EUROPEAN CENTRAL BANK

EUROSYSTEM

T2S CHANGE REQUEST FORM			
General Information (Origin of Request) ☐ User Requirements (URD) or GUI Business Functionality Document (BFD) ☒ Other User Functional or Technical Documentation (SYS)			
Request raised by: ECB	**Institute:** ECB	**Date raised:** 30/11/2023	
Request title: CRDM Certificate DN management restrictions		**Request No.:** T2S 0820 SYS	
Request type: Common	**Classification:** Scope enhancement	**Urgency:** Fast-track[1]	
1. Legal/business importance parameter[2]: Medium		**2. Market implementation efforts parameter**[3]: Low	
3. Operational/Technical risk parameter[4]: Low		**4. Financial impact parameter**[5]: (provided by 4CB)	
Requestor Category: Eurosystem		**Status:** Allocated to a release	

Reason for change and expected benefits/business motivation:

This change request is raised in the context of the cross-service impact of T2-CR-129 '*CRDM admin users access rights scope limitation'.*

With the current CRDM implementation, the data scope related to update or deletion of a Certificate Distinguished Name (Certificate DN) is the system entity. This means that any user having the right privileges can update and delete any Certificate DN within its own system entity (provided they are not linked to any users), even if that user belongs to a party with no direct link to the party for which the DN was created.

As a result of this configuration, the RISK ID 19 of the T2 Risk Report was registered: "DN being not linked to a user can be deleted by any user". The risk refers to the increased likelihood of a Certificate DN being mistakenly or fraudulently deleted, due to the fact that a user of a party with no direct link to the party for which the Certificate DN was created can execute such deletion.

In addition, any Certificate DN is visible to any user in the system (with the right privileges). The Certificate DN Search/List screens in CRDM shows all Certificate DNs configured in CRDM, independently of the System Entity of the users who created them or the user(s) they are linked to. These Certificate DNs may include information which should not be visible to users belonging to parties not linked to the party for which the Certificate DN was created.

This change request is intended to mitigate the RISK 19 on the DN deletion while also addressing peripheral risks associated to the visibility or update of DNs.

Description of requested change:

[1] Fast-track justification: A fast-track approach is requested since the T2S users already raised an incident to highlight the urgency to restrict the visibility of the Certificate DNs to the default data scope, while keeping the possibility to create user-certificate DN links using DNs defined in different system entities.
[2] Legal/business importance parameter was set to 'Medium' because with this change the security concerns raised by the fact that a user can now see the certificate DNs defined in other system entities will disappear. Moreover, it will improve the management of this reference data.
[3] Market implementation effort parameter was set to 'Low' because it is not expected that a long implementation test campaign will be needed on the side of the CBs and CSDs.
[4] Operational/technical risk parameter was set to 'Low' since although the operational teams will need to get used to the new re-type functionality to link Certificate DNs defined in other system entities, it is not expected to have an operational impact on the side of CBs and CSDs.
[5] Low < 100kEUR < Low-Medium < 200 kEUR < Medium < 400kEUR < High < 700kEUR < Very high

The change introduces Certificate DN restrictions in following 2 areas:

1. Visibility restriction of Certificate DNs: the change is:

   - **restricting the full visibility** of Certificate DNs to the data scope i.e., users should only see DNs associated to a party within their data scope e.g., CSD/CBs users (with the right privileges) should be able to view Certificate DNs of their own users and the ones of their respective participants. Participants should be able to view on Certificate DNs associated to their own parties. A Certificate is associated to a party if it has been created by that party or if it is linked to a user of that party with a user-certificate DN link. The goal is to reinforce General Data Protection Regulation (GDPR) compliance and to limit security risks by limiting the access of information on a "need to know" basis.

   - **Introducing re-key (re-type) functionality**: If a DN needs to be linked to a user of a different party, the user with the right privileges (e.g. admin user) linking the DN with that user needs to re-type the full DN. If the DN was already created, it will appear on screen and the admin user can link it to a user. This means a DN can be queried in the Certificate DN Search/List screens. If the query includes the full string, it will appear in the results (as unique result). If the query does not contain the full string or uses wildcards, it will not appear in the results and therefore cannot be linked to a user.
     The possibility to link the DN should remain across system entities i.e. across the whole system.

