EUROPEAN CENTRAL BANK

EUROSYSTEM

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

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.

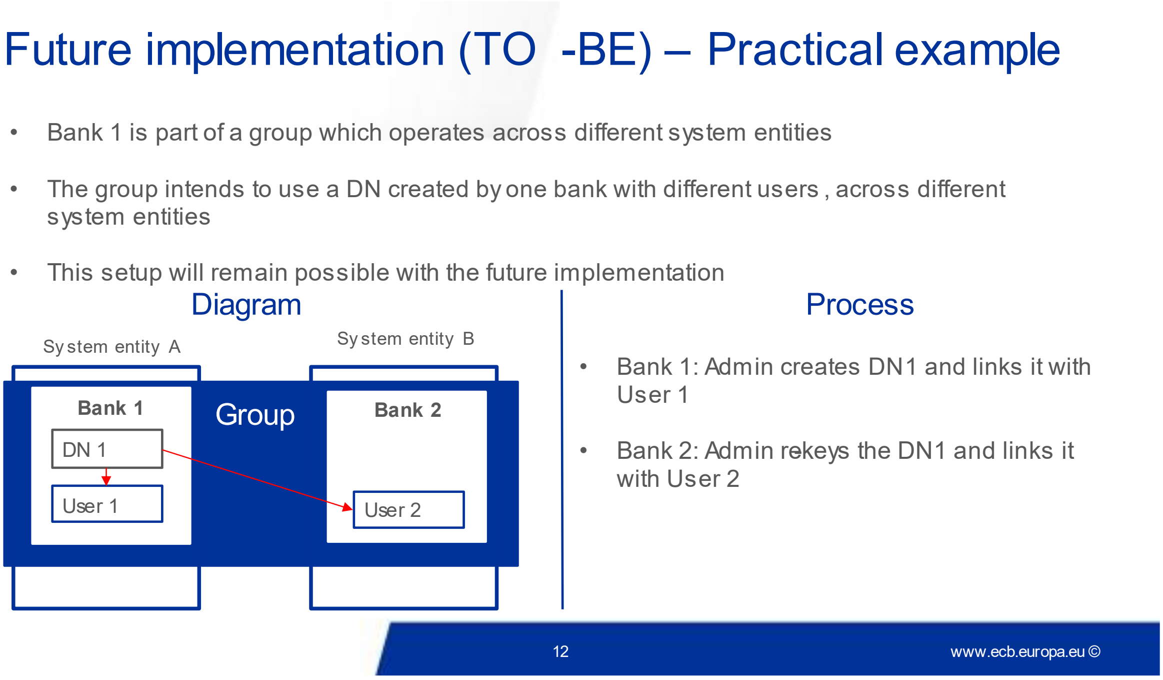
3. Participants:

		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

System entity A

System entity B

Group

Bank 1

DN 1

User 1

Bank 2

User 2

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:

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.

Documentation to be updated:

Preliminary assessment:

Detailed assessment: