Rapprocher des identités dans PRONOTE

Version 2.0

Cycle de vie du document				
Action	**Date**	**Rédacteur**	**Version**	**Commentaire**
Création	21/04/2016	Equipe E.D.I.	1.0	Création du document
Modification	23/05/2018	Equipe E.D.I.	2.0	Passage en V2.0 du schéma XSD de rapprochement des identités
Modification	11/06/2018	Equipe E.D.I.	2.0	Présence obligatoire d'au moins 1 établissement et 1 établissement géré

Table des matières

1. Introduction

La société Index-Education propose aux fournisseurs d'identités et aux partenaires qui le souhaitent la possibilité d'intégrer dans la base PRONOTE d'un établissement scolaire les identifiants uniques des individus qui seront utilisés comme unique clé d'identification pour l'authentification unique.

Le but est d'une part de garantir aux établissements scolaires un haut niveau de sécurisation des données personnelles de leurs usagers à importer dans PRONOTE au titre du rapprochement des identités.

D'autre part, il s'agit de restreindre les contenus des échanges sécurisés qui sont établis entre PRONOTE et l'applicatif tiers dans le contexte de l'authentification unique, le but étant de n'avoir comme attribut de négociation qu'un identifiant opaque ne permettant pas d'identifier un individu en cas de fuite des données.

Les données XML permettant le rapprochement des identités dans un millésime de PRONOTE antérieur à 2018 sont spécifiées par le schéma RapprochementSSO1.0.xsd (version 1.0) qui n'est pas concerné par cette documentation n'utilisera donc pas cette version du schéma.

Les données XML permettant le rapprochement des identités dans un millésime de PRONOTE supérieur ou égal à 2018 seront spécifiées par le schéma RapprochementSSO2.0.xsd (version 2.0).

2. Présentation du cadre d'exposition des liens vers le site partenaire

2.1. Nos clients

Nos logiciels Index-Education sont vendus directement aux établissements scolaires. Un établissement qui achète une licence PRONOTE peut administrer un serveur PRONOTE sur lequel tous les utilisateurs se connectent. Les utilisateurs, en fonction de leurs profils (voir le paragraphe suivant), peuvent se connecter soit par le biais d'un logiciel à installer (client lourd), soit par le biais d'une interface web (client léger).

Dans le cadre de la délégation de l'authentification à PRONOTE qui nous intéresse ici, seuls les clients ayant acquis une licence d'hébergement dans nos centres Index-Education et qui ont donc leur applicatif serveur PRONOTE qui tourne sur nos serveurs (soit plus de 3000 établissements en 2016), ont la possibilité de proposer à un utilisateur authentifié à PRONOTE d'accéder à son espace personnel sur le site du partenaire sans réauthentification depuis un lien mis à disposition dans la rubrique « Liens utiles » de la page d'accueil du client PRONOTE[1].

2.2. Nos utilisateurs

Nos logiciels Index-Education sont utilisés par des utilisateurs de profils très divers. Les utilisateurs potentiels de cette délégation de l'identification à PRONOTE peuvent être :

- L'utilisateur Administratif qui accède à toutes les fonctions d'administration du logiciel depuis PRONOTE client en mode Administrateur ou depuis l'Espace Administratif (SPR) de PRONOTE.net (*nouveauté 2018*),
- Les professeurs qui se connectent à la fois sur PRONOTE client en mode Enseignant et sur l'Espace Professeurs de PRONOTE.net,
- Les personnels de vie scolaire qui se connectent à la fois sur le PRONOTE client en mode Vie scolaire ou sur l'Espace Vie Scolaire de PRONOTE.net,
- Les élèves qui se connectent sur l'Espace Elèves de PRONOTE.net,
- Les parents qui se connectent sur l'Espace Parents de PRONOTE.net,
- Les maîtres de stage qui se connectent sur l'Espace Entreprise de PRONOTE.net
- Les inspecteurs académiques qui se connectent sur l'Espace Académie de PRONOTE.net.

2.3. Applicatifs partenaires concernés par le rapprochement d'identités

Pour un établissement scolaire donné, la base de données PRONOTE et la base de données de l'applicatif partenaire travaillent sur la même population d'individus tout en format deux référentiels distincts.

Le rapprochement des identités permet le stockage dans la base PRONOTE de l'identifiant unique de chaque individu commun aux deux référentiels utilisateurs. Etant donné que l'identifiant est le recours ultime dans une interface graphique pour régler un

[1] Emplacement non garanti dans PRONOTE.

problème de correspondance, la société Index-Education interdit au partenaire de fournir des identifiants uniques qui ne diffèrent que par la casse ou par les accents. De plus, le partenaire devra garantir l'unicité de chaque identifiant associé à chaque individu de sa base clients peu importe le nombre d'établissements que doit gérer le partenaire.

Les types de partenaires susceptibles d'exporter vers PRONOTE un tel fichier de rapprochement d'identités sont les suivants :

- Fournisseurs d'identités : Espaces Numériques de Travail (ENT), Learning Management System (LMS), portails de connexions (etc.) qui exposent un serveur CAS ou ADFS pour l'authentification unique,
- Editeurs ou fournisseurs de ressources numériques pédagogiques,
- Prestataires de gestion de la restauration scolaire et/ou du contrôle d'accès,
- Applicatifs spécialistes de la gestion administrative et financière des établissements scolaires privés ou français de l'étranger ou étrangers.

3. Création d'un fichier de rapprochement d'identités

Le rapprochement sera possible via les informations nominatives de chaque individu. Il se fera en deux étapes :

1) Les informations nominatives plus les identifiants uniques sont exportés dans un fichier sécurisé depuis le le socle ENT ou l'applicatif partenaire,
2) Le fichier ainsi exporté depuis le socle ENT ou l'applicatif partenaire est importé dans PRONOTE pour le rapprochement d'identités.