2. Creation/Deletion/Update restriction of Certificate DNs: the change is:

   - **Restricting the Creation/Deletion/Update of Certificate DN to own's scope** (instead of the system entity currently): a user with the right privilege (e,g, admin user) can create/update/delete only their own DNs or DNs associated to a party within their data scope. For CSDs/CBs, this would mean all DNs associated to their own parties and to the ones of the respective participants. For participants, this would imply the DNs associated to their own parties. Associate to a party means that either it was created for that party or it is linked to a user of that party.

     The goal is to limit the risk of accidental/malicious deletion of DNs before they are linked to a user. As today, the deletion/update will be possible only if the DN is not linked to a user

The above restrictions apply only to the system entities and participants levels. The operator keeps full access rights across the whole system. i.e. The operator will keep the ability to view, update or delete any Certificate DN if it is not linked to a user and

User/Certificate DN links:

For User/Certificate DN links, the implementation will remain as today. The visibility/creation/deletion/update will continue to be limited to own's data scope. CBs/CSDs with the right privileges can view/create/delete/update user/DN link for users belonging to their own system entity (to own party or to their participants). Participants will be able to view/create/delete/update user/DN link for users belonging to their own data scope (party).

Impact overview on privileges

L2 has identified the following impact of the proposed implementation on privileges related to the visibility, update, and deletion of Certificate DNs and on the creation and deletion of User/DN links.

1. Operator:

		Visibility DNs	Create/Delete/Update DNs		
Parties	Roles	CRDM Privileges			
		Certificate Query	Create Certificate DN	Delete Certificate DN	Update Certificate DN
Operator	N/A	X	X	X	X

- No change
- The operator has all access across the system

2. CBs/CSDs:

		Visibility	Create/Delete/Update DNs		
Parties	Roles	CRDM Privileges			
		Certificate Query	Create Certificate DN	Delete Certificate DN	Update Certificate DN
CBs/CSDs	**Admin** (CB Access rights admin 2/4E)	X	X	X	X
	Normal user (CB Reader 2E)	X			

- **Certificate Query will allow CBs/CSDs to:**
  - Within their data scope (system entity):
    - i.e. see all DNs (their own and those of their participants)
  - Beyond their data scope (system entity):
    - i.e. see all DNs after a re-key (i.e. re-type). This means that an "open" query without any specific parameters would return all DNs within the normal data scope of the requestor. In order to display a DN belonging for example to another system entity, the requestor would have to re-key it in full. In this case the query result would be limited to that one single DN.

- **Create/Delete/Update Certificate DN will allow CBs/CSDs to:**
  - Create/Delete/Update DN associated to their own system entity (to own party and to their participants)

Note: Like today, the deletion/update will be possible only if the DN is not linked to a user.

3. Participants:

		Visibility	Create/Delete/Update DNs		
Parties	Roles	CRDM Privileges			
		Certificate Query	Create Certificate DN	Delete Certificate DN	Update Certificate DN
Participants	**Admin (AH Access Rights Admin 2E/4E)**	X	X	X	X

- **Certificate Query_AH will allow participants to:**
  - Within their data scope (party): see all DNs
  - Beyond their data scope (party) across the system: see all DNs after a re-key (i.e. re-type)

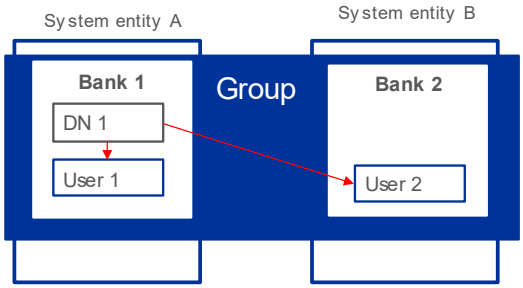
- **Create/Delete/Update Certificate DN_AH will allow participants to:**
  - Create/Delete/Update DN associated to their own data scope (party)

Practical example of the future implementation

Future implementation (TO -BE) – Practical example

- Bank 1 is part of a group which operates across different system entities
- The group intends to use a DN created by one bank with different users , across different system entities
- This setup will remain possible with the future implementation

Diagram



Process

- Bank 1: Admin creates DN1 and links it with User 1
- Bank 2: Admin rekeys the DN1 and links it with User 2

12 www.ecb.europa.eu ©

Although based on participants, this example is also applicable to system entities e.g CSD or CB user can be linked to a Certificate DN associated to a different CSD or CB.

