BANQUE DE FRANCE
EUROSYSTÈME

TARGET2/T2S CONSOLIDATION

BANQUE DE FRANCE
SERI

JANVIER 2022

BANQUE DE FRANCE
EUROSYSTÈME

PROCÉDURE CONCERNANT L'UTILISATION ET LE PARAMÉTRAGE DU USER A2A

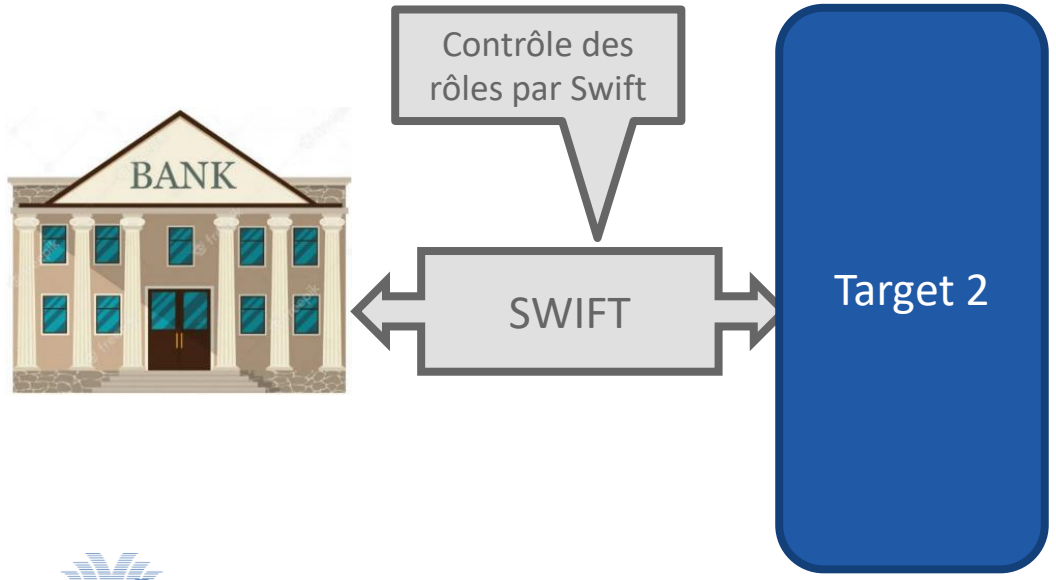
BANQUE DE FRANCE
SERI

JANVIER 2022

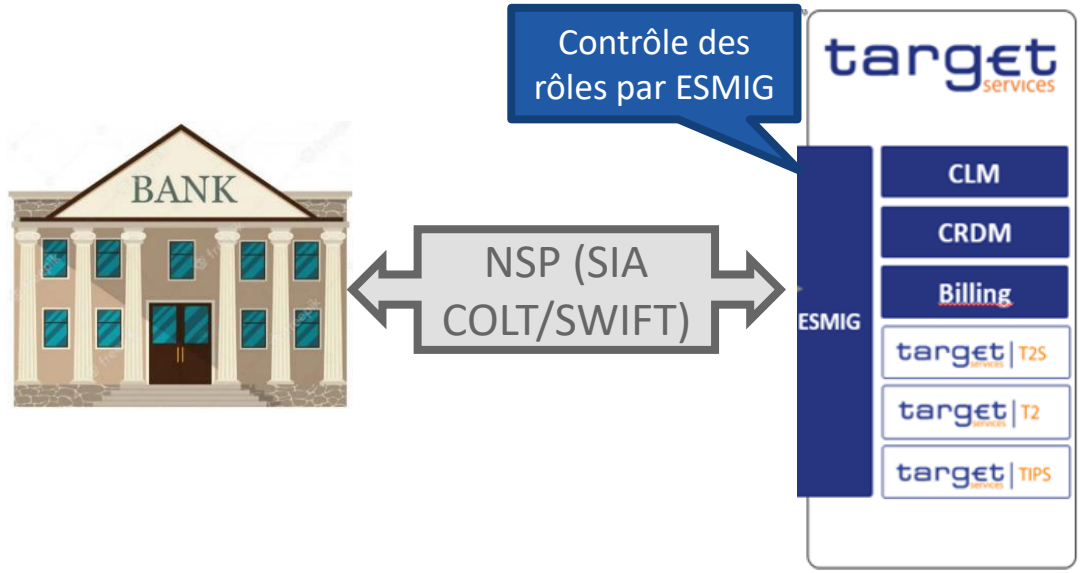
Procédure concernant l'utilisation et le paramétrage du user A2A

- Le User A2A est nécessaire afin de permettre un contrôle des rôles (contenant des privilèges) sur les messages entrant dans ESMIG en A2A.
- Dans Target2, Les rôles (RBAC) était accordés et contrôlés par Swift.
- Target Services est un service agnostique en terme de NSP (Network Service Provider). Les rôles sont donc accordés par CRDM et contrôlés par ESMIG.

Fonctionnement Actuel de T2



Fonctionnement avec Target Services



Procédure concernant l'utilisation et le paramétrage du user A2A

Où ESMIG cherche le User A2A pour contrôler les rôles?

- L'élément « System User Reference » du User A2A doit figurer dans le BFH (Business File Header ou Head.002) ou dans le BAH (s'il n'y a pas de BFH) (Business Application Header ou Head.001).
- Ce contrôle est effectué pour tous messages entrant dans ESMIG en A2A, quelque soit le type de participation (Direct ou Multi-addressee pour RTGS) et le type de management (Direct, co-manager ou co-managé).

- L'exemple à droite est un head.001 (BAH) d'un pacs.009 envoyé par la BdF à un participant multi-addressee. Le User A2A de la BdF est donc renseigné.

```
<AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
    <Fr>
        <FIId>
            <FinInstnId>
                <BICFI>BDFEFR2TXXX</BICFI>
                <ClrSysMmbId>
                    <ClrSysId>
                        <Prtry>T2</Prtry>
                    </ClrSysId>
                    <MmbId>BDFEFR2TXXX-A2A</MmbId>
                </ClrSysMmbId>
            </FinInstnId>
        </FIId>
    </Fr>
    <To>
        <FIId>
            <FinInstnId>
                <BICFI>ZYDQFR20BQM</BICFI>
            </FinInstnId>
        </FIId>
    </To>
    <BizMsgIdr>CTO-CBtoPBmultiAddresseeMD1</BizMsgIdr>
    <MsgDefIdr>pacs.009.001.08</MsgDefIdr>
    <CreDt>2021-10-04T08:30:00Z</CreDt>
    <Sgntr>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    </Sgntr>
</AppHdr>
```

