

Service de restriction d'accès à l'ESAA dans le cadre des incidents VDCP

Expression de besoin

Auteur(s) : Quentin Viale
Type de document : Expression de besoin
Référence : Néant
Date de dernière mise à jour : 15/11/2024

Historique des versions

Version	Date	Auteurs	Modification
V2	15/11/2024	Q. Viale	Création du document

Documents de références :

Table des matières

1	Fiche d'identification projet.....	2
1.1	Glossaire.....	2
1.2	Contexte.....	2
1.3	Besoin	3
2	Introduction	3
2.1	Situation actuelle	3
2.2	Périmètre	3
3	Description du besoin.....	3
3.1	Résumé.....	3
3.2	Service de restriction d'accès	4
3.3	Utilisateur bloqué.....	Error! Bookmark not defined.

1 FICHE D'IDENTIFICATION PROJET

1.1 Glossaire

- ESAA : Espace Sécurisé Agirc-Arrco. Site internet permettant aux affiliés Agirc-Arrco d'obtenir des informations personnalisées
- Private office : Interface administrateur et gestionnaire du portail ESAA. Le private office propose de nombreux services afin de pouvoir travailler sur les dossiers des individus (vision miroir, visionneuse GED) ainsi que des outils permettant d'administrer le portail (CMS, activation/désactivation de service)
- LDAP : Annuaire des comptes inscrits sur le portail ESAA. Un compte = une entrée sur le LDAP.
- VDCP : Violation de Données à Caractère Privée

1.2 Contexte

Lorsqu'un incident VDCP est ouvert, nous sommes tenus d'être très réactifs. La durée de prise en charge d'un tel incident (en ce qui concerne l'ESAA) correspond à la durée entre l'ouverture de l'incident et le blocage de l'accès au portail ESAA pour les utilisateurs concernés. Il ne s'agit pas de la seule action mais celle-ci est l'action prioritaire qui permet par la suite de faire les nettoyages et corrections avec plus de sérénité.

1.3 Besoin

La présente EB décrit la mise en place d'un service dédié à la restriction de l'accès au portail pour une liste d'utilisateurs.

Cette restriction pourra être réalisée via le private office par les administrateurs. Elle sera immédiate et révocable.

De plus, la liste des utilisateurs avec accès sera disponible.

2 INTRODUCTION

2.1 Situation actuelle

Actuellement, lorsque nous devons bloquer l'accès à l'ESAA à un ou plusieurs utilisateurs, ne disposant pas de fonctionnalité dédiée à cela, nous réalisons un script de mise à jour SQL dans la table `fidt_ind` en plaçant le code certifié à N (non certifié). Le portail n'étant pas accessible aux non certifiés, le blocage est effectif.

En revanche, cette méthode présente plusieurs inconvénients :

- La durée d'exécution (réception incident, recherche et création SQL, création DU, exécution en prod par une équipe dédiée)
- Cette manipulation n'est pas définitive et peut être annulée sans que l'on fasse de script de déblocage : en cas de réception de données de mise à jour de l'individu via le batch individu (HWRC02Q).

2.2 Périmètre

Le service permettant de bloquer l'accès au portail ESAA à un utilisateur (et de le rétablir) doit être proposé via le private office aux administrateurs et à la MOA.

Le blocage d'accès concerne tout individu éligible au portail ESAA, qu'il dispose d'un compte ou pas, quel que soit le mode de connexion.

3 DESCRIPTION DU BESOIN

3.1 Résumé

L'objectif de cette évolution est de proposer un outil sur le private office permettant de bloquer l'accès à l'ESAA instantanément à un utilisateur ou à une liste d'utilisateur, qu'il(s) dispose(nt) déjà d'un compte ou pas encore. Cet outil permettra également de visualiser la liste des utilisateurs dont l'accès au portail est bloqué, de les débloquent tous ou un sous-ensemble.

Concernant l'internaute qui disposerait d'un accès bloqué, la méthode de restriction d'accès doit être identique dans le fonctionnement à celle empêchant les non certifiés d'accéder au portail. **(Hors périmètre de cette EB, déjà pris en compte dans deco loca. A ce sujet, la table de blocage existe déjà, `t_tra_userblock`. En revanche, il sera nécessaire de lui ajouter une nouvelle colonne, celle des Ref. ITOP. On le verra dans le paragraphe dédié).**

3.2 Service de restriction d'accès

3.2.1 Périmètre

Le service de restriction d'accès doit être proposé aux profils suivants uniquement :

- 203 : Administrateur (rôle ADMIN)
- 204 : Administrateur VIP (rôle ADMIN_VIP)

Il n'y a aucune recommandation sur la couleur de la tuile, le picto de la tuile ainsi que sa position par profil, le choix est libre.

