Mandats et contrôle d'accès – Règles générales

1. User Management

1. Celui qui n'est pas repris dans le User Management de la Sécurité Sociale (UMAN), ne peut poser aucun acte dans le cadre de Base de données Pensions Complémentaires.

2. Le UMAN fonctionne uniquement AU SEIN D'UNE SEULE ENTITE. Toutes les compétences, applications, fonctions et rôles du UMAN se situent au sein de cette entité.

<table>
<tr><td colspan="7">Entité</td></tr>
<tr><td colspan="7">Responsable juridique de l'entité</td></tr>
<tr><td colspan="7">RAE
pour toute l'entité (1 par entité)</td></tr>
<tr><td colspan="2">Gestionnaire local (GL)
d'une compétence spécifique (max.1)</td><td colspan="5">GL'Gestion Pensions Complémentaires' (1)</td></tr>
<tr><td>Application 1</td><td>Application n</td><td>DB2 Pre-Load</td><td colspan="2">DB2P Simulation</td><td colspan="2">DB2P Production</td></tr>
<tr><td>1 ou plusieurs rôles</td><td>1 ou plusieurs rôles</td><td>Utilisateur</td><td>Utilisateur</td><td>Gestion Mandats & Accès</td><td>Utilisateur</td><td>Gestion Mandats & Accès</td></tr>
<tr><td>Utilisateur *
(n)</td><td>Utilisateur *
(n)</td><td>Utilisateur */***
(n)</td><td colspan="2">Utilisateur *
(n)</td><td colspan="2">Utilisateur *
(n)</td></tr>
<tr><td colspan="2">Utilisateur technique (max.1) **</td><td colspan="5">Utilisateur technique (max.1) **</td></tr>
</table>

* Le Gestionnaire Local donne à chaque Utilisateur un ou plusieurs rôles pour une application bien définie au sein de la compétence.

** Il n'y a qu'un seul Utilisateur Technique par compétence. Si pour chaque application d'une compétence un Utilisateur Technique doit être désigné, il s'agira dès lors toujours du même Utilisateur Technique. Un Utilisateur Technique aura aussi toujours les rôles d'une application.

*** Vu que le Pre-Load ne peut être exécuté qu'en batch (par l'Utilisateur Technique), cela n'a aucun sens de désigner des Utilisateurs pour cette application.

3. La gestion des mandats et le contrôle d'accès (voir plus loin) n'a aucun lien avec ceci.
La gestion des mandats joue entre Entités (qui peuvent éventuellement chacune être reprise de manière séparée dans le UMAN) et non au sein du UMAN d'une seule Entité.
Le contrôle d'accès permet de paramétrer des critères en termes de droit d'utilisation au sein du groupe d'Utilisateurs d'une application bien déterminée d'une compétence, au sein d'une Entité bien définie.

Les **mandats** portent sur les relations entre les Entités.
Ceci n'a aucun lien avec le Uman.

Dans le **UMan**, on reste toujours au sein de l'Entité. Le UMan ne règle pas la relation entre entités.	Organisateur	Organisme de pension	Prestataire de services
	RAE	RAE	RAE
	Gestionnaire local	Gestionnaire local	Gestionnaire local
	Utilisateur	Utilisateur	Utilisateur
Le **Contrôle d'accès** n'a rien à voir avec le UMan, mais porte toujours sur les Utilisateurs d'une Entité.			

4. Il n'est par conséquent pas possible pour une Entité A de désigner un Utilisateur d'une autre Entité B comme étant Utilisateur de cette Entité B.

5. Il est – uniquement dans le cadre de DB2P – bel et bien possible pour l'Entité A de désigner un employé de l'Entité B comme étant Utilisateur de l'Entité A. Dans le UMAN, cette personne agit dès lors au nom de et pour compte de A, même s'il est repris sur le payroll de B.

6. Celui qui est Utilisateur de plusieurs Entités devra, lors de la connexion, préciser à quelle Entité il se connecte de sorte que la responsabilité juridique portant sur les actions qui vont en découler pourra être clairement déterminée. De même ses possibilités d'action au sein de DB2P seront déterminées par ce choix: il n'est pas possible, en une session, de disposer de l'ensemble des possibilités que l'on a auprès des diverses Entités dont on est Utilisateur, puisqu'elles ne sont pas imputables juridiquement.

Le schéma ci-dessous illustre les points 4 et 5 pour ce qui porte sur la situation d'une Entité sans personnel, mais est également imputable en dehors. Pour résumer, ce schéma ne tient pas compte des applications et des rôles. Il est également valable uniquement pour les Utilisateurs physiques.