Procédure concernant l'utilisation et le paramétrage du user A2A

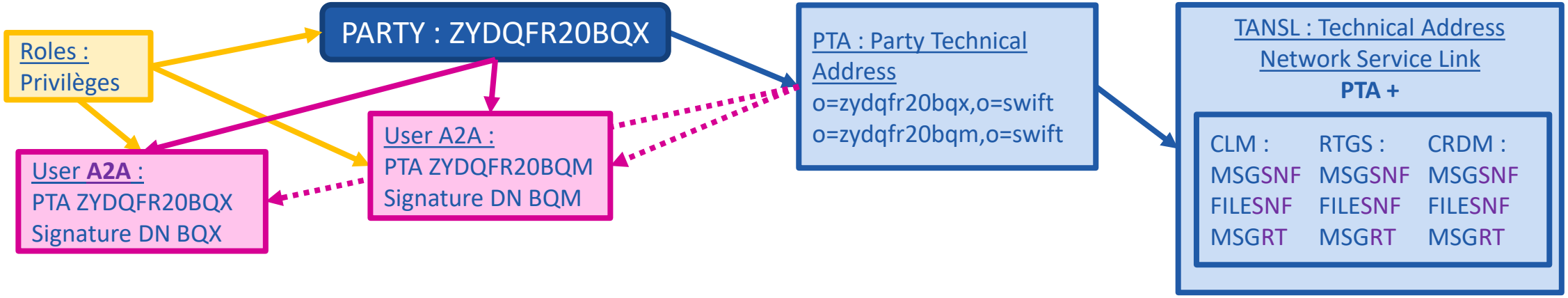
Qui paramètre le User A2A dans CRDM pour qui ?

- Les messages A2A émis vers Target services doivent contenir un User A2A.
- Un même User A2A peut être utilisé pour un ou plusieurs modules en fonction des rôles qui lui sont accordés (CLM/RTGS/T2S/…)

- **Pour les participants directs :** Ils paramètrent leur propre User A2A et lui accorde les rôles dans CRDM.
- **Pour les participants Multi-Addressee (MAA) :** C'est le participant direct qui communique son propre User A2A à ses participants MAA ou crée un (ou plusieurs) nouveau User A2A à usage de ses participants MAA et lui (leur) accorde des rôles.
- **Pour les participants Addressable :** pas de User A2A car ils n'envoient pas de message directement à ESMIG.
- **Pour les co-managers :** Ils paramètrent leur propre User A2A (et leur accorde des rôles) qui leur permettra également d'envoyer des messages pour le compte de leurs co-managés.
- **Pour les co-managés :** pas de User A2A à paramétrer car ils n'envoient pas de message A2A.

Procédure concernant l'utilisation et le paramétrage du user A2A

Quels sont les éléments nécessaires au bon fonctionnement du User A2A?



- **PTA Party technical Addresses :** Ce sont les DNs utilisés par le participant direct et le(s) participant(s) multi-addressee. (Les participants addressable passent par le participant direct et n'ont pas de DN propre.) pour les échanges A2A et enregistrés au niveau du Party.
- **TANSL Technical Address Network Service Link** (nous utilisons dans l'exemple Swift comme NSP) : Ce paramétrage associe le PTA aux services Swift utilisés, module par module de Target Services.
- **DN de Signature :** DN utilisé pour signer le message. Il peut être identique au PTA ou différent. La signature est présente dans le BAH (Head.001).
- **User A2A :** identifiant présent dans le BAH (head.001) des messages envoyés aux modules Target Services.
- **Roles :** Ces rôles contiennent des privilèges qui permettent l'accès aux modules Target Services et à leurs différentes fonctions. Ils doivent d'abord être rattachés à la « Party » par la SAR, pour que les administrateurs de cette entité puissent ensuite les affecter à leurs utilisateurs
  - Affectés à un user A2A, ils déterminent la capacité des messages envoyés avec le DN associé à ce user à voir/modifier les données du participant (par exemple à régler des paiements sur ses comptes)

Procédure concernant l'utilisation et le paramétrage du user A2A

Qui paramètre quel élément ?

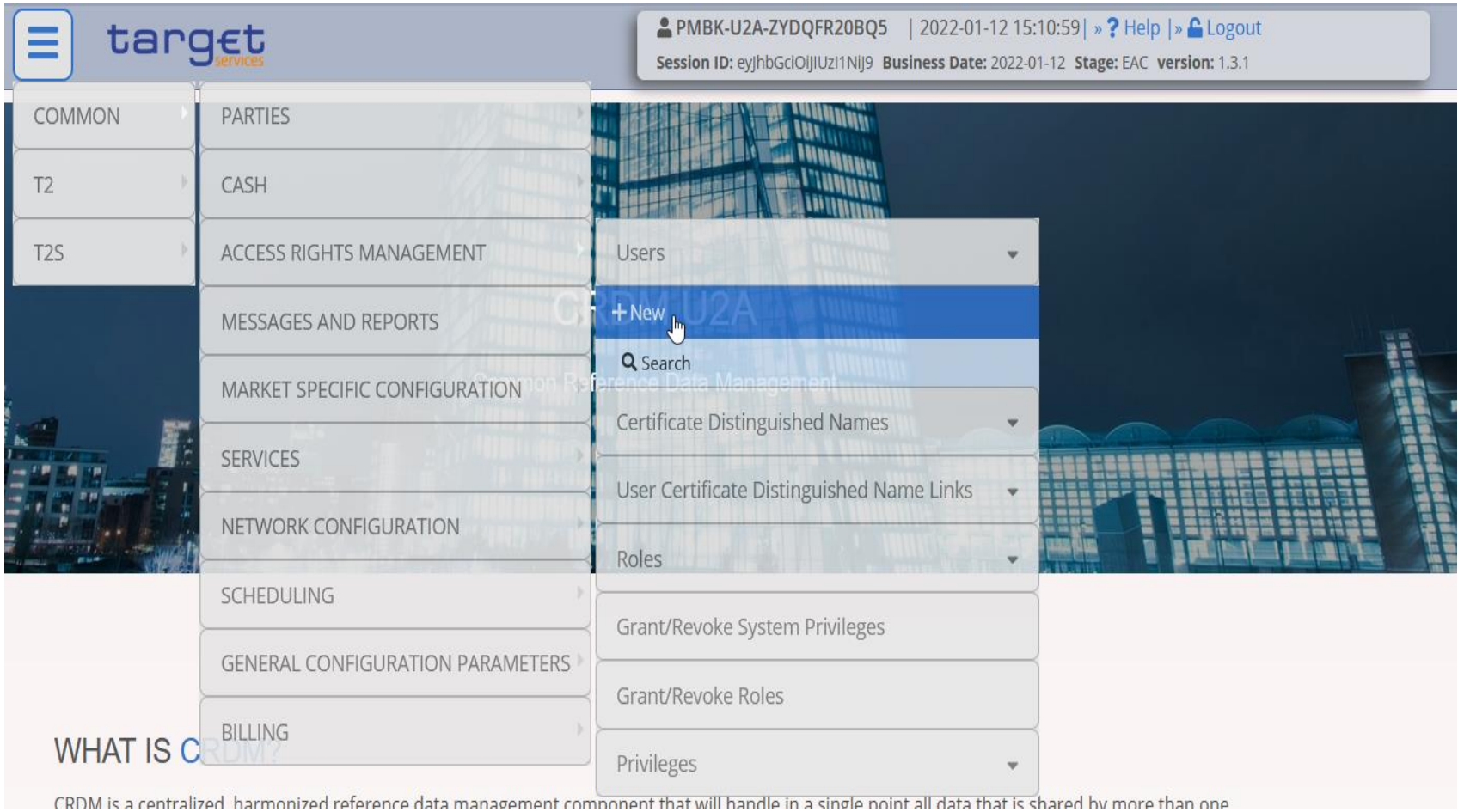
- La BdF sur la base du formulaire fournit par le participant paramètre :
  - La création du Party
  - L'ajout des Party Technical Address au Party
  - L'attribution des rôles au Party

