ▌ Submit button	"Opening Date" or "Close Date" invalid	When performing a Party Update request, it is only possible to update the 'Opening Date' if it is greater than the current business date. The new specified value must be equal to or greater than the current business date and it must not be greater than the opening date of the DCA for which the party is the Account holder.
DPU1207	▌ Valid From field ▌ Valid To field ▌ Submit button	"Valid To" invalid	When performing a Party Update request, the specified Party Restriction 'Valid To' must be equal to or greater than the current timestamp, greater than the relevant Valid From, equal to or greater than the Valid From of the relevant Restriction Type and equal to or less than the Valid To of the relevant Restriction Type.
DPU1208	▌ Opening Date field ▌ Closing Date field ▌ Valid From field ▌ Submit button	'Valid From' invalid	When performing a Party update request, the Valid From specified in a Party Restriction create request must be equal to or greater than the current timestamp, equal to or greater than the Valid From of the relevant Restriction Type and equal to or less than the Valid To of the relevant Restriction Type.
DPU1300	▌ Type field ▌ Valid from field ▌ Valid to field ▌ Submit button	Party Restriction overlaps with existing instance	When performing a Party Update request, in case of request for creation/update of Party Restriction, the new or updated restriction must not overlap with any other Party Restriction having the same Restriction Type on the same Party.
DPU1500	▌ Valid From field ▌ Submit button	Minor entity is not the one currently in use or the future one	When performing a Party Update request, the update request of a historical "minor" entity (such as Party Name, Party Address) must refer to an instance currently in use or having a future validity.
DPU1501	▌ Valid From field ▌ Submit button	Party Code to be updated must have a future validity	When performing a Party Update request, the update request of Party Code must refer to an instance having a future validity.

4.3.2.29 Party Service Link – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DPD4001	▌ Delete button	Requestor not allowed	Party-Service Links can be deleted or restored only by the Service Operator, CSDs or NCBs. CSDs and NCBs can delete or restore Links within their own System Entities, but not for their own Party.
DPD4002	▌ Delete button	Unknown, deleted or open Party-Service Link	Deletion requests must refer to existing, active and closed Party-Service Links.
DPD4003	▌ Party BIC field ▌ Restore button	Unknown, active or open Party-Service Link	Restore requests must refer to existing, deleted and non-open Party-Service Links.
DPD4004	▌ Restore button	Unknown, deleted or closed Party	In a restore request, the linked Party must be an existing, active and non-closed Party.
DPD4005	▌ Service field ▌ Restore button	Unknown or deleted Service	In a restore request, the linked Service must be an existing and active Service.
DPD4006	▌ Service field ▌ Restore button	Validity period overlaps with duplicate Party-Service Link entry	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.
DPD4007	▌ Party BIC field ▌ Restore button	TIPS Party-Service Link already defined for this Party BIC	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.

4.3.2.30 Party Service Link – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DPC4001	▌ Submit button	Requestor not allowed	Party-Service Links can be created only by the Service Operator, CSDs or NCBs. CSDs and NCBs can create Links for Parties within their own System Entities, but not for their own Party.