Il y a en revanche une contrainte sur le nom du service qui ne doit pas faire mention des termes « blocage » et « déblocage » car un service de déblocage de compte existe déjà et ne correspond pas du tout à ce que l'on met en place via cette EB (et je pense même qu'il est plus que déconseillé de l'utiliser étant donné notre volume de comptes. Une demande est en cours pour pouvoir le désactiver).

3.2.2 Présentation générale du service de restriction d'accès

Le service doit permettre trois actions principales :

- Soumettre une liste de NSS pour restriction
- Soumettre une liste de NSS pour lever la restriction
- Réaliser l'export de la table de blocage

Enfin, le service doit permettre de consulter le contenu de la table de blocage en direct.

Le fil d'Ariane est également proposé en position habituelle et permet de retourner sur la grille des services du private office.

3.2.3 Aspect général du service au chargement

Le service de présente de la sorte :

Accueil / Restrictions

Ajouter des restrictions Supprimer des restrictions Exporter

Num SS	Date restriction	Ref. ITOP	Dern. connexion
1880706083027	15/11/2024	R123321	
1900807077034	13/10/2023	R451238	10/10/2023
2420608937658	25/07/2022	R789546	
2610806083027	29/11/2024	R123456	25/11/2024
1730213893458	29/11/2024	R123456	12/07/2020
2891106083045	30/11/2024	R123456	

« < 1 2 3 > » Nb. lignes 10 ▼

On distingue 4 zones principales :

- Le bouton d'ajout de restriction
- Le bouton de suppression de restriction
- Le bouton d'export de la table de blocage
- Le tableau des blocages actuels

Chacune de ces zones va être décrite au sein d'un chapitre dédié.

NB : Il ne faut pas oublier le fil d'ariane qui permet de retourner sur la grille des tuiles du private office.

3.2.4 Tableau des blocages actuels

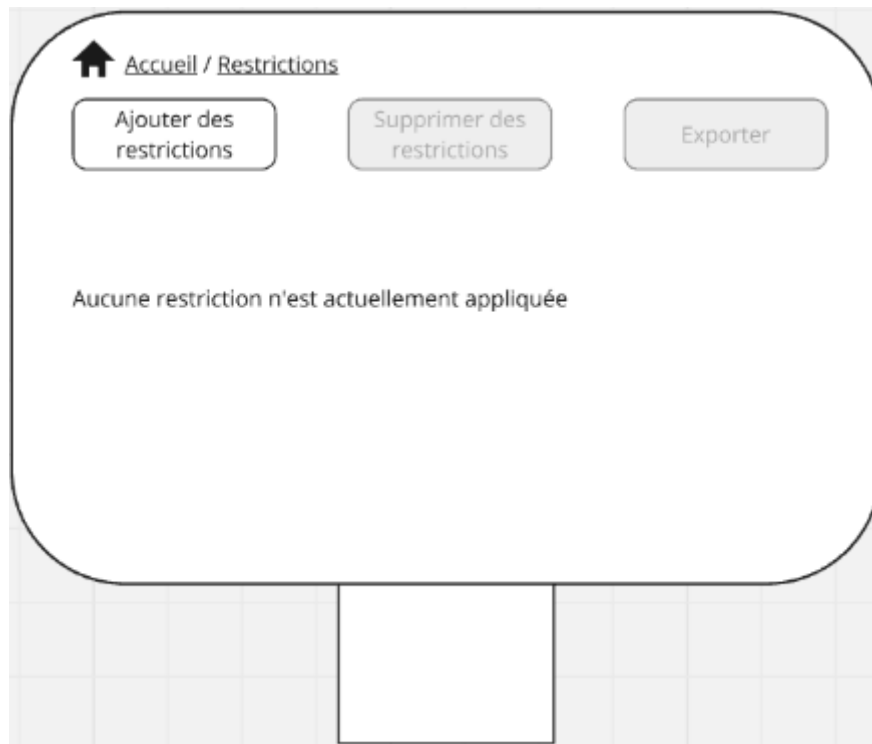
Par défaut, lors du chargement de la page, les données sont affichées non filtrées, triées par numéro de sécurité sociale, avec un tableau contenant 10 lignes par page.

La plupart des données sont issues de la table de blocage (Num SS, Date restriction, Ref. ITOP).