- Le participant paramètre :
  - La création du/des User A2A
  - L'ajout des rôles à/aux User A2A dans la limite des rôles accordés au Party
  - L'ajout du lien entre Party Technical Address + DN de signature et le User A2A (plusieurs PTA et DN de signature peuvent être liés à un User A2A)

Procédure concernant l'utilisation et le paramétrage du user A2A

Comment créer un User A2A dans CRDM ?

Connectez vous à CRDM en U2A, puis sélectionnez COMMON > ACCESS RIGHTS MANAGEMENT > Users > New



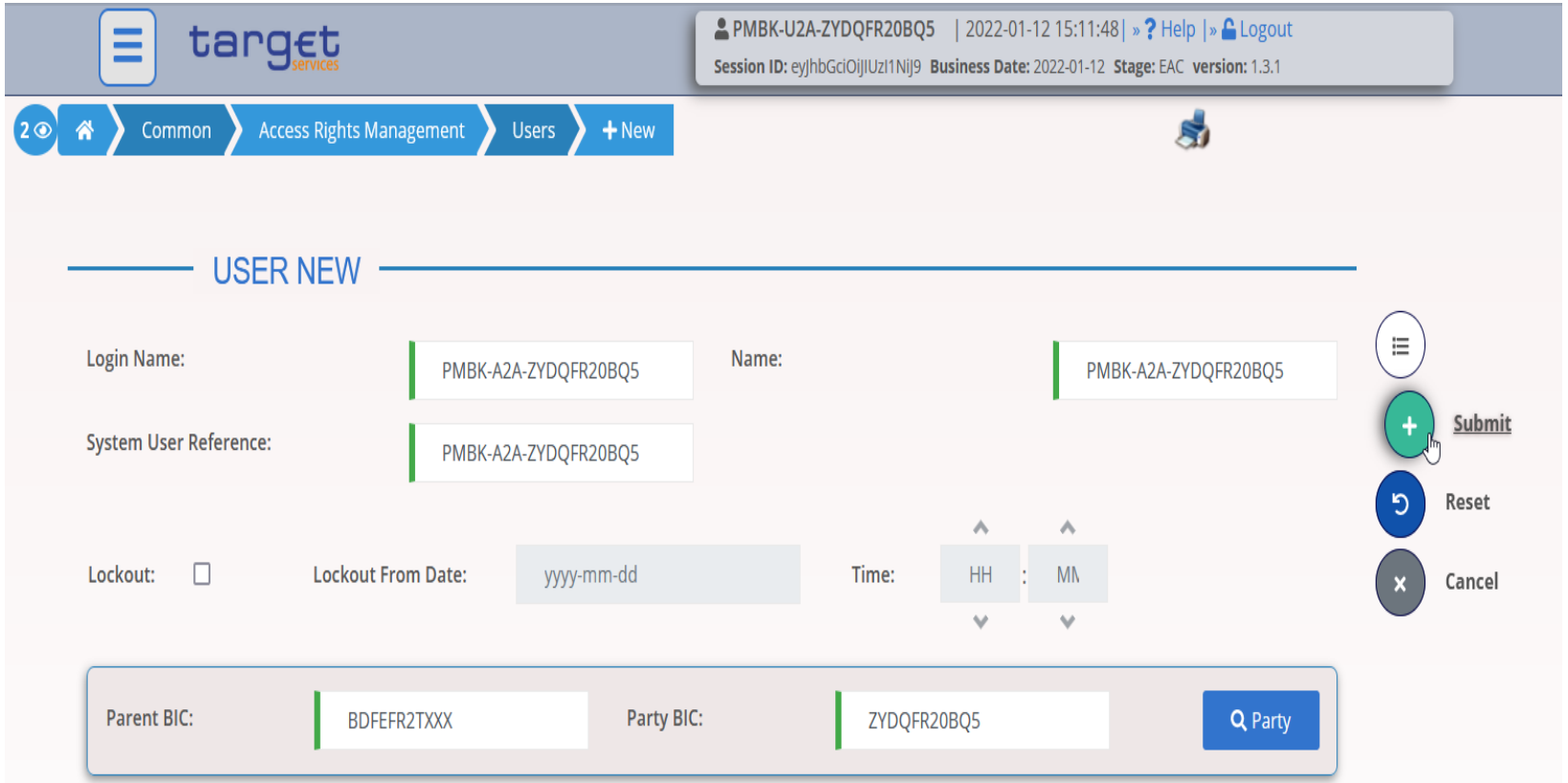
Procédure concernant l'utilisation et le paramétrage du user A2A

Comment créer un User A2A dans CRDM ?

Rentrez vos informations et cliquez sur submit, votre User A2A est maintenant créé.

Recommandation:

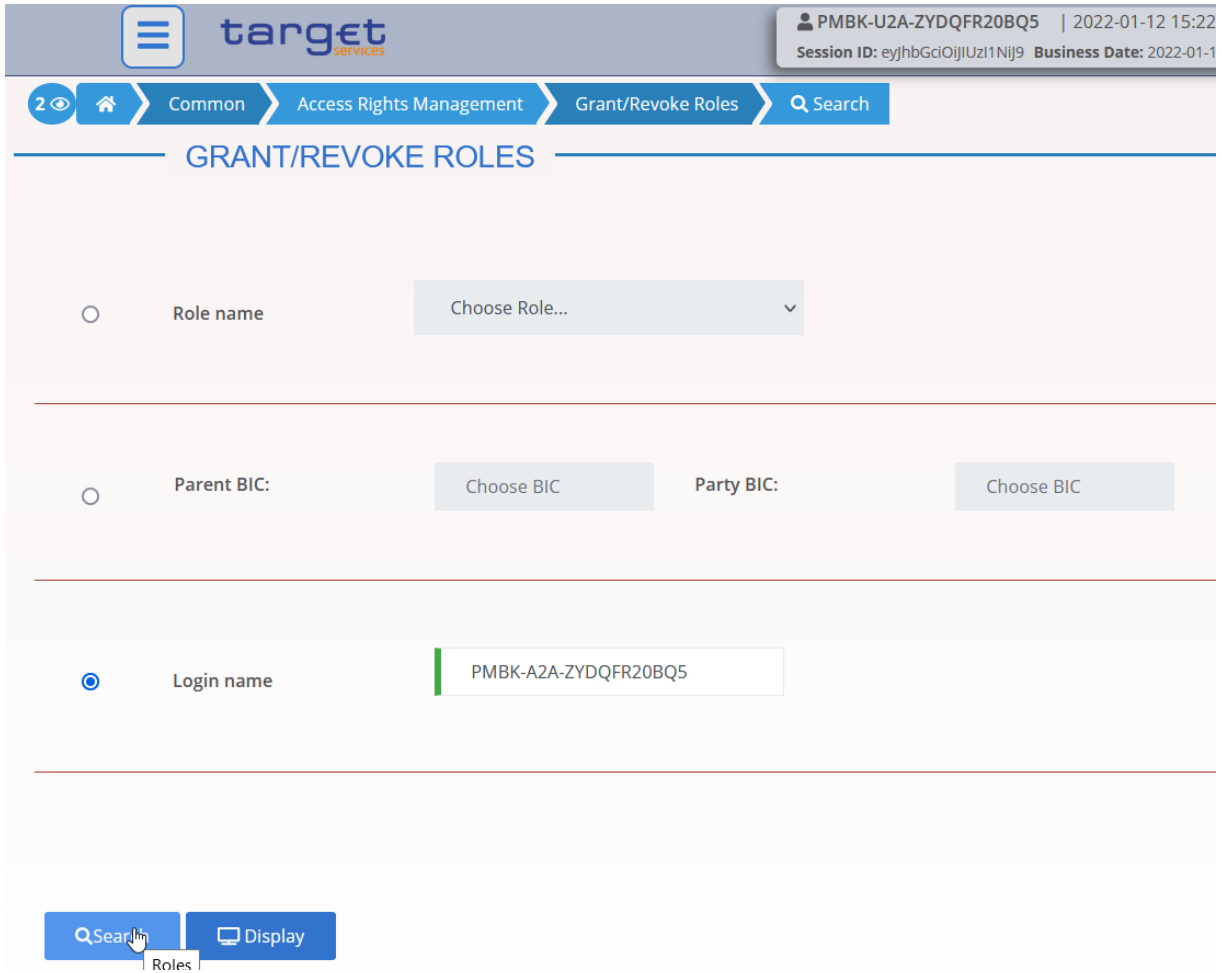
- Utiliser la même valeur pour '*login name*' et '*system user reference*'
- Utiliser la nomenclature « UserA2A-<partyBIC(11c)> -<suffixe(facultatif)>»



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment accorder des rôles à son un User A2A dans CRDM ?

Sélectionnez Login Name et indiquez le Login Name de votre User A2A puis cliquez sur Search

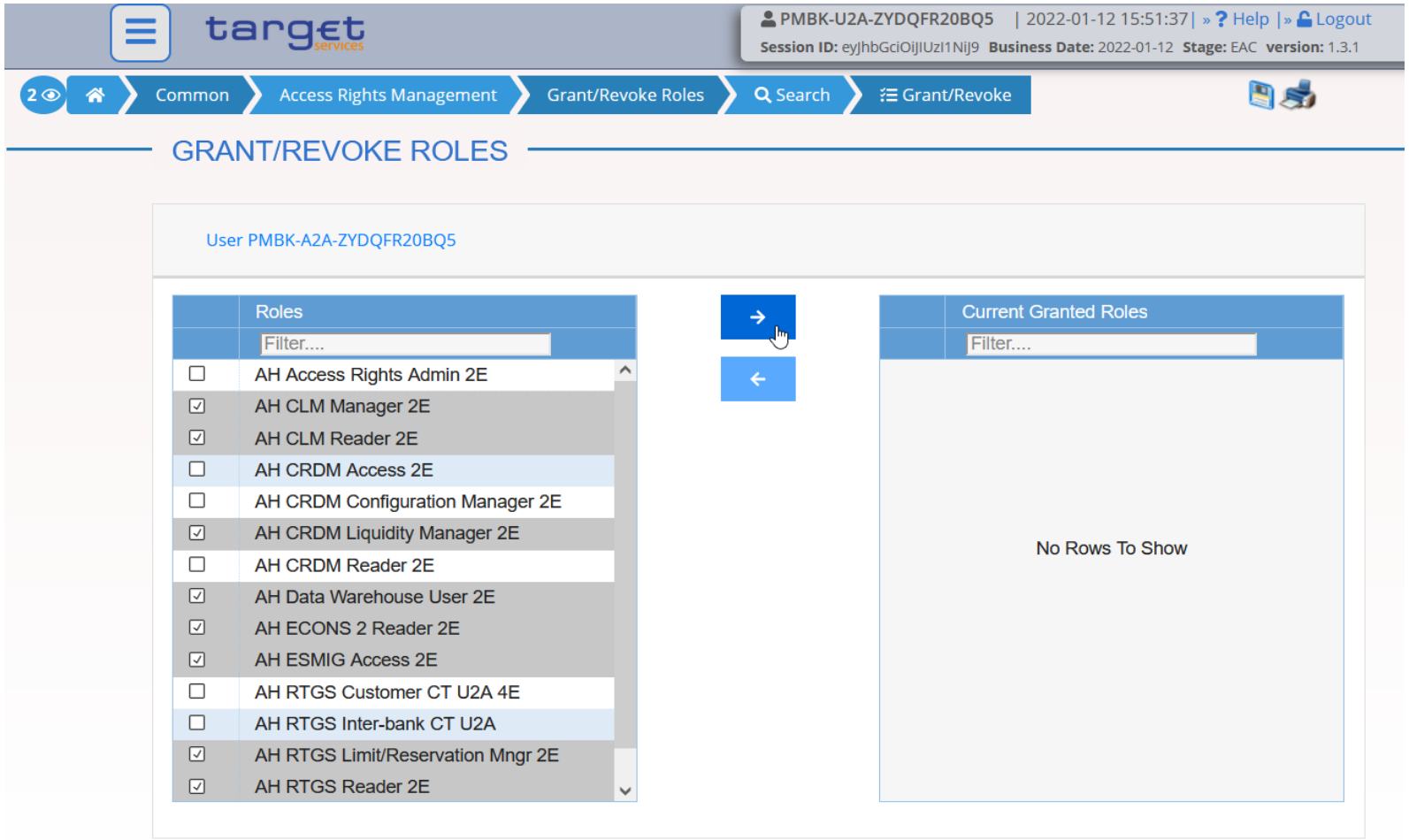


Attention : On accorde des rôles au User qui contiennent des privilèges. Il ne faut pas accorder directement de privilège à votre User. Cela créerait des conflits vous empêchant d'accorder les rôles contenant ces privilèges.