Submitted annexes / related documents:

- T2S CR820-DN Allocation rules – excel file.
- CR129 Certificate DN Migration principles – presentation.

Outcome/Decisions:

*CRG on 5 December 2023: The CRG agreed to recommend CR-0820 for Steering Level authorisation, following a fast-track approach.
*AMI-SeCo on 21 December 2023: the AMI-SeCo agreed with the CRG recommendation of CR-820 for T2S Steering Level authorisation.
*CSG on 21 December 2023: the CSG agreed to authorise CR-820.
*NECSG on 21 December 2023: the NECSG agreed to authorise CR-820.
*MIB on 21 December 2023: the MIB agreed to authorise CR-820.
*OMG on 25 October 2024: the OMG agreed to approve the DN migration principles, which are submitted as an annex for CR-0820.
*OMG on 4 March 2025: the OMG identified an operational impact from the scope of CR-0820, due to the required migration of existing Certificate DNs for the implementation of CR-0820.
*CRG on 4 March 2025: the CRG agreed to recommend to the PMG the inclusion of CR-0820 in the scope of R2025.NOV.
*PMG on 5 March 2025: the PMG agreed to recommend the inclusion of CR-0820 in the scope of R2025.NOV.
*CSG on 14 March 2025: the CSG approved the inclusion of CR-0820 in the scope of R2025.NOV.
*NECSG on 14 March 2025: the NECSG approved the inclusion of CR-0820 in the scope of R2025.NOV.
*MIB on 27 March 2025: the MIB approved the inclusion of CR-0820 in the scope of R2025.NOV.

Documentation to be updated:

UDFS
1.2.2.1.2 Privilege
[…]