<table>
<tr><td>Entité</td><td>Entité A
Organisateur</td><td>Entité B
Organisme de Pension</td><td>Entité C
Prestataire de services</td></tr>
<tr><td>Représentant juridique de l'entité</td><td>ex. Administrateur délégué</td><td>ex. Président C.A.</td><td>ex. CEO</td></tr>
<tr><td>RAE</td><td>Doit faire partie de l'Entité</td><td>RAE
Doit être une personne habilitée statutairement, car il n'y a pas de personnel.</td><td></td></tr>
<tr><td>Gestionnaire local (GL)</td><td rowspan="2">Peut être 'n'importe qui'</td><td>GL de B
ex. gestionnaire/administrateur,
Membre du personnel organisateur,
Membre du personnel Prestataire de services,</td><td rowspan="2"></td></tr>
<tr><td>Utilisateur</td><td>Utilisateur de B
ex. gestionnaire/administrateur,
Membre du personnel organisateur,
Membre du personnel Prestataire de services,</td></tr>
</table>

Note : RAE, GL et Utilisateur peuvent être une seule et même personne. Dans ce cas, celles-ci doivent faire partie de l'Entité.

7. Dans le UMAN, des Utilisateurs au sein des applications DB2P (Simulation et Production) pourront avoir un ou plusieurs rôles. Les deux rôles prévus pour DB2P sont *Utilisateur général* et *Gestion Mandats et accès*. Les déclarations SetDelegation et SetAuthorization, dont il est question ci-après, sont uniquement disponibles pour le deuxième type d'Utilisateurs.

2. Mandats

1. Il est en principe interdit pour une Entité A de faire des déclarations au nom d'une Entité B. Cela n'est possible que si et dans la mesure où l'Entité B a donné un mandat à l'Entité A pour faire cela. C'est pour cette raison que l'on parle d'un **système fermé**.

2. C'est pour cela qu'un mandat doit toujours être **explicite et précis**. Aucun mandat n'est présumé, et l'étendue du mandat doit également être explicitée.

3. Pour la même raison, le mandat doit toujours avoir été donné avant que tout autre acte supposant la présence du mandat ne puisse être posé. La déclaration du mandat **précède donc toujours** les déclarations de mise en œuvre.

4. Vu que le mandat doit être explicite et précis, **une règle précise précède toujours une règle générale**. Si un conflit apparaît dans une série de règles du mandat dans une déclaration de mandat, une règle précise pour une situation bien définie aura priorité sur une règle générale.

> ex. une règle générale (c.à.d. une règle qui ne porte pas sur un nombre de dispositions bien définies, mais règle des droits en général) stipule que le mandataire peut faire des déclarations et des consultations pour toutes les dispositions du mandant, et une règle précise affirme que le mandataire ne peut pas faire de déclarations et de consultations pour une disposition bien définie ou pour une liste explicite de dispositions, la règle précise aura dès lors priorité pour cette (ces) disposition(s) lors de l'appréciation des mandats.

5. Vu que le mandat doit être explicite et précis, une déclaration des règles du mandat (SetDelegation) sera toujours bloquée lorsqu'elle contiendra deux règles générales ou précises pour la même situation.

ex. une déclaration SetDelegation contient deux règles générales du type AccountModel (c.à.d. deux règles qui toutes les deux règlent les droits en termes de déclarations de comptes).

ex. une déclaration SetDelegation contient deux règles précises du type RegulationModel pour les dispositions A, B et D.

6. On ne peut donner aucun mandat pour quelque chose que l'on ne peut faire soi-même. On ne peut pas mandater ce que l'on peut mal faire soi-même sur mandat. **On ne peut pas mandater ce qui a été mandaté**.

7. Un mandat **n'est pas exclusif**. Un mandant peut toujours agir lui-même et il peut donner un même mandat à une autre partie. Vu le point 8, cela est toutefois à plutôt déconseiller pour les mandats de Déclaration.

8. Le mandat fonctionne au niveau des déclarations, non des données en général.

ex. Un mandat de consultation uniquement pour déclarations propres (own), signifie que les déclarations faites par le mandant lui-même ou par un autre mandataire ne pourront être vues.

9. **Seule la** déclaration SetDelegation **la plus récente** est valable: une déclaration SetDelegation remplace toujours complètement la déclaration SetDelegation précédente. Une série de déclarations SetDelegation, même si elles ne sont pas en conflit l'une avec l'autre, ne fonctionne donc pas de manière cumulative. Lors d'une modification d'une règle du mandat bien précise, il faut donc toujours répéter toutes les règles du mandat en vigueur.

10. La seule manière de corriger une règle du mandat erronée est la déclaration d'une toute nouvelle SetDelegation. Vu que la déclaration SetDelegation ne peut être annulée ou corrigée, il n'y a d'ailleurs aucune anomalie non bloquante sur ces déclarations.