En revanche la date de dernière connexion provient du ldap. Il faudra donc accéder, pour chaque Num SS affiché, à son compte LDAP s'il existe. S'il n'existe pas, on laissera la cellule vide.

Attention, la consommation du LDAP pouvant poser des problèmes de performance côté ESAA, il faudra prévoir un paramètre qui permettra de désactiver l'appel à celui-ci. Si l'appel est désactivé, la colonne « Dern. Connexion » sera toujours vide.

Si aucune donnée n'est disponible en base, alors le tableau et la zone de pagination ne sont pas affichés. Un message est affiché à la place : « Aucune restriction n'est actuellement appliquée. »



Si en revanche des données sont disponibles, alors on les affiche, dans la limite de la pagination proposée.

En ce qui concerne la pagination, on propose par défaut 10 lignes par page mais on peut modifier cette valeur avec 20 ou 50. Bien évidemment, le contenu de cette liste (10, 20, 50) doit s'adapter en fonction du nombre total de lignes que restitue le service (par exemple si moins de 10 lignes, pas besoin de proposer les valeurs 20 ou 50).

Toujours au sujet de la pagination, on ne proposera que 3 pages à l'affichage dans la liste :



Et cette liste s'adaptera à la page courante (par exemple si on est page 7 et qu'il n'y a plus qu'une page après, on affiche : ... 6 7 8. En revanche si on est page 7 et qu'il reste encore 3 pages, on affichera : ... 6 7 8).

Enfin, au niveau du tableau, des filtres peuvent être appliqués sur les colonnes Num SS et Ref. Itop.

Si le résultat du filtrage est une liste vide, il faut afficher le tableau avec uniquement les entêtes (pour permettre de changer les filtres).

Le filtre déclenche un nouvel appel au service qui restitue la liste des lignes et cela impacte donc l'affichage de la pagination.

3.2.5 Bouton d'export de la table des blocages

Le bouton d'export permet de déclencher le téléchargement du contenu de la table de blocage au format CSV (avec en tête).

Attention, si la table est vide, le bouton est grisé et le service d'export ne peut pas être appelé.

3.2.6 Bouton d'ajout de restriction

Le clic sur le bouton d'ajout de restriction déclenche l'ouverture d'une popin :



Le clic sur le bouton importe déclenche l'ouverture d'un explorateur de fichier permettant de sélectionner le fichier à uploader.

Une fois le fichier sélectionné, l'appel au service REST d'ajout de restriction est déclenché.

A propos de ce service, il doit tout d'abord faire des contrôles sur le fichier :

- Il ne peut pas être null
- Il ne peut pas être vide
- Il est obligatoirement au format CSV

- Il ne contient pas d'en tête.
- La première colonne est obligatoire et contient les NSS
- Il n'y a que deux colonnes maximums. La seconde colonne est optionnelle et contient la référence de l'ITOP ayant conduit au blocage de l'individu

Si au moins un des contrôles est KO, cela génère un rejet du service. Le comportement de l'ihm en cas de rejet va être décrit plus bas.

Si aucun contrôle n'est levé, alors le fichier est valide et il peut être traité.

Chaque ligne du fichier doit subir une phase de contrôle supplémentaire :

- L'individu existe-t-il dans le référentiel individu ?
- L'individu n'existe pas dans la table de blocage.

Si la réponse aux deux contrôles est OUI, alors on peut insérer l'individu dans la table de blocage.

Sinon, la ligne est en rejet. On tente de traiter les autres lignes du fichier.

Trois scénarios sont alors possibles :

- A°) Le fichier est en rejet ou toutes les lignes du fichier sont en rejets.
- B°) Le fichier n'est pas en rejet mais au moins une ligne du fichier est rejetée (et au moins une ligne du fichier est intégrée).
- C°) Le fichier n'est pas en rejet et toutes les lignes du fichier sont traitées.