Procédure concernant l'utilisation et le paramétrage du user A2A

Comment accorder des rôles à son un User A2A dans CRDM ?

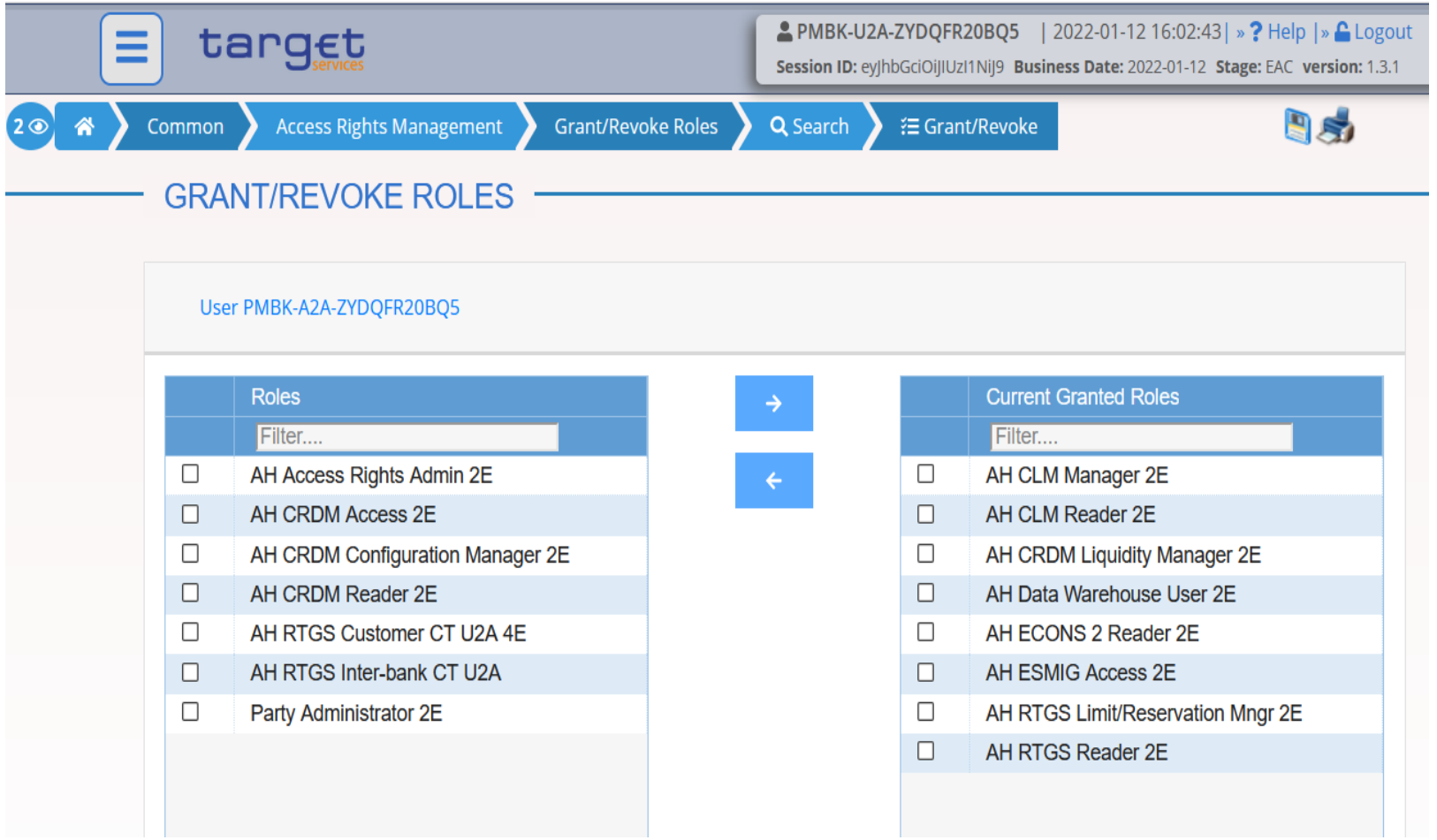
Sélectionnez les rôles souhaitez et cliquez sur la flèche du haut pour les transférer à votre user.



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment accorder des rôles à son un User A2A dans CRDM ?

