MonComptePro - fournisseur d’identité

Lorsqu’un utilisateur ne peut pas être rattaché à un fournisseur d’identité externe (ex : annuaire d’un Ministère, Pôle emploi, Mission locale, CAF ou autre), alors **MonComptePro devient le fournisseur d’identité par défaut.**

Objet de la note

L’objet de cette note est de clarifier le fonctionnement de MonComptePro en tant que fournisseur d’identité.

Lexique

Fournisseur d’identité : tout dispositif permettant d’authentifier un utilisateur.

Fournisseur de service : entité proposant un ou des services applicatifs métiers nécessitant une authentification en ligne

Inscription : processus spécifique que l’utilisateur doit suivre pour accéder aux contenus et fonctionnalités proposés par les fournisseurs de services

Authentification : processus qui permet de vérifier l'identité d'une personne qui souhaite accéder à un service. Ce processus est souvent réalisé en entrant un nom d'utilisateur et un mot de passe, comme c’est le cas dans AgentConnect. Si ces informations correspondent à ce qui est enregistré dans la base utilisateur du service, l'accès est autorisé.

Autorisation (*ou habilitation*) : processus qui détermine ce qu'un utilisateur authentifié est autorisé à faire ou à voir une fois qu'il a accès à une application. L’autorisation est gérée au niveau du fournisseur de service : des dispositifs comme AgentConnect se chargent de l’authentification mais pas de l’autorisation.

AgentConnect : fédérateur d’identité à destination actuellement des agents de la fonction publique d’état, territoriale et hospitalière.

MonComptePro : fournisseur d'identité professionnel fourni par la DINUM, connecté à Agent Connect.

Préambule

Le NIST (service du gouvernement américain qui établit un équivalent de la norme eIDAS en europe) distingue 2 échelles :

- *Identity assurance level* (IAL) > c'est la preuve d'identité : est-ce que l'identité est déclarative (niveau faible), est-ce que l'identité a été vérifiée à distance (niveau substantiel), est ce que l'identité a été vérifiée en présentiel (élevé)
- *Authentication assurance level* (AAL) > c'est la preuve d'authentification : est-ce que j'ai utilisé un login et un mot de passe (niveau faible), un double facteur (niveau substantiel), ou est-ce que j'ai utilisé deux facteurs de catégories différentes (ex: carte à puce + empreinte digitale) (niveau élevé).

Cette distinction des deux échelles est intéressante pour comprendre le fonctionnement de MonComptePro en tant que fournisseur d'identité, par rapport à un fournisseur d'identité basé sur un annuaire interne d'un Ministère ou sur l'annuaire interne de Pôle emploi par exemple.

A date, les fournisseurs d'identité reliés à AgentConnect sont réputés avoir un niveau d'IAL élevé dans le sens où le fournisseur d'identité a rencontré la personne physiquement (processus RH interne de recrutement qui permet d'obtenir des accès). Ce sera également le cas d'un fournisseur d'identité Pôle emploi - France Travail.

L'enjeu de MonComptePro est de proposer un fournisseur d'identité aux diverses structures (si on prend l'exemple de l'insertion : employeurs solidaires, associations etc.) qui ne peuvent pas être rattachées à un fournisseur d'identité en propre (à la différence des agences Pôle emploi par exemple), avec un niveau d'IAL minimum garanti. Le but étant de rehausser au mieux ces niveaux (IAL et AAL) tout en veillant à ne pas complexifier les parcours et bloquer l'usage pour ces acteurs très diverses parfois peu structurés, qui ne peuvent pas suivre les mêmes processus que des acteurs institutionnels traditionnels.

Pour le fournisseur d'identité MonComptePro, le niveau IAL va se situer entre le faible et le substantiel. Les identités sont déclaratives mais passent par plusieurs filtres de vérification (automatiques et manuels) qui sont décrits ci-dessous. Pour rehausser le niveau IAL vers du substantiel, des facteurs de preuve sont mis à disposition et détaillés ci-dessous.

Fonctionnement général de MonComptePro

L’utilisateur se crée un compte nominatif (nom - prénom - email - poste occupé, en option téléphone) sur MonComptePro et l’associe à l’organisation qu’il représente. Cette organisation est identifiée à date par son numéro SIRET.