DPC4002	▌ Submit button	Unknown, deleted or closed Party	The Party Identifier must refer to an existing, active and non-closed Party.
DPC4003	▌ Service field ▌ Submit button	Unknown or deleted Service	The Service Identifier must refer to an existing and active Service.
DPC4004	▌ Valid from field ▌ Submit button	Valid From cannot be set to a past date	The Valid From must be equal to or greater than the current business date.
DPC4005	▌ Valid to field ▌ Submit button	Valid To cannot be set to a past date or to a date before Valid From	The Valid To must be equal to or greater than the current business date, and equal to or greater than the Valid From.
DPC4006	▌ Party type for service field ▌ Submit button	The Service Party Type must be consistent with the linked Party Type.	The Service Party Type must be consistent with the linked Party Type.
DPC4007	▌ Party type for service field ▌ Submit button	Service Party Type is not consistent with linked Service	The Service Party Type must be consistent with the linked Service.
DPC4008	▌ Opening Date field ▌ Closing Date field ▌ Submit button	Validity period overlaps with duplicate Party-Service Link entry	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.
DPC4009	▌ Party BIC field ▌ Submit button	TIPS Party-Service Link already defined for this Party BIC	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.
DPU4001	▌ Submit button	Requestor not allowed	Party-Service Links can be updated only by the Service Operator, CSDs or NCBs. CSDs and NCBs can update Links within their own System Entities, but not for their own Party.
DPU4002	▌ Submit button	Unknown, deleted or closed Party-Service Link	Update requests must refer to existing, active and open Party-Service Links.
DPU4003	▌ Opening Date field ▌ Submit button	Valid From cannot be modified	The Valid From can only be modified if the current Valid From is later than the current business date.
DPU4004	▌ Opening Date field ▌ Submit button	Valid From cannot be set to a past date	The Valid From must be equal to or greater than the current business date.

DPU4005	❚ Closing Date field ❚ Submit button	Valid To cannot be set to a past date or to a date before Valid From	The Valid To must be equal to or greater than the current business date and equal to or greater than the Valid From.
DPU4006	❚ Submit button	Validity period overlaps with duplicate Party-Service Link entry	At any given point in time, there cannot be more than one Party-Service Link between a given Party-Service couple.
DPU4007	❚ Closing Date field ❚ Submit button	Party-Service Link cannot be closed due to a priority constraint	The Valid To must be equal to or greater than the Closing Date of every Cash Account owned by the linked Party for the relevant linked Service.
DPU4008	❚ Party BIC field ❚ Submit button	TIPS Party-Service Link already defined for this Party BIC	At any given point in time, there cannot be more than one Party-Service Link for TIPS for multiple Payment Bank Parties with the same Party BIC.

4.3.2.31 Report Configuration – Details Screen

Reference for error message	Field or Button	Error Text	Description
DRDV001	❚ Restore button ❚ Delete button	Requestor not allowed	Report Configuration can be deleted/restored only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only delete/restore Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only deleted/restored Report Configuration for his own party
DRDV004	❚ Parent BIC field ❚ Party BIC ❚ Restore button	Unknown Party Identifier	When performing a Report Configuration restore request, the Owner Party Technical Identifier to be restored must refer to an existing and active Party with the same System Entity of the Report Configuration.
DRDV005	❚ Restore button ❚ Parent BIC field ❚ Party BIC field	Unknown Party Identifier	When performing a Report Configuration restore request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party with the same System Entity of the Report Configuration.
DRDV008	❚ Configuration Name field	Configuration Name already	When performing a Report Configuration restore request, the Configuration Name

		assigned	specified must be unique within the same System Entity
	❙ Restore button		
DRDV020	❙ Status field ❙ Delete button	Invalid Report Configuration to be delete	The request to delete a Report Configuration must refer to an existing and active Report Configuration in CRDM.
DRDV030	❙ Status field ❙ Restore button	Invalid Report Configuration to be restored	The request to restore a Report Configuration must refer to an existing and deleted Report Configuration in CRDM.
DRDV050	❙ Restore button ❙ Valid from field ❙ Valid to field	Invalid Report Configuration to be restored	When performing a Report Configuration restore request, all the Report Configuration Party Link must be closed or must have a future Valid From
DRDV060	❙ Delete button ❙ Valid from field ❙ Valid to field	Invalid Report Configuration to be deleted	When performing a Report Configuration delete request, all the Report Configuration Party Link must be closed or must have a future Valid From.
DRDV070		Invalid currency	When performing a Report Configuration restore request, the specified Currency must refer to an existing Currency.
DRDV110			When performing a Report Configuration restore request, if it refers to a TIPS Report and the Delta flag is set to TRUE, the Report must be defined as available in Delta mode in the related Attribute Domain.

