EUROPEAN CENTRAL BANK

EUROSYSTEM

T2-0129-URD “CRDM admin users access rights scope limitation”

TIPS-CG meeting

12/10/2023

T2-0129-URD: Main changes

1) Limit the ability to view, create/update/delete DNs, create/delete user-DN link to the data scope of relevant party in **3 layers** :

- Operator
- System Entity (CBs and CSDs)
- Participants

2) Attach a DN to a party: create an additional attribute (party) in DN

Current implementation

	Current implementation
Visibility	System-wide i.e. any DN in the system can be: 1) viewed by any user 2) linked to one's own logical User (through a User-DN link)
Update/Deletion	System entity i.e. DN can be updated/deleted only by any admin users belonging to the same entity as the user who created it (provided that: that Certificate DN is not linked to any user)

Scope of Risk 19: “DN being not linked to a user can be deleted by any user within the same system entity as the DN”

Current implementation: background and constraints (1/2)

	Current implementation
Visibility	System-wide i.e. any DN in the system can be: 1) viewed by any user 2) linked to one's own logical User (through a User-DN link)

Background

- ECB Risk Management (LoD2): risk due to disclosure of information to non-interested parties which needs to be mitigated/documented.

Constraints

- System-wide visibility is an important T2S requirement. T2S participants require visibility of Certificate DNs, independently of the system entity of the users they belong to. T2 participants also require for some use cases.
- NCB admin users need access to update/delete on behalf of participants.

Current implementation: background and constraints (2/2)

	Current implementation
Update/Deletion	System entity i.e. DN can be updated/deleted only by any user belonging to the same entity as the user who created it (provided that: that Certificate DN is not linked to any user)

Background

- This is the scope of risk 19 → a mitigation is needed
- ECB Risk Management (LoD2) : The risk is limited as the update/deletion scope is system-entity and only non-linked DNs can be deleted)

Constraints

- NCB admin users need access to update/delete on behalf of participants

Challenges

- Current DN format does not identify the party

T2-0129-URD implementation: Visibility

Visibility restriction

- Restrict the full visibility: Users should only see the DNs associated to a party within their data scope. “Associated” means:
  - Created by a user of that party (or a party under their responsibility for CSDs/CBs)
  - Linked to a user of that party (or a party under their responsibility for CSDs/CBs)

→ Objectives: limit the information to “need to know basis”, GDPR compliance.

- Re-key (Re-type) functionality: If a DN needs to be linked to a user of a different party, the admin user linking the DN with that user needs to re-type the DN. Then this admin user will see that the DN was already created, and can link it. The possibility to link the DN should remain across system entities

T2-0129-URD implementation: Update/Deletion

Update/deletion restriction

- Restrict the update/deletion to own's scope (instead of the system entity): An admin user can delete only DNs associated to a party within their data scope

→ Objectives: limit the risk of accidental/malicious deletion of DNs before they are linked to a user.

Impact on User/DN links

- “User DN links”: No change. The implementation of “User/DN links” will remain as today.

→ The visibility/creation/deletion/update of User/DN links 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).

What it is the impact in terms of privileges?

Current implementation

		Visibility	Create/Delete/Update DNs			Create/Delete User/DN links	
		CRDM Privileges					
Parties	**Roles**	**Certificate Query**	**Create Certificate DN**	**Delete Certificate DN**	**Update Certificate DN**	**Create User Certificate DN Link**	**Delete User Certificate DN Link**
Operator	N/A	X	X	X	X	X	X
CB	**Admin** (CB Access rights admin 2/4E)	X	X	X	X	X	X
	Normal user (CB Reader 2E)	X	-	-	-	-	-
Participants	**Admin** (AH Access Rights Admin 2E/4E)	X	X	X	-	X	X
	Normal user (AH Reader 2E)	-	-	-	-	-	-

Impact in terms of privileges

Proposed future implementation (TO-BE) - Operator

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

- No change: the privileges and the user functions they can trigger will remain the same

- The operator has all access across the system

Impact in terms of privileges

Proposed future implementation (TO-BE) – CBs/CSDs

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

The privileges will remain the same. But the scope of the user functions they can trigger will change.

- **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)

- **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.

- **Create/Delete User Certificate DN Link will allow CBs/CSDs to:**

- Create/Delete user/DN link for users belonging to their own system entity (to own party or to their participants)

Impact in terms of privileges

Proposed future implementation (TO-BE) - Participants

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

The privileges will remain the same. But the scope of the user functions they can trigger will change.

- **Certificate Query 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 will allow participants to:**

- Create/Delete/Update DN associated to their own data scope (party)

Note: the privilege to update the DN shall be granted to the participant Admin as well.

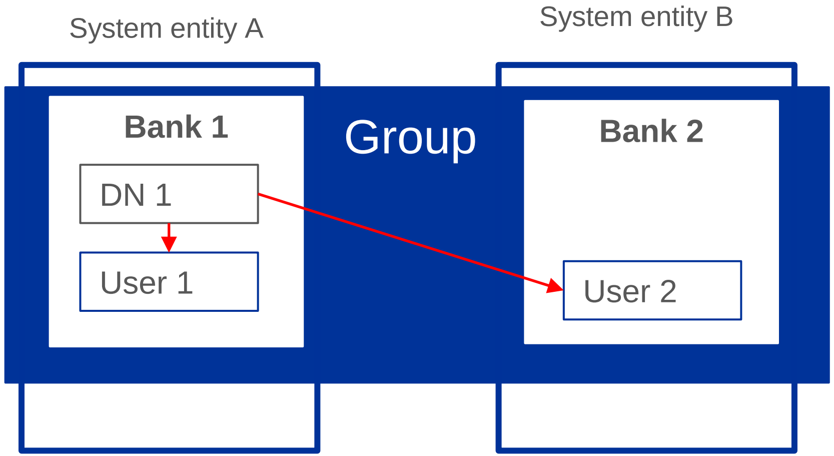
- **Create/Delete User Certificate DN Link will allow participants to:**

- Create/Delete user/DN link for users belonging to their own data scope (party)

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 re-keys the DN1 and links it with User 2