Change Request form

General Information (Origin of Request)		
☒ User Requirements Document (URD) ☐ User Detailed Functional Specification (UDFS) ☐ User Handbook (UHB) ☐ Other User Functional or Technical Documentation (SYS)		
Request raised by: Eurosystem	**Institution:** ECB	**Date raised:** 11/04/2024
Request title: CRDM admin users access rights scope limitation		**Request ref. no:** TIPS-0079-URD
Request type: Alignment Change Request		
1. Legal/business importance parameter:		**2. Market implementation efforts parameter – Stakeholder impact:**
3. Operational impact:		**4. Financial impact parameter:**
5. Functional/ Technical impact:		**6. Interoperability impact:**
Requestor Category: ECB		**Status:** Allocated to a release

Reason for change and expected benefits/business motivation:

As the certificate DNs migration plan will affect all TIPS users, this alignment change request is drafted to enable the tracking of the different steps related to this migration in the TIPS STP (e.g. for the testing).

Description of requested changes:

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.

   - **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 en tities 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:** 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 above restrictions are on participants' level. 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

Change Request form

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. Participants will be able to view/create/delete/update user/DN link for users belonging to their own data scope (party).

Submitted annexes / related documents:

Annex 1: Overview impact on privileges

Annex 2: Practical example of the future implementation

Proposed wording for the Change request:

High-level description of Impact:

Impacts on other projects and products:

Outcome/Decisions:

Annex 1: 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)

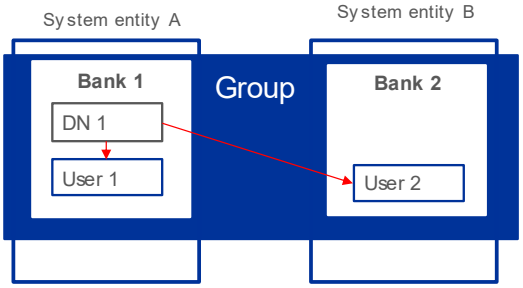
- **Create/Delete/Update Certificate DN_AH will allow participants to:**
  - Create/Delete/Update DN associated to their own data scope (party)

Annex 2: 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

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.