4.3.2.32 Report Configuration – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRCV001	❙ Submit button	Requestor not allowed	Report Configuration can be created only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only create Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only create Report Configuration for his own party.
DRCV004	❙ Submit button	Unknown Party Identifier	When performing a Report Configuration creation request, the Owner Party Technical Identifier specified must refer to an existing and active Party in CRDM.
DRCV005	❙ Parent BIC field ❙ Party BIC field ❙ Submit button	Unknown Party Identifier	When performing a Report Configuration creation request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party belonging to

			the System Entity Code specified.
DRCV008	❙ Configuration Name field ❙ Submit button	Configuration Name already assigned	The Configuration Name specified in the Report Configuration creation request must be unique with the same System Entity.
DRCV020	❙ Submit button	"System Entity Code" invalid	When performing a Report Configuration create request, the System Entity Code must be equal to the System Entity Code of the requestor or, in case the requestor is a Service Operator, to an existing System Entity with System Entity type equal to CSD or NCB.
DRCV030	❙ System Entity Wide Reporting Flag field ❙ Submit button	"System Entity Wide Report" invalid	When performing a Report Configuration creation request, the System Entity Wide Report must be set to FALSE in case the Owner Party Technical Identifier specified refers to a Party Type equal to CSD Participant or Payment Bank.
DRCV040	❙ Valid from field ❙ Submit button	"Valid From" invalid	When performing a Report Configuration creation request, the Valid From specified in the Report Configuration Party Link section must be greater than the current business date.
DRCV050	❙ Valid to field ❙ Submit button	"Valid To" invalid	When performing a Report Configuration creation request, the Valid To specified in the Report Configuration Party Link section must be greater than the Valid From.
DRCV070	❙ Submit button	Invalid currency	When performing a Report Configuration create request, the specified Currency must refer to an existing Currency.
DRCV080	❙ Submit button	Currency not relevant	When performing a Report Configuration create request, the Currency field can only be used in combination with a currency-dependent event and one of the currency-related report types listed in the T2S documentation.
DRCV110	❙ Submit button	Invalid Party for TIPS reports.	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name, the Opting Party must be equal to the Owner Party. Furthermore the Party Type must be Payment Bank.
DRCV120	❙ Report Name field ❙ Submit button	Invalid fields for TIPS reports.	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name, the System Entity Wide flag must be set to FALSE and the Push flag to TRUE. Furthermore the Execution Time, Event Type and Currency fields must not be used.
DRCV130	❙ Frequency field ❙ Submit button	Frequency must be specified for TIPS reports in	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name and the Delta flag

		Delta mode.	is set to TRUE, the report Frequency must be specified. If a non-TIPS Report is selected or if the Delta flag is set to FALSE, the report Frequency cannot be specified.
DRCV140	▮ Submit button	Report not available in Delta mode	When performing a Report Configuration creation request, if a TIPS Report is selected as Report Name and the Delta flag is set to TRUE, the Report must be defined as available in Delta mode in the related Attribute Domain.
DRUV001	▮ Submit button	Requestor not allowed	Report Configuration can be updated only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only update Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only update Report Configuration for his own party
DRUV003	▮ Submit button	Data to be updated not found	When performing a Report Configuration update request, it must refer to an existing and active instance of Report Configuration.
DRUV005	▮ Parent BIC field ▮ Party BIC field ▮ Submit button	Unknown Opting Party Identifier	When performing a Report Configuration update request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party with the same System Entity of the Report Configuration.
DRUV010	▮ Submit button	Unknown Report Configuration Party Link	When performing a Report Configuration update request, in case of request to update a Report Configuration Party Link, it must refer to an existing and active minor entity.
DRUV020	▮ Valid from field ▮ Valid to field ▮ Submit button	Unknown Report Configuration Party Link	When performing a Report Configuration update request, in case of request to delete a Report Configuration Party Link, it must refer to an existing and active minor entity with a future Valid From or already Closed.
DRUV030	▮ Valid from field ▮ Submit button	Invalid Valid From	When performing a Report Configuration update request, in case of request to create a Report Configuration Party Link, the Valid From must be greater than the current date.
DRUV040	▮ Valid from field ▮ Valid to field ▮ Submit button	Invalid Valid To	When performing a Report Configuration update request, in case of request to create/update a Report Configuration Party Link, the Valid To must be greater than the current date and greater than the relevant Valid From.
DRUV070	▮ Submit button	Invalid currency	When performing a Report Configuration update request, the specified Currency must refer to an existing Currency.