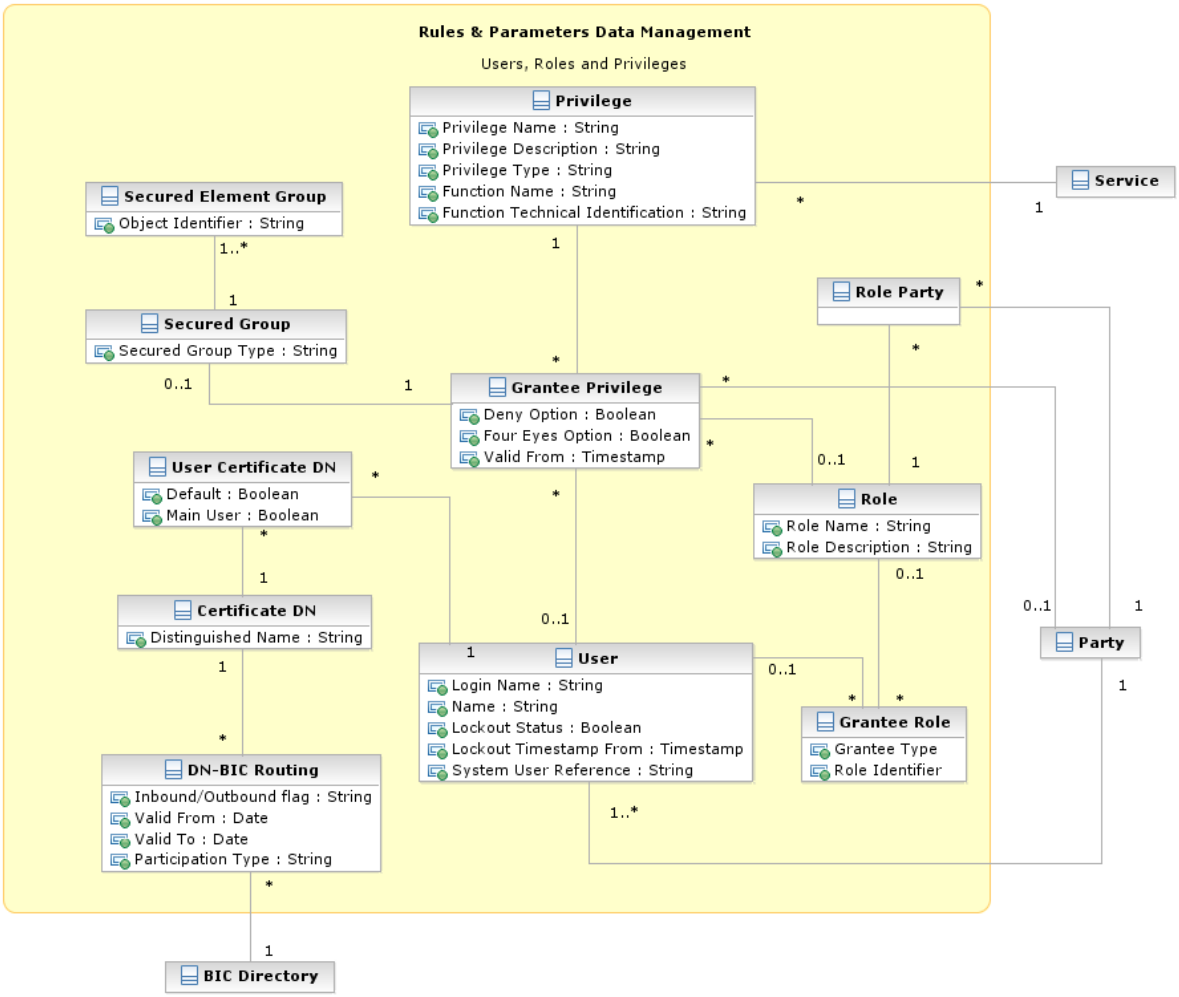
TABLE 1 – ACCESS RIGHTS MANAGEMENT

These privileges are related to user functions within CRDM. As such, it is possible to use the same privilege(s) to maintain data related to multiple Services/components. For example, the same privileges can be used to configure a User to access different Services.

PRIVILEGE	USER FUNCTION	PRIVILEGE TYPE	OBJECT TYPE	DEFAULT DATA SCOPE
[…]				
Update Certificate Distinguished Name	Certificate DN – Edit	System	n/a	Certificate DN within own System Entity (for CSDs and Central Banks) or own Party (for CSD Participants/External CSDs/Payment Banks/Ancillary Systems).
Delete Certificate Distinguish Name	Certificate DN – Delete/Restore	System	n/a	Certificate DN within own System Entity (for CSDs and Central Banks) or own Party (for CSD Participants/External CSDs/Payment Banks/Ancillary Systems).
[…]				

1.3.6 Access rights management

The following diagram shows the conceptual data model for *Users*, *Roles* and *Privileges* management.



[…]

2. Certificate DN

This entity includes all reference data for *Certificate DN*.

ATTRIBUTE	DESCRIPTION
Distinguished Name	It specifies the distinguished name.

~~Each~~ *Certificate DN* are linked to the *Party* they belong to and can be linked to one or many *Users*.

4.5.3.29 Certificate Distinguished Name

- Record Type: “Certificate DN”

The record is used to create a certificate distinguished name.

Flat file	Excel Column	Column Name	Format	Description	Rules	Occurs per Record	Occurs per Group
2	B	Record Id	NUMERIC (10)	Unique identifier of the record.		1..1	
Group “Certificate Distinguished Name”						1..1	

3	C	Certificate Distinguished Name	VARCHAR (256)		EPC SCT Inst and ISO15022 interoperability character set restrictions do not apply	1..1	
Group "Party"					1..1		
4	I	Parent BIC	CHAR (11)	Party parent BIC.			
5	J	BIC	CHAR (11)	Party BIC.			1..1

UHB

2.3.3.4 Certificate Distinguished Names – Search/List Screen

Context of Usage

This screen enables the user to display a list of Certificate Distinguished Names matching the entered criteria.

This screen gives also the possibility to update, delete and restore a selected Certificate Distinguished Name (only active items can be deleted or updated, only deleted items can be restored) and to show Revisions and Audit trail of a selected one.

Finally, it is possible to create a new Certificate Distinguished Name.

Duly authorised users can:

- see and manage Certificate Distinguished Names under their data scope,
- See Certificate Distinguished Names outside their data scope if the same are linked to users under the data scope of the requestor
- See Certificate Distinguished Name outside the data scope of the requestor when searching for the complete name without wildcard.

~~The Certificate Distinguished Names are visible to all the users with no datascope restriction.~~

[…]

Screenshot

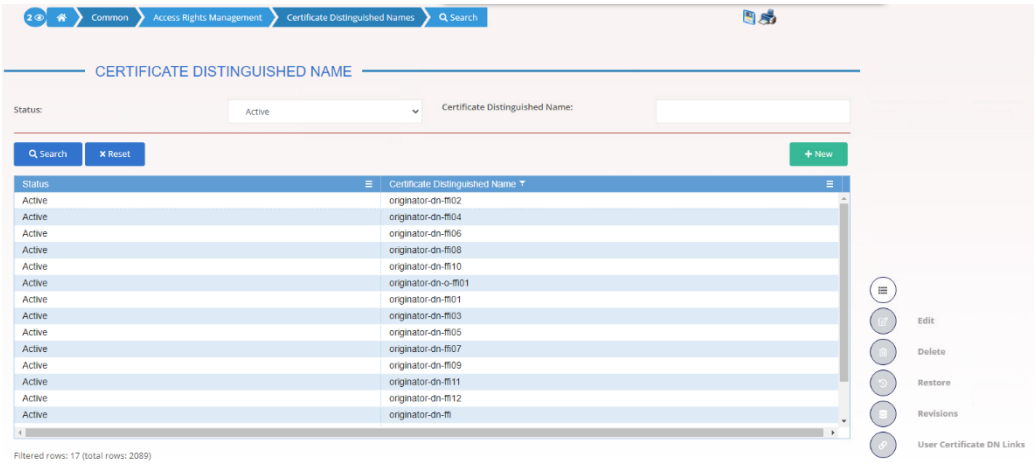


Illustration 1: Certificate Distinguished Names – search/list screen

Fields Description

Certificate Distinguished Names - Search Criteria	
Status	Select the status of the Certificate Distinguished Names from the possible values: ▌All ▌Active (default value) ▌Deleted Reference for error message [ ]: ▌DRDA003 ▌DRDA004 This field is mandatory.
Certificate Distinguished Name	Enter the Distinguished Name of the Certificate you want to search. Reference for error message [ ]: ▌DRDA002 Required format is: max 256x characters (UTF-8 except '>', '<', '&').
Parent BIC	Enter or select the parent BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRDA007 Required format is: max. 11x characters.
Party BIC	Enter or select the BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRDA007 Required format is: max. 11x characters.

Certificate Distinguished Names - List	
Status	Shows the status of the Certificate Distinguished. Reference for error message [ ]: ▌DRDA003 ▌DRDA004

Certificate Distinguished Name	Shows the Distinguished Name of the Certificate. Reference for error message [ ]: ▌DRDA002
Parent BIC	Shows the parent BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRDA001
Party BIC	Shows the BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRDA001
Party Short Name	Shows the short name of the party related to the Certificate Distinguished Name.

2.3.3.5 Certificate Distinguished Names – New/Edit Screen

Context of Usage

The screen "Certificate Distinguished Name – New/Edit" enables the user to create a new Certificate Distinguished Name or to update an existing active one. As far as the update is concerned, the users can only update the case of the letters of the existing DN: the existing DN cannot be amended in the content (changing the existing values, space included) but only changing lowercase letters in uppercase ones or the other way around.

Duly authorised users can manage Certificate Distinguished Names under their data scope.