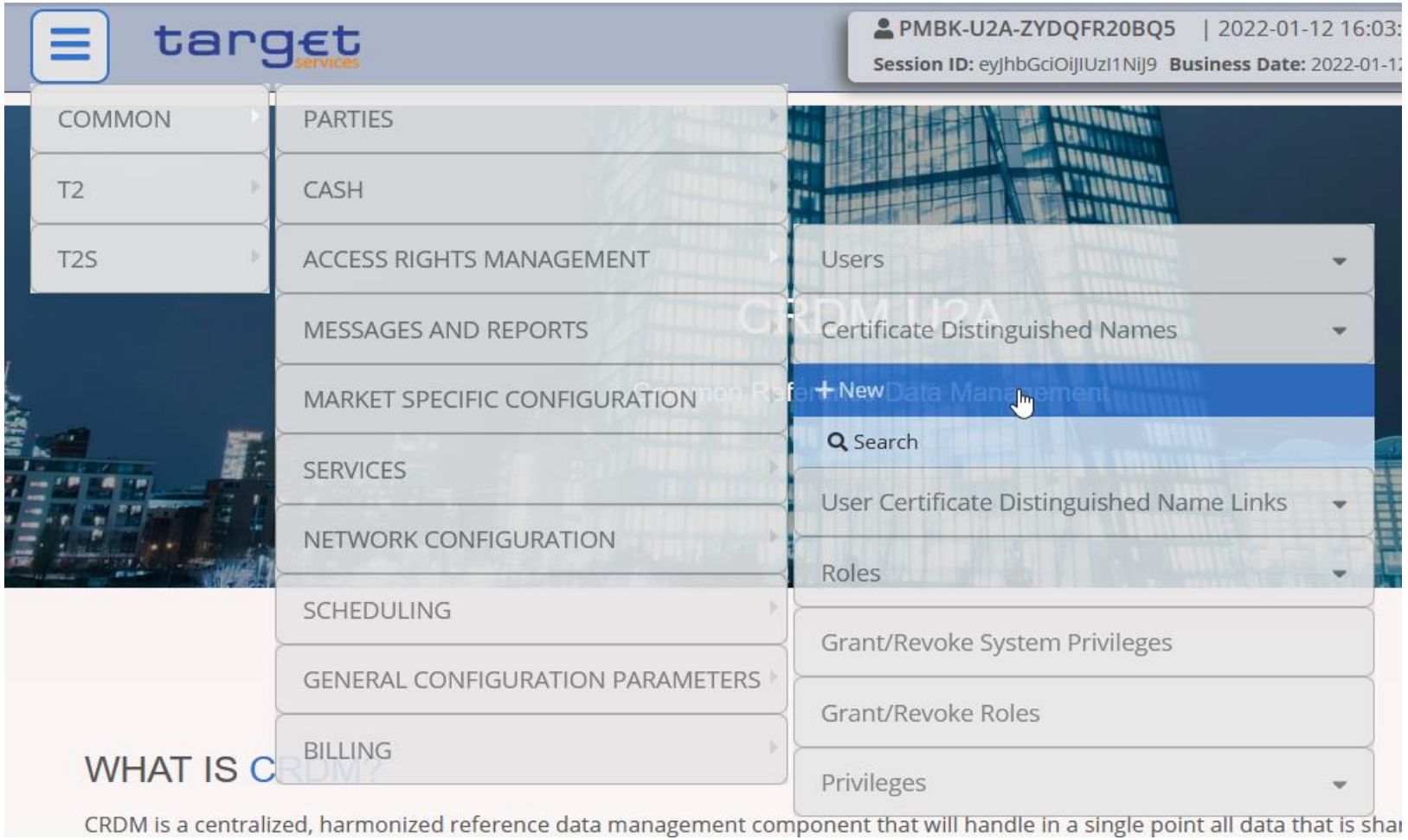
Les rôles choisis sont maintenant attribués à votre user A2A.



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

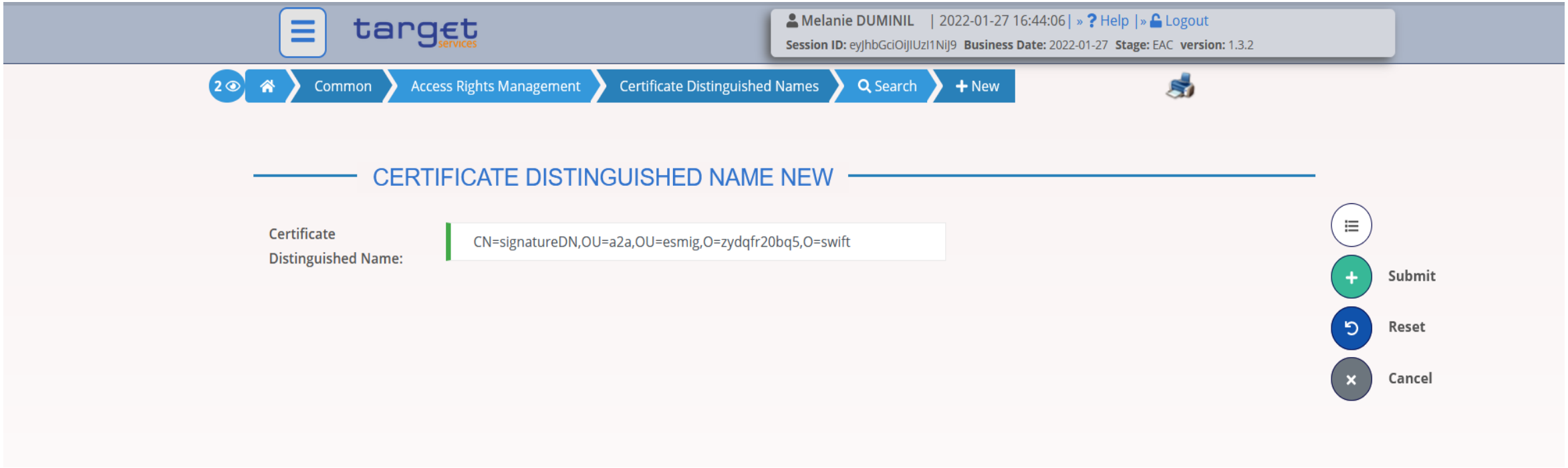
Enregistrez votre Signature DN et votre PTA en allant dans COMMON > ACCESS RIGHTS MANAGEMENT > Certificate Dinstinguished Names > New



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

Rentrez votre Signature DN puis cliquez sur Submit. Puis répétez la même action pour le PTA (qui doit être différent de votre signature DN).