DRUV110	▌ Submit button	Invalid Party for TIPS reports.	When performing a Report Configuration update request, if it refers to a TIPS Report, the Opting Party must be equal to the Owner Party. Furthermore the Party Type must be Payment Bank.
DRUV120	▌ Push mode flag ▌ Submit button	Invalid fields for TIPS reports.	When performing a Report Configuration update request, if it refers to a TIPS Report, the Push Mode flag must be set to TRUE. Furthermore the Execution Time, Event Type and Currency fields must not be used.
DRUV130	▌ Frequency field ▌ Submit button	Frequency can only be specified for TIPS reports in Delta mode.	When performing a Report Configuration update request, the Frequency field can only be specified for TIPS Reports that are available in Delta mode.

4.3.2.33 Report Configurations – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRDV001	▌ Restore button ▌ Delete button	Requestor not allowed	Report Configuration can be deleted/restored only by Service Operator, CSD, NCB, CSD Participant or Payment Bank. A user belonging to a CSD or NCB can only delete/restore Report Configuration for parties that fall under their responsibility according to the Hierarchical Party Model. A user belonging to a CSD Participant or Payment Bank can only deleted/restored Report Configuration for his own party
DRDV004	▌ Parent BIC field ▌ Party BIC field ▌ Restore button	Unknown Party Identifier	When performing a Report Configuration restore request, the Owner Party Technical Identifier to be restored must refer to an existing and active Party with the same System Entity of the Report Configuration.
DRDV005	▌ Parent BIC field ▌ Party BIC field ▌ Restore button	Unknown Party Identifier	When performing a Report Configuration restore request, the Opting Party Technical Identifier specified in the Report Configuration Party Link section, must refer to an existing and active Party with the same System Entity of the Report Configuration.
DRDV007	▌ Report Name field ▌ Restore button	Unknown Report Name	When performing a Report Configuration restore request, the Report Name specified must refer to an existing and active Attribute Domain Name of an Attribute Domain instance.
DRDV008	▌ Configuration Name field	Configuration Name already	When performing a Report Configuration restore request, the Configuration Name

	▌ Restore button	assigned	specified must be unique within the same System Entity
DRDV020	▌ Status field ▌ Delete button	Invalid Report Configuration to be deleted	The request to delete a Report Configuration must refer to an existing and active Report Configuration in CRDM.
DRDV030	▌ Status field ▌ Restore button	Invalid Report Configuration to be restored	The request to restore a Report Configuration must refer to an existing and deleted Report Configuration in CRDM.
DRDV050	▌ Valid From field ▌ Restore button	Invalid Report Configuration to be restored	When performing a Report Configuration restore request, all the Report Configuration Party Link must be closed or must have a future Valid From.
DRDV060	▌ Valid From field ▌ Delete button	Invalid Report Configuration to be deleted	When performing a Report Configuration delete request, all the Report Configuration Party Link must be closed or must have a future Valid From.
DRDV110	▌ Restore button		When performing a Report Configuration restore request, if it refers to a TIPS Report and the Delta flag is set to TRUE, the Report must be defined as available in Delta mode in the related Attribute Domain.

4.3.2.34 Restriction Type – Search/List Screen

No references for error messages.

4.3.2.35 Revisions/Audit Trail – List Screen

No references for error messages.

4.3.2.36 Revisions/Audit Trail – Details Screen

No references for error messages.