Si on est dans la situation A, l'IHM se comporte de la manière suivante :

Accueil / Restrictions

Ajouter des restrictions Supprimer des restrictions Exporter

Num SS	Date restriction	Ref. ITOP	Dern. connexion
188070608302			
190080707703			10/2023
242060893765			
2610806083027	29/11/2024	R123456	25/11/2024
1730213893458	29/11/2024	R123456	12/07/2020
2891106083045	30/11/2024	R123456	

Navigation: << < 1 2 3 > >> Nb. lignes: 10 ▼

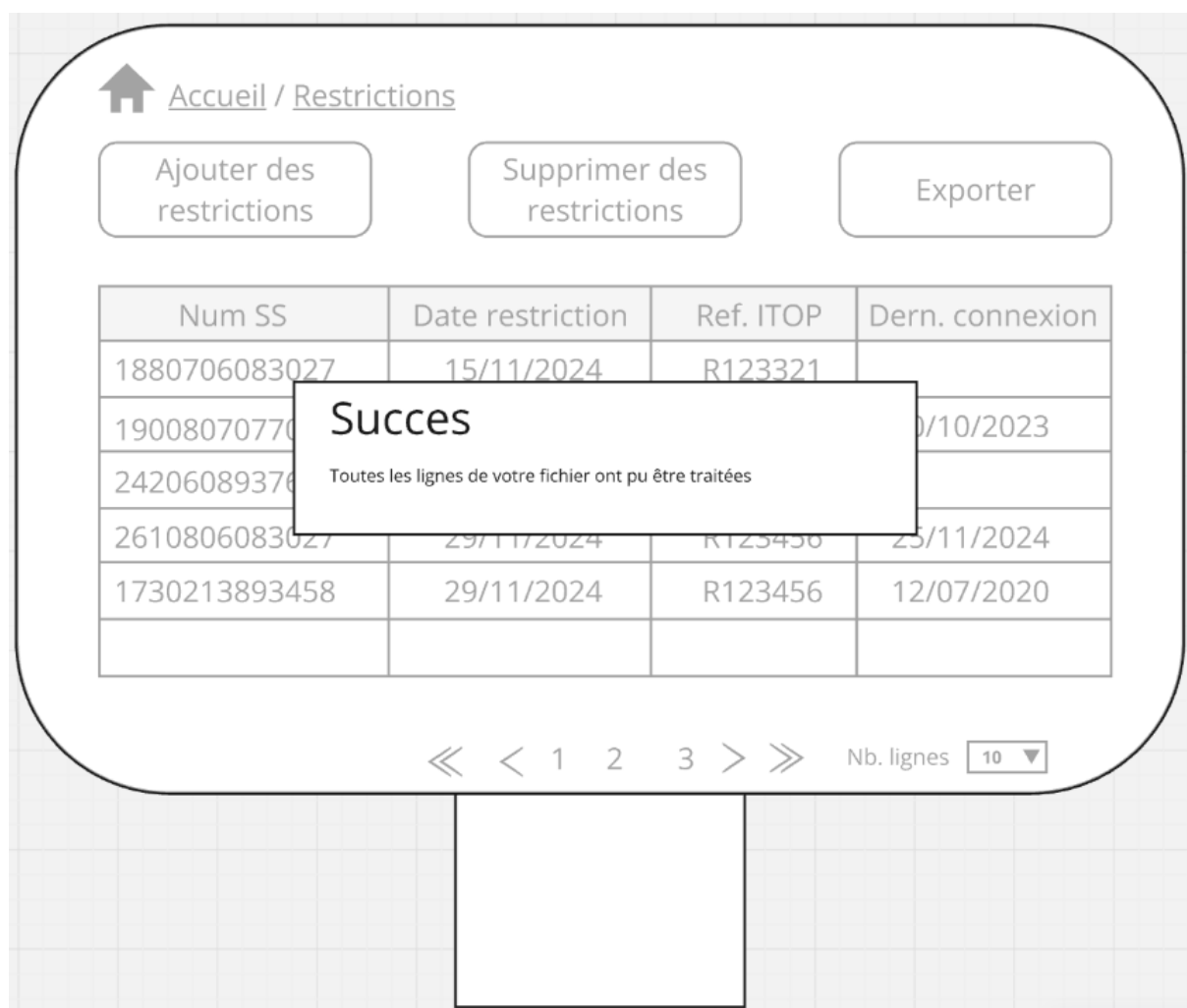
Si on est dans la situation B, l'IHM se comporte de la manière suivante :

The screenshot shows a web interface titled 'Accueil / Restrictions'. It features three buttons: 'Ajouter des restrictions', 'Supprimer des restrictions', and 'Exporter'. Below these is a table with four columns: 'Num SS', 'Date restriction', 'Ref. ITOP', and 'Dern. connexion'. A success message box is overlaid on the table, stating: 'Succes', 'Sur N lignes contenues dans votre fichier, X ont été prises en compte.', and 'Pour plus de détail, téléchargez la liste des lignes en rejet [ici](#).' The table contains several rows of data, with the last row being: 2891106083045, 30/11/2024, R123456, and an empty date field. At the bottom of the interface, there are navigation arrows and a 'Nb. lignes' dropdown menu set to 10.