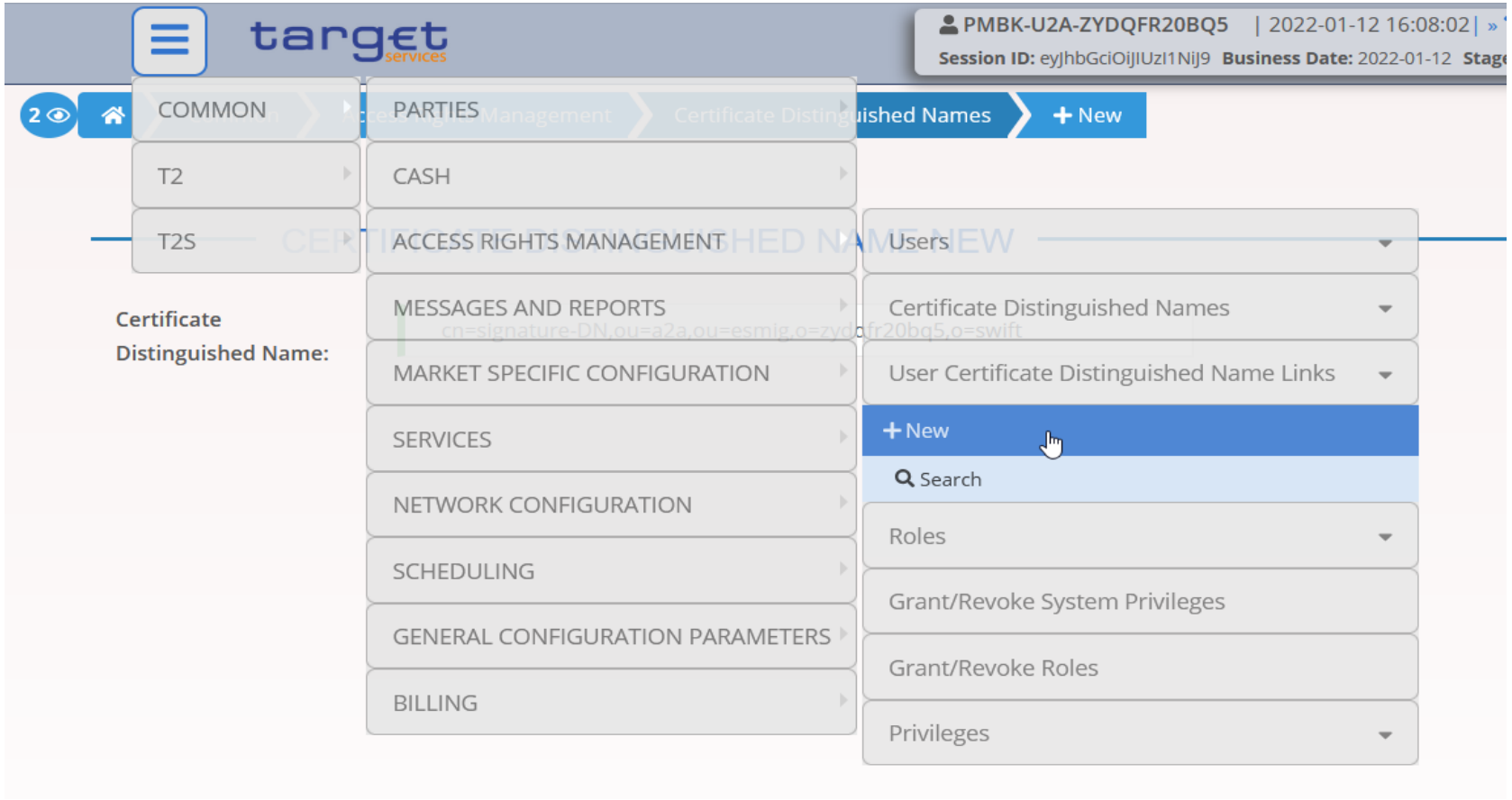


Attention : Il faut enregistrer le **PTA en minuscule sans espace** : cn=pta,ou=a2a,ou=esmig,o=zydqfr20bq5,o=swift
Il faut enregistrer le **Signature DN en majuscule sans espace** : CN=signatureDN,OU=a2a,OU=esmig,O=zydqfr20bq5,O=swift

Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

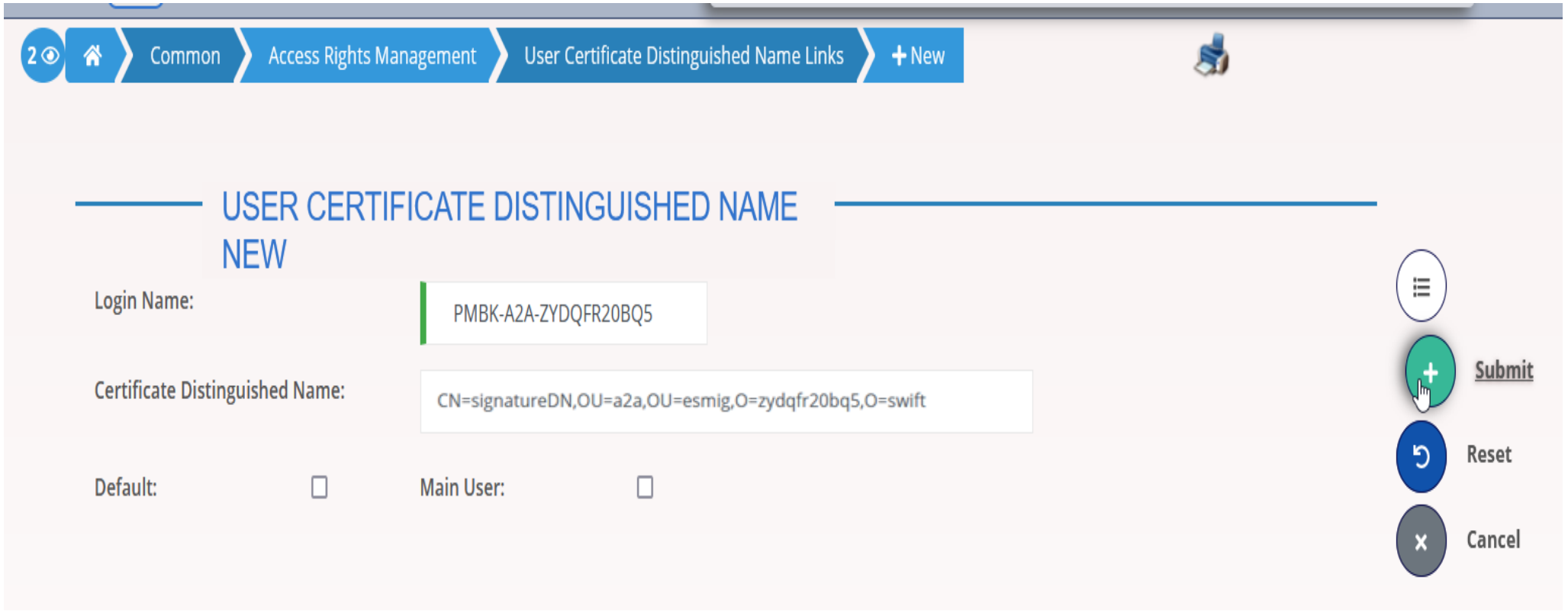
Liez votre Signature DN et PTA à votre User A2A en allant dans COMMON > ACCESS RIGHTS MANAGEMENT > User Certificate Dinstinguished Names Links > New