4.3.2.37 Role – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRC6001	▌ Submit button	Requestor not allowed	A Role can be created only by Service Operator, CSD or NCB.
DRC6006	▌ Role Name field ▌ Submit button	Role Name already assigned	When performing a Role creation request, the Role Name specified must not be already assigned within the same System Entity.
DRU6001	▌ Submit button	Requestor not allowed	A Role can be updated only by Service Operator, CSD or NCB. A User is authorised to update only data belonging to its own System Entity.

DRU6003	▌ Submit button	Data to be updated not found	When performing a Role update request it must refer to an existing and active instance of Role.
DRU6006	▌ Role Name field ▌ Submit button	Role Name already assigned	When performing a Role update request, the Role Name, if specified, must not be already assigned within the same System Entity.

4.3.2.38 Roles – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRD6001	▌ Restore button ▌ Delete button	Requestor not allowed	A Role can be deleted/restored only by Service Operator, CSD or NCB. A User is authorised to delete/restore only data belonging to its own System Entity.
DRD6002	▌ Role Name field ▌ Restore button	Role Name already assigned	When performing a Role restore request, the Role Name must not be already assigned within the same System Entity.
DRD6003	▌ Status field ▌ Delete button	Data to be deleted/restored not found	When performing a Role deletion request it must refer to an existing and active instance of Role
DRD6044	▌ Status field ▌ Restore button	Data to be deleted/ restored not found	When performing a Role restore request it must refer to an existing and deleted instance of Role.
DRD6050	▌ Delete button	The Role cannot be revoked due to a priority constraint.	A Role cannot be deleted if there still are valid instances of the following entities linked to it: Role Party, Role User.

4.3.2.39 Technical Addresses Network Services Link – Details Screen

No references for error messages.

4.3.2.40 Technical Addresses Network Services Link – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DPC3001	▌ Submit Row button	Requestor not allowed	Technical Address Network Service Link can only be created by Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only create Technical Address Network Service Links that fall under their responsibility according to the Hierarchical

			Party Model.
DPC3002	❚ Submit Row button	Unknown party	When performing a Technical Address Network Service Link create request, the Party must refer to an existing and active Party in CRDM.
DPC3003	❚ Technical Address field ❚ Submit Row button	Unknown technical address	When performing a Technical Address Network Service Link create request, the Technical Address must refer to an existing, active Technical Address in CRDM belonging to the Party provided in input.
DPC3004	❚ Network Service field ❚ Submit Row button	Unknown network service	When performing a Technical Address Network Service Link create request, the Network Service must refer to an existing, active Network Service in CRDM.
DPC3005	❚ Technical Address field ❚ Submit Row button	Invalid Technical Address Type	When performing a Technical Address Network Service Link create request, the Technical Address Type provided in input must be compliant with the Technical Address Type of the Network Service provided.
DPC3006	❚ Submit Row button	Technical Address Network Service Link for TIPS already defined for Party	When performing a Technical Address Network Service Link create request, each Party can have no more than one link to a Network Service for TIPS notifications and reports.
DPD3001	❚ Delete Row button	Requestor not allowed	Technical Address Network Service Link can only be deleted/restored by Service Operator, CSD or NCB. A user belonging to a CSD or NCB can only delete/restore Technical Address Network Service Links that fall under their responsibility according to the Hierarchical Party Model.
DPD3003	❚ Delete Row button	Unknown Technical Address Network Service Link	When performing a Technical Address Network Service Link Delete request, it must refer to an existing and active instance.
DPD3004	❚ Restore Row button	Technical Address Network Service Link is not deleted	When performing a Technical Address Network Service Link restore request, it must refer to an existing and deleted Technical Address Network Service Link.
DPD3005	❚ Restore Row button	Unknown Technical Address	When performing a Technical Address Network Service Link restore request, the 'Technical Address' linked must refer to an existing, active Technical Address in CRDM.
DPD3006	❚ Restore Row button	Unknown Party	When performing a Technical Address Network Service Link Restore request, the 'Party' linked must refer to an existing,