Num SS	Date restriction	Ref. ITOP	Dern. connexion
18807060830			
19008070770			0/10/2023
24206089376			
26108060830			5/11/2024
17302138934			2/07/2020
2891106083045	30/11/2024	R123456	

Le clic sur le lien permet de télécharger un fichier CSV de rejet. La première colonne contient le NSS en rejet, la seconde colonne contient le motif du rejet (« nss déjà présent dans la table » ou « individu inconnu du référentiel »).

Si on est dans la situation C, l'IHM se comporte de la manière suivante :



Que la mise à jour soit totale (cas C) ou partielle (cas B), elle doit déclencher un rafraichissement des données du tableau.

3.2.7 Bouton de suppression de restriction

Le clic sur le bouton de suppression n'est possible que si la table de blocage contient au moins une ligne.

Le clic sur le bouton de suppression de restriction déclenche l'ouverture d'une popin :

Accueil / Restrictions

Ajouter des restrictions Supprimer des restrictions Exporter

Suppression de restriction

Merci de bien vouloir uploader un fichier csv (sans entête) contenant la liste des NSS pour lesquels vous souhaitez lever la restriction.

Attention : si certains d'entre eux sont absent de la table de blocage, ils seront en rejets.

Importer

Num SS	Date de connexion	R123456
188070608302		
190080707703	10/2023	
242060893765		
261080608302	11/2024	
173021389345	07/2020	
2891106083045	30/11/2024	R123456

Nb. lignes 10 ▼

Le clic sur le bouton importe déclenche l'ouverture d'un explorateur de fichier permettant de sélectionner le fichier à uploader.

Une fois le fichier sélectionné, l'appel au service REST d'ajout de restriction est déclenché.

A propos de ce service, il doit tout d'abord faire des contrôles sur le fichier :

- Il ne peut pas être null
- Il ne peut pas être vide
- Il est obligatoirement au format CSV
- Il ne contient pas d'en tête.
- La première colonne est obligatoire et contient les NSS
- Il n'y a qu'une seule colonne maximum.

Si au moins un des contrôles est KO, cela génère un rejet du service. Le comportement de l'ihm en cas de rejet va être décrit plus bas.

Si aucun contrôle n'est levé, alors le fichier est valide et il peut être traité.

Chaque ligne du fichier doit subir une phase de contrôle supplémentaire :

- L'individu existe-t-il dans la table de blocage ?

Si la réponse au contrôle est OUI, alors on peut supprimer l'individu de la table de blocage.
Sinon, la ligne est en rejet. On tente de traiter les autres lignes du fichier.

Trois scénarios sont alors possibles :


- A°) Le fichier est en rejet ou toutes les lignes du fichier sont en rejets.
- B°) Le fichier n'est pas en rejet mais au moins une ligne du fichier est rejetée (et au moins une ligne du fichier est traitée).
- C°) Le fichier n'est pas en rejet et toutes les lignes du fichier sont traitées.

Si on est dans la situation A, l'IHM se comporte de la manière suivante :

The screenshot shows a web interface titled 'Accueil / Restrictions'. It features three buttons: 'Ajouter des restrictions', 'Supprimer des restrictions', and 'Exporter'. Below these is a table with four columns: 'Num SS', 'Date restriction', 'Ref. ITOP', and 'Dern. connexion'. The table contains six rows of data. An error dialog box is overlaid on the table, displaying the text 'Error' and 'Aucune des lignes de votre fichier n'a pu être traitée.' Below the table, there are navigation arrows and a 'Nb. lignes' dropdown menu set to '10'.

Num SS	Date restriction	Ref. ITOP	Dern. connexion
188070608302			
190080707703			10/2023
242060893765			
2610806083027	29/11/2024	R123456	25/11/2024
1730213893458	29/11/2024	R123456	12/07/2020
2891106083045	30/11/2024	R123456	

Si on est dans la situation B, l'IHM se comporte de la manière suivante :


[Accueil / Restrictions](#)

Ajouter des restrictions

Supprimer des restrictions

Exporter

Num SS	Date restriction	Ref. ITOP	Dern. connexion
18807060830			
19008070770			0/10/2023
24206089376			
26108060830			5/11/2024
17302138934			2/07/2020
2891106083045	30/11/2024	R123456	

Succes

Sur N lignes contenues dans votre fichier, X ont été prises en compte.

 Pour plus de détail, téléchargez la liste des lignes en rejet [ici](#).