Screen Access

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

▌*Common >> Access Rights Management >> Certificate Distinguished Names >> New*

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

Privileges

To use this screen, the following Privileges are needed [▶]:

▌Create Certificate Distinguished Name

▌Update Certificate Distinguished Name

Screenshot

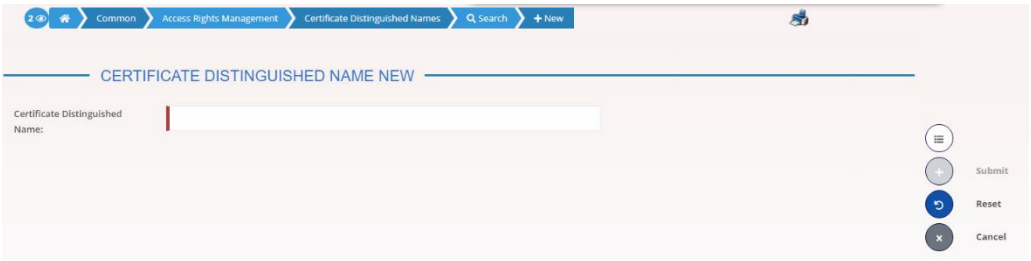


Illustration 2: Certificate Distinguished Names – new/edit screen

Fields Description

Certificate Distinguished Names	
Certificate Distinguished Name	Enter the distinguished name of the certificate you want to create. Reference for error message [▶]: ▌DRCA002 ▌DRUA002 ▌DRUA003 The field is mandatory. Required format is: max 256x characters (UTF-8 except '>', '<', '&').
Parent BIC	Enter or select the parent BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRCA003 This field is mandatory in create mode. This field is read-only in edit mode. Required format is: 11x characters.
Party BIC	Enter or select the BIC of the party related to the Certificate Distinguished Name. Reference for error message [▶]: ▌DRCA003 This field is mandatory in create mode. This field is read-only in edit mode.

	Required format is: 11x characters.

Buttons

Submit	This function enables the user to create a new certificate distinguished name or to update an existing active one according to the information entered in the fields. Reference for error message [ ]: ▪ DRCA001 ▪ DRCA002 ▪ DRUA001 ▪ DRUA002 ▪ DRUA003
Cancel	This function enables the user to cancel the process and return to the previous screen.
Reset	This function enables the user to set all fields to default value and blanks out all optional fields.

4.3.2.26 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 and if falls under the requestor's responsibility according to the Hierarchical Party Model..
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.
DRDA007	▪ Parent BIC field ▪ Party BIC field ▪ Restore button	Unknown Party Identifier	When performing a Certificate DN Restore request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM in the data scope of the requestor.

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.

4.3.2.27 Certificate Distinguished Names – New/Edit 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.
DRCA003	▮ Parent BIC field ▮ Party BIC field ▮ Submit button	Unknown Party Technical Identifier	When performing a Certificate DN Create request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM in the data scope of the requestor.
DRUA001	▮ Submit button	Requestor not allowed	A Certificate DN can be updated only by users with the correct privilege ~~that belong to the same System Entity as the Certificate DN~~ and if falls under the requestor's responsibility according to the Hierarchical Party Model.
DRUA002	▮ Submit button	Certificate DN not found	When performing a Certificate DN Update request, it must refer to an existing and active Certificate DN.
DRUA003	▮ Certificate Distinguished Name field ▮ Submit button	Only uppercase/lowercase changes allowed	When performing a Certificate DN Update request, the Distinguished Name string can only be modified by changing uppercase characters into the corresponding lowercase ones and vice versa.

Preliminary assessment:

Detailed assessment:

			Process	User Interaction	Business Data Definition	Non-functional Requirements
CENTRAL LIQIDITY MANAGEMENT (CLM)	GENERAL	CLM Payment Order				
		CLM Liquidity Transfer Order				
		CLM Liquidity Reservation				
	CENTRAL BANK SERVICES	Modify Credit Line				
		Connected Payments				
		Overnight Deposit				
		Marginal Lending				
		Minimum Reserve Management				
		EoD General Ledger Files				
REAL-TIME GROSS SETTLEMENT (RTGS)	GENERAL	RTGS Payment Order				
		Queue Management				
		RTGS Liquidity Transfer Order				
		RTGS Liquidity Reservation				
		RTGS Services for Ancillary Systems (AS)				
	CB SER-VICES					
COMMON COMPONE	GENRAL	ESMIG				
		CRDM		x		