			active party in CRDM.
DPD3007	▌ Restore Row button	Unknown Network Service	When performing a Technical Address Network Service Link restore request, the 'Network Service' linked must refer to an existing, active Network Service in CRDM.
DPD3008	▌ Restore Row button	Technical Address not belongs to the linked party	When performing a Technical Address Network Service Link restore request, it must refer to a 'Technical Address' belonging to the same linked Party in CRDM.
DPD3009	▌ Restore Row button	Technical Address Network Service Link for TIPS already defined for Party	When performing a Technical Address Network Service Link restore request, each Party can have no more than one link to a Network Service for TIPS notifications and reports.

4.3.2.41 User – Details Screen

Reference for error message	Field or Button	Error Text	Description
DRD7001	▌ Restore button ▌ Delete button	Requestor not allowed	A User can be deleted/restored by CRDM Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only delete/restore users that fall under their responsibility according to the Hierarchical Party Model.
DRD7002	▌ Login Name field ▌ Restore button	Login Name already assigned	When performing a User Restore request, the Login Name must not be already assigned to another User in CRDM.
DRD7003	▌ Status field ▌ Delete button	Data to be deleted/restored not found	When performing a User Delete request, it must refer to an existing and active instance.
DRD7004	▌ Status field ▌ Restore button	Data to be deleted/restored not found	When performing a User Restore request, it must refer to an existing and deleted instance.
DRD7005	▌ Restore button ▌ System User Reference field	System User Reference already assigned	When performing a User Restore request, the System User Reference must not be already assigned to another User in CRDM.
DRD7007	▌ Parent BIC field ▌ Party BIC field ▌ Restore button	Unknown Party Identifier	When performing a User Restore request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM
DRD7008	▌ Restore button	Deletion not allowed due to	When performing a User Delete Request, there cannot be any existing and active

		existing links to Certificate DN	instances of User Certificate DN linked to it.

4.3.2.42 User – New/Edit Screen

Reference for error message	Field or Button	Error Text	Description
DRC7001	❚ Submit button	Requestor not allowed	A User can be created by Service Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only create users that fall under their responsibility according to the Hierarchical Party Model.
DRC7005	❚ Parent BIC field ❚ Party BIC field ❚ Submit button	Unknown Party Technical Identifier	When performing a User Create request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM.
DRC7006	❚ Login Name field ❚ Submit button	User Name already assigned	When performing a User Create request, the Login Name specified must not be already assigned to another User in CRDM.
DRC7007	❚ Submit button ❚ System User Reference field	Unknown Party Technical Identifier	When performing a User Create request, the System User Reference must not be already assigned to another User in CRDM.
DRU7001	❚ Submit button	Requestor not allowed	A User can be updated by Service Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only update users that fall under their responsibility according to the Hierarchical Party Model.
DRU7003	❚ Submit button ❚ Delete button	Data to be updated not found	When performing a User Update request, it must refer to an existing and active instance.
DRU7005	❚ Submit button ❚ System User Reference field	The specified System User Reference is already assigned	When performing a User Update request, the System User Reference must not be already assigned to another User in CRDM.
DRU7008	❚ Login Name field ❚ Submit button	The specified Login Name is already assigned	When performing a User Update request, the Login Name specified must not be already assigned to another User in CRDM.