<<

<

1

2

3

>

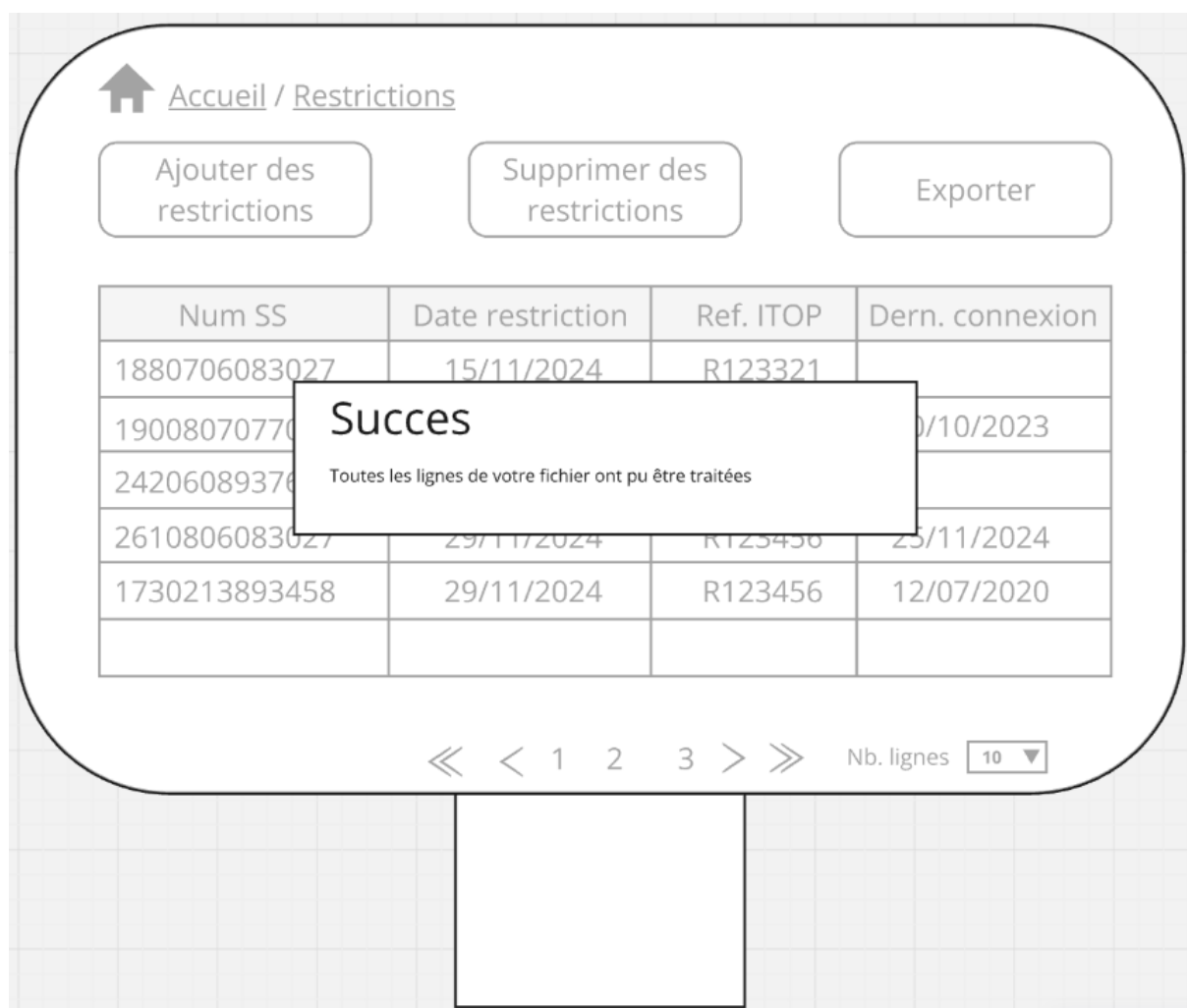
>>

Nb. lignes

10 ▾

Le clic sur le lien permet de télécharger un fichier CSV de rejet. La première colonne contient le NSS en rejet, la seconde colonne contient le motif du rejet (« nss absent de la table »).

Si on est dans la situation C, l'IHM se comporte de la manière suivante :



Que la mise à jour soit totale (cas C) ou partielle (cas B), elle doit déclencher un rafraichissement des données du tableau.

4 ANNEXES

La board miro suivante résume le comportement du service dans les grandes lignes : https://miro.com/app/board/uXjVLE4zoBo=