MonComptePro utilise des traitements manuels et automatiques pour vérifier la légitimité de l’utilisateur à représenter son organisation.

Mesures mises en place pour vérifier l’identité

Actuellement

Lorsqu'un utilisateur souhaite rejoindre une organisation sur MonComptePro (comme premier membre et pour les suivants), un processus automatisé est suivi :

- **Validation du SIRET et vérification de l’activité de l’organisation** : si le SIRET n’est pas valide ou que l’organisation est inactive dans la base SIREN, alors l’inscription est bloquée.
- **Traitements basés sur le type d’organisation et les noms de domaine des e-mails** : en particulier, les noms de domaine sont automatiquement comparés à ceux des adresses officielles de l’organisation (telles que déclarées sur l’annuaire service public ou l’annuaire de l’éducation nationale), pour autoriser ou non le rattachement.
- **Si des doutes subsistent, une modération manuelle est réalisée par un membre de l’équipe MonComptePro :** aujourd’hui environ 30% des demandes nécessitent une modération.

Le détail est disponible dans les annexes des CGU du service

Lorsqu’un utilisateur est rattaché à une organisation existante, **a minima un membre de l’organisation est notifié de son rattachement par e-mail**, et **peut ainsi s’opposer** en cas de doute sur la légitimité de la personne à rejoindre l’organisation.

Un utilisateur devient inactif au bout de 3 mois en l’absence de preuve d’accès à la boite mail. Un tel utilisateur devra, pour réactiver son compte, soit se connecter par lien de connexion, soit restituer un OTP (O*ne Time Password*) envoyé par mail.

A venir (2024)

Gestion des organisations par un administrateur interne : ce système pourra remplacer les traitements automatiques / manuels réalisés par MonComptePro. Ce membre administrateur pourra donc ajouter / supprimer / modifier les membres de son organisation.

Une procédure d'enrôlement sécurisée sera mise en place pour donner à la personne habilitée les droits de gestions pour son organisation → à définir avec les juristes de la DINUM.

L’objectif est d’augmenter le niveau IAL de MonComptePro.

Perspectives

Le niveau IAL dépend de chaque fournisseur d’identité utilisé et **AgentConnect vise à pouvoir faire connaître ces détails aux fournisseurs de services qui décideront de l’acceptabilité de tel ou tel fournisseur d’identité en fonction de leurs contraintes de sécurité**.

Nos objectifs 2024 :

- Laisser la main aux fournisseurs de services sur le niveau de IAL et d’AAL souhaité. Ceci sera rendu possible via le protocole OpenId Connect qui prévoit que le fournisseur de service définisse le niveau minimal de sécurité.
- Fournir un niveau AAL substantiel en introduisant un deuxième facteur d’authentification avec le fournisseur d’identité interministériel MonComptePro et en activant le double facteur chez les fournisseurs de services qui le permettent.
- Simplification des marques AgentConnect et MonComptePro au profit de authentification.numerique.gouv.fr

Enfin, dans le cadre de l’interopérabilité des services interministériels, des travaux sont lancés sur un gestionnaire d’habilitation. Il sera intéressant d’évaluer avec les équipes de Pôle emploi, d’Inclusion Connect et des fournisseurs du service du secteur de l’inclusion, si ces travaux pourraient répondre à des besoins (*qui restent à déterminer, aujourd’hui non validés*) de cette verticale métier (self service des organismes partenaires, traçabilité des accès aux ressources, …).

👉 Dans le cadre de France Travail, ces différentes évolutions permettront aux fournisseurs de services d'adapter leur niveau d'exigence en fonction de leurs besoins (*ex : si traitement de données sensibles*).
Il faudra cependant être vigilant à ne pas introduire trop de complexité pour les utilisateurs (notamment pour ceux qui seront dépendants du fournisseur d'identité par défaut, car ne faisant pas partie d'une structure institutionnelle disposant de son propre fournisseur d'identité). Dans le cadre du déploiement du service d'Inclusion Connect, nous avons remarqué que de nombreuses organisations (de petites tailles) partagent un même compte pour accéder à différents services, rendant délicate l'application de mesures de sécurité de type 2FA ou OTP / et de nombreuses difficultés au niveau de l'appropriation des outils numériques (manque de formation).