4.3.2.43 User Certificate Distinguished Name Link – New Screen

Reference for error message	Field or Button	Error Text	Description
DRC0001	❚ Submit button	Requestor not allowed	A Certificate DN can be created only by users with the correct privilege.
DRC0002	❚ Login Name field ❚ Submit button	Invalid User	When performing a User Certificate DN creation request, the specified User must be within the System Entity of the requestor (if the requestor is a CSD or NCB) or within the Party of the requestor (if the requestor is a Payment Bank, External CSD or CSD Participant)
DRC0003	❚ Login Name field ❚ Submit button	Unknown or not active User	When performing a User Certificate DN creation request, the specified User must be an existing and active instance in CRDM.
DRC0004	❚ Certificate Distinguished Name field ❚ Submit button	Unknown or not active Certificate DN	When performing a User Certificate DN creation request, the specified Certificate DN must be an existing and active instance in CRDM.
DRC0005	❚ Login Name field ❚ Certificate Distinguished Name field ❚ Submit button	Link already exists	When performing a User Certificate DN creation request, there cannot be more than one active link between the same User and Certificate DN.
DRC0006	❚ Default field ❚ Submit button	Default Link already exists	When performing a User Certificate DN creation request, there can only be one User Certificate DN with Default flag set to TRUE for any given Certificate.
DRC0007	❚ Default field ❚ Submit button	Main User already exists for the same Party BIC	When performing a User Certificate DN creation request, there can only be one User Certificate DN with Main User flag set to TRUE for all the Users of any Party using the same BIC.

4.3.2.44 User Certificate Distinguished Name Links – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRD0001	❚ Restore button ❚ Delete button	Requestor not allowed	A Certificate DN can be deleted/restored only by Users belonging to the Party responsible for the User, or to said Party's CSD/NCB.
DRD0002	❚ Status field ❚ Delete button	Unknown or not active link	When performing a User Certificate DN delete request, it must refer to an existing and active instance.

DRD0003	▌ Login Name field ▌ Restore button	Unknown or not active User	When performing a User Certificate DN restore request, the specified User must be an existing and active instance.
DRD0004	▌ Certificate Distinguished Name field ▌ Restore button	Unknown or not active Certificate DN	When performing a User Certificate DN restore request, the specified Certificate DN must be an existing and active instance.
DRD0005	▌ Certificate Distinguished Name field ▌ Login Name field ▌ Restore button	Link already exists	When performing a User Certificate DN restore request, there cannot be more than one link between the same User and Certificate DN.
DRD0006	▌ Default field ▌ Restore button	Default link already exists	When performing a User Certificate DN restore request, there can only be one User Certificate DN with Default flag set to TRUE for any given Certificate.
DRD0007	▌ Status field ▌ Restore button	Unknown or not deleted link	When performing a User Certificate DN restore request, it must refer to an existing and deleted instance.
DRD0008	▌ Main User field ▌ Restore button	Main User already exists for the same Party BIC	When performing a User Certificate DN restore request, there can only be one User Certificate DN with Main User flag set to TRUE for all the Users of any Party using the same BIC

4.3.2.45 Users – Search/List Screen

Reference for error message	Field or Button	Error Text	Description
DRD7001	▌ Restore button ▌ Delete button	Requestor not allowed	A User can be deleted/restored by CRDM Operator, CSD, NCB, CSD Participant, External CSD or Payment Bank. Users belonging to CSDs, NCBs, CSD Participants, External CSDs and Payment Banks can only delete/restore users that fall under their responsibility according to the Hierarchical Party Model.
DRD7002	▌ Login Name field ▌ Restore button	Login Name already assigned	When performing a User Restore request, the Login Name must not be already assigned to another User in CRDM.
DRD7003	▌ Status field ▌ Delete button	Data to be deleted/restored not found	When performing a User Delete request, it must refer to an existing and active instance.
DRD7004	▌ Status field ▌ Restore button	Data to be deleted/restored not found	When performing a User Restore request, it must refer to an existing and deleted instance.

DRD7005	▌ System User Reference field ▌ Restore button	System User Reference already assigned	When performing a User Restore request, the System User Reference must not be already assigned to another User in CRDM.
DRD7007	▌ Parent BIC field ▌ Party BIC field ▌ Restore button	Unknown Party Identifier	When performing a User Restore request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM.
DRD7008	▌ Delete button ▌ Restore button	Deletion not allowed due to existing links to Certificate DN	When performing a User Delete Request, there cannot be any existing and active instances of User Certificate DN linked to it.