		Business Day				
		User Roles and Access				
		Information and Reporting				
		Data Warehouse Services				
	CENTRAL BANK SERVICES	Billing				
		Legal Archiving				
		Contingency Settlement				

Impact on major documentation		
Document	**Chapter**	**Change**
Impacted UDFS chapter	1.2.2.1.2 Privilege 1.3.6 Access rights management 4.5.3.29 Certificate Distinguished Name	Change of default data scope for Update/Delete Certificate Distinguish Name privilege Amendment of data model in order to include the link between the Certificate DN and Party Introduction of fields 'Parent BIC' and 'Party BIC' for Data Migration Tool when creating a certificate DN.
Additional deliveries for Message Specification (UDFS, MyStandards, MOP contingency templates)		
UHB	2.3.3.4 Certificate Distinguished Names – Search/List Screen 2.3.3.5 Certificate Distinguished Names – New/Edit Screen	Introduction of fields Parent BIC and Party BIC as search criterion and Parent BIC, Part BIC and Party Short Name as fields in the list. Introduction of fields Parent BIC and Party BIC in New/Edit mode.
External training materials		
Other impacted documentation	Data Model	Amendment of data model in order to include the link between the Certificate DN and Party
Impacted GDPR message/ screen fields		

Links with other requests				
Links	Reference		Title	

OVERVIEW OF THE IMPACT OF THE REQUEST ON THE T2SYSTEM AND ON THE PROJECT

Summary of functional, development, infrastructure and migration impacts

CRDM

Introduction of the following fields in CRDM **Certificate Distinguished Names** GUI screen:

- Search/List: Parent BIC and Party BIC as search criterion and Parent BIC, Part BIC and Party Short Name as fields in the list
- New/Edit: Parent BIC and Party BIC (read only in edit mode)

Introduction of the following fields in CRDM **Certificate Distinguished Names** DMT:

- New: Parent BIC and Party BIC

Introduction of the following new business rules:

- DRDA007: When performing a Certificate DN Restore request, the specified Party Technical Identifier

must refer to an existing, active and open or future Party in CRDM.
- DRCA003: When performing a Certificate DN Create request, the specified Party Technical Identifier must refer to an existing, active and open or future Party in CRDM.

Amendment of the following business rule:
- DRUA001 allowing the update of a Certificate Distinguished Name only when belonging to the data scope of the requestor.
- DRDA001 allowing the deletion of a Certificate Distinguished Name only when belonging to the data scope of the requestor.

The visibility of Certificate Distinguished Names must be amended as follows:
- Certificate distinguished Names retrieved by the query for CSDs and Central Banks must show only objects under the proper System Entity
- Certificate distinguished Names retrieved by the query for Party CSD Participants/External CSDs/Payment Banks/Ancillary System must show only objects owned by the requestor Party
- Additional visibility criterion: If the query includes the full Certificate distinguished Name without wildcard, it will appear in the list, even if the object is not under the data scope of the requestor party.
- Additional visibility criterion: The query retrieves also Certificate Distinguished Names outside the datascope of the requestor if there exists in CRDM an User-DN Link between this DN and a user in the data scope of the requestor.

Change in suggested values for field Certificate Distinguished Name in CRDM **User-Certificate Distinguished Names Link** screen:
- The fields becomes an auto-complete select box with the possibility to enter Certificate Distinguished Names outside of the data scope of the requestor even if not suggested.

Main cost drivers

CRDM:
- Introduction of new fields and business rules for Certificate Distinguished Name Search/List and New/Edit Screen.
- Modification of data scope and query search criteria for Certificate Distinguished Name
- Changes for Certificate DN on DMT side (Creation), on CRDM BE side (Create, Update, Delete, view and visibility), on CRDM GUI side (Search/List screen, New screen, Edit screen, User-Certificate Distinguished Names Link).

Impact on other TARGET Services and projects

TIPS: No impact on TIPS. Nevertheless, a TIPS-ICN will be drafted to inform TIPS users on the restrictions introduced in CRDM on the relevant common object (i.e. Certificate DN).

ECMS: No impact on ECMS.

Summary of project risk

None

Security analysis

No adverse effect has been identified during security assessment.