3. Contrôle d'accès

1. Le contrôle d'accès est valable uniquement pour les Utilisateurs physiques, non pour l'Utilisateur technique. L'Utilisateur Technique peut toujours tout faire.

2. DB2P est une banque de données officielle, non une application locale sur laquelle les déclarants peuvent faire tourner leur business proces internes. En conséquence, les accès à DB2P devraient être exceptionnels.

3. Du point de vue confidentialité, seule la notification dans le User Management est importante. Tous les accès au User Management se font sous la responsabilité du RAE de l'entité de l'Utilisateur. Le RAE a donc tout intérêt à limiter le nombre d'Utilisateurs à un strict minimum. En clair: le RAE n'est pas responsable des agissements concrets commis par les Utilisateurs autorisés dans le cadre d'une application. Ces actes tombent directement sous la responsabilité de l'Entité.
Les précisions complémentaires qui sont apportées via le SetAuthorization, n'ajoutent donc rien de plus à la protection de la confidentialité; elles facilitent uniquement les proces organisationels internes pour les déclarants. Le fait de faire ou pas une SetAuthorization n'est en soi pas pertinent pour DB2P, mais peut-être bien pour le déclarant.

4. Celui qui n'est pas repris dans le User Management ne peut rien faire dan DB2P.

5. Celui qui est connecté au User Management et a accès à DB2P, tombe sous la règle par défaut jusqu'à ce qu'une autre règle ait été définie en ce qui le concerne. La règle par défaut est, conformément à la règle 3, que tout est permis (il s'agit, en d'autres termes, d'un système ouvert).

‘Tout’ est à ce propos toujours matière à appréciation en fonction de ce que peut faire l’entité dont l’Utilisateur fait partie. Un Utilisateur d’une entité ne peut jamais effectuer plus d’actes DB2P que ce qui est possible pour l’entité (soit directement, soit parce que cette entité a un mandat).

6. Un utilisateur tombe sous la règle par défaut jusqu’à ce qu’une règle explicite ait été définie pour un groupe d’utilisateurs auquel il appartient. A partir de ce moment-là ne seront plus valables pour lui que les règles particulières. 'Tout est possible' est ensuite remplacé sur-le-champ par 'uniquement ce qui est autorisé, est encore possible'.
Si l’individu, à un moment donné, ne fait plus partie d’un groupe d’utilisateurs, mais est toujours répertorié comme utilisateur, la règle par défaut est pour lui à nouveau d’application.

7. Les droits d’accès finaux d’un individu sont toujours égals aux sommes de tous les droits dont il dispose sur base de son adhésion à un ou plusieurs groupes d’utilisateurs ayant des droits d’accès spécifiques. Une règle qui donne un droit est également toujours supérieure à une règle qui impose une interdiction. Voici quelques exemples pour illustrer ceci :

ex. un individu fait partie d’un groupe d’utilisateurs I avec des droits pour les dispositions A, B et C, et d’un groupe d’utilisateurs II avec des droits pour les dispositions D, E et F. Ses droits d’accès finaux comprennent les dispositions A à F y compris. Si l’individu est retiré de ces deux groupes, il retombe alors à la règle par défaut et l’individu peut à nouveau tout refaire (y compris A à F);

ex. un individu fait partie d’un groupe d’utilisateurs ayant uniquement des droits de consultation (et qui interdit des déclarations). Il est aussi classé auprès d’un deuxième groupe pouvant bien faire des déclarations. L’individu pourra dans ce cas aussi bien consulter que déclarer.

ex. une entité décide de limiter au maximum les accès en répartissant tous les utilisateurs dans un groupe d’utilisateurs global n’ayant aucun droit. Il n’y a maintenant plus aucun utilisateur pour qui vaut la règle par défaut. L’entité en a, en d’autres termes, fait un système fermé. Ensuite, l’entité répartit les utilisateurs dans des groupes d’utilisateurs. Les droits de chaque individu sont maintenant égals au Total des droits qu’ils ont sur base des groupes d’utilisateurs octroyant des droits, sans tenir compte du fait qu’ils appartiennent en même temps à un groupe sans droits. Si un individu est maintenant retiré de tous les groupes d’utilisateurs octroyant ces droits, cet individu retombe alors sur le groupe d’utilisateurs sans droits et non sur la règle par défaut (remarquez que dans ce cas-ci, il y a un utilisateur sans droits et qu’il vaut finalement mieux également le retirer du user management);

ex. une entité crée un groupe d’utilisateurs comprenant tous les individus et ayant tous les droits. Un individu est ensuite également classé dans un groupe d’utilisateurs avec des droits spécifiques. L’individu conservera cependant tous les droits, car c’est la somme de ses droits sur base de son adhésion au deux groupes d’utilisateurs.