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

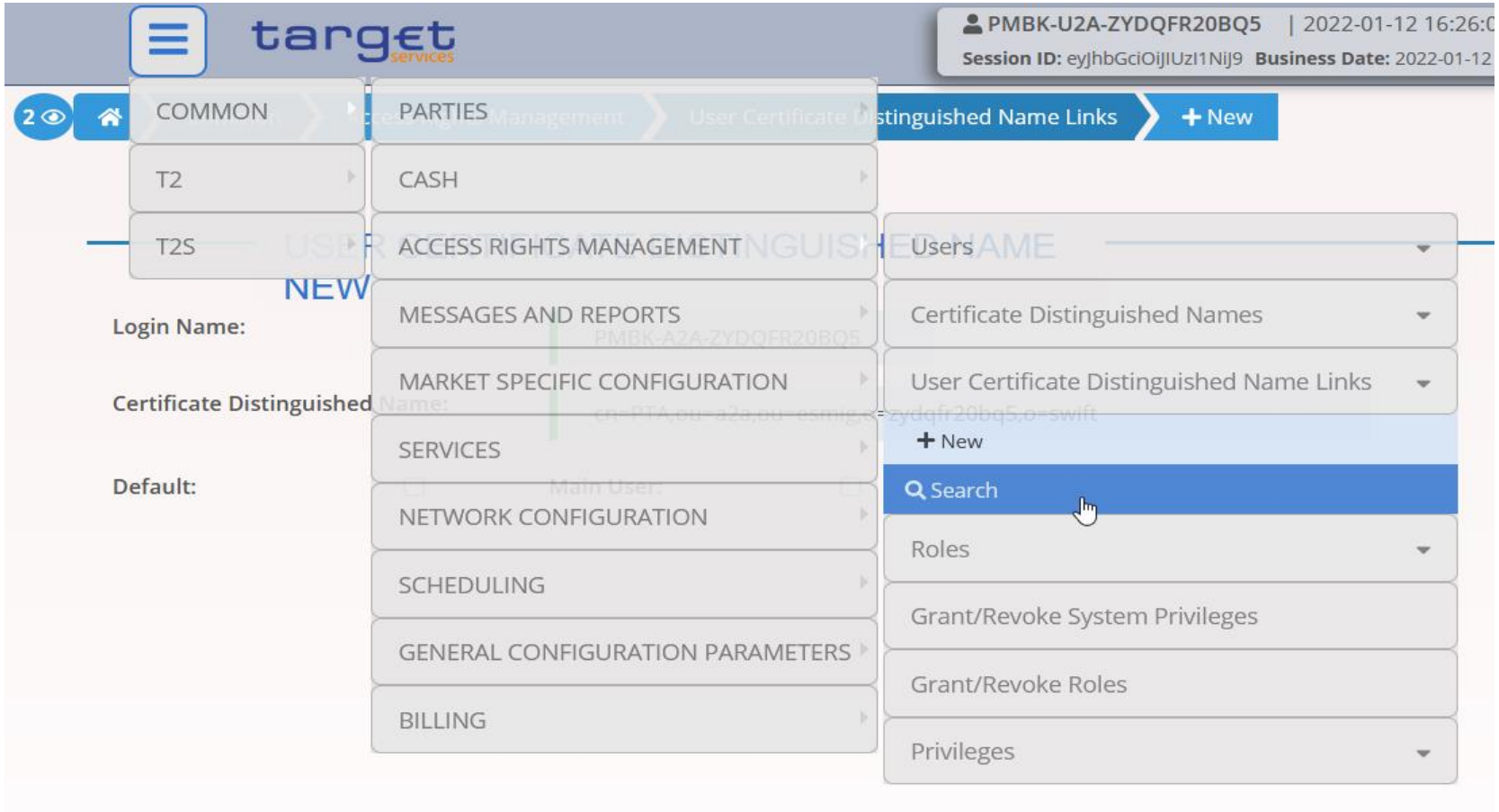
Entrez le Login Name de votre User A2A, puis votre Signature DN, puis cliquez sur Submit.
Puis répétez la même action pour le PTA.



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

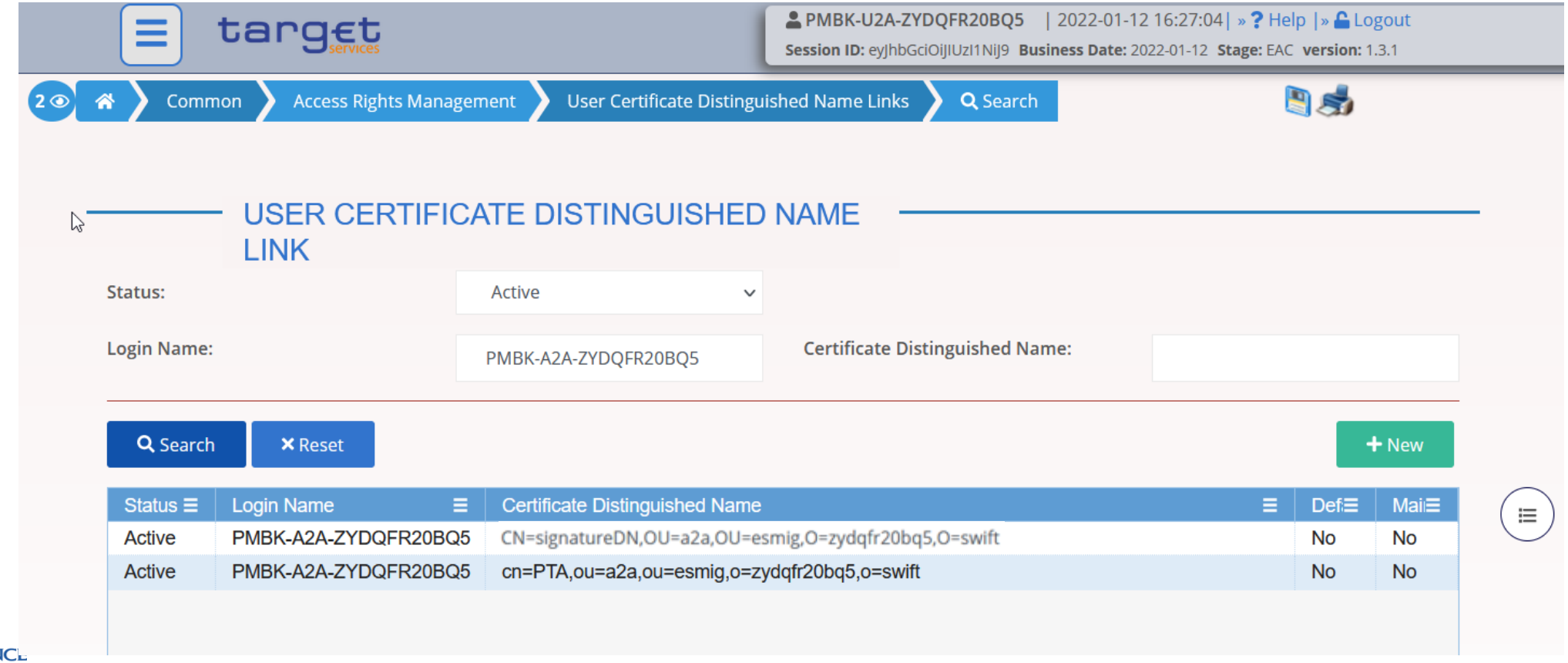
Pour vérifier quel PTA/Signature DN sont liés à votre User A2A, allez dans COMMON > ACCESS RIGHTS MANAGEMENT > Use Certificate Distinguished Name > Search



Procédure concernant l'utilisation et le paramétrage du user A2A

Comment lier son PTA et Signature DN à son un User A2A dans CRDM ?

Rentrez le Login Name de votre User A2A puis cliquez sur Search.
Les PTA/Signature DN liés au User A2A s'affichent.



Procédure concernant l'utilisation et le paramétrage du user A2A

Votre User A2A est maintenant prêt à être utilisé.