3.1. Export d'un fichier de rapprochement d'identités depuis le logiciel partenaire

La première étape est d'exporter, depuis le système partenaire contenant les informations nominatives des utilisateurs associées à leurs identifiants uniques, un fichier XML contenant le flux de données qui permettra à PRONOTE après import de réaliser la correspondance des identités.

Ce fichier de rapprochement d'identités doit être incorporé dans un document XML « conteneur » « sécurisé » répondant au schéma de spécification « ConteneurImportChiffre.xsd » (voir la documentation intitulée « Format sécurisé échange partenaire Index-Education » fournie en annexe). La sécurisation des données contenues dans ce fichier utilise la combinaison de deux méthodes de chiffrement :

1) Chiffrement du flux par un couple AES (clé, vecteur d'initialisation) généré aléatoirement lors de chaque export du partenaire,
2) Chiffrement asymétrique RSA 2048 bits du couple AES.

L'imbrication de ces deux techniques de chiffrement assure que le flux à échanger est chiffré de manière performante.

La clé publique RSA utilisée est la clé Index-Education au format .pub qui sera fournie au partenaire. La connaissance exclusive de la clé privée RSA associée garantit à Index-Education d'être le seul acteur à pouvoir déchiffrer le flux et donc à pouvoir exploiter les données après déchiffrement.

Ce fichier XML sécurisé ainsi généré permet de transmettre un flux XML « sensible » contenant des informations personnelles des individus présents dans la base de données du partenaire. Le flux XML issu du déchiffrement est spécifié par le schéma « RapprochementSSO2.0.xsd » dans lequel il est nécessaire de renseigner l'espace de nommage suivant :

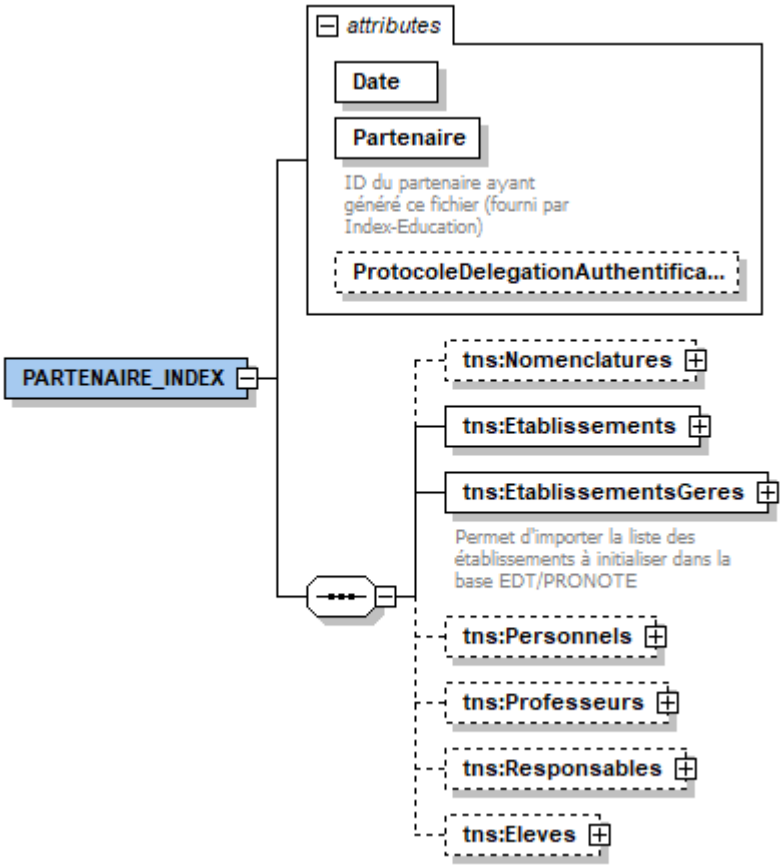
http://www.index-education.com/rapprochemenntssoV2.0

Le schéma « RapprochementSSO2.0.xsd » nécessite la connaissance de la valeur attendue pour l'attribut « Partenaire » devra être communiquée par Index-Education. Il impose également la présence d'au moins un établissement et d'au moins un établissement géré.

Si le rapprochement d'identités concerne des identifiants CAS ou ADFS car le serveur PRONOTE et/ou le serveur PRONOTE.net va déléguer l'authentification au serveur CAS ou ADFS du socle ENT, alors la valeur de l'attribut « ProtocoleDelegationAuthentification » (type xs:string) doit être renseignée dans le flux XML en ne pouvant prendre que 2 valeurs possibles :

- '*CAS*' si l'authentification à PRONOTE est déléguée à un serveur CAS (méthode samlValidate)
- '*ADFS*' s'il y a délégation d'authentification à un serveur ADFS (protocole WS-Federation).

Nous proposons que la règle de nommage du fichier XML sécurisé à importer dans PRONOTE soit la suivante : « *RapprochementIdentités_CodePartenaire.xml* », où « Code_Partenaire » prendra la valeur de l'attribut « Partenaire » précisée par Index-Education.



3.2. Import d'un fichier de rapprochement d'identités dans PRONOTE

La seconde étape de l'échange est d'importer ce fichier XML sécurisé dit de rapprochement d'identités dans PRONOTE pour pouvoir stockage en base l'identifiant unique de chaque individu rapproché. Pour ce faire, Index-Education a développé des interfaces graphiques[2] de gestion des échanges avec :

- Le fournisseur d'identités (ex : socles ENT) dont les serveurs CAS ou ADFS assurent l'authentification unique à la place du serveur PRONOTE et/ou du serveur PRONOTE.net
- Les applicatifs partenaires qui ont délégué l'authentification au serveur CAS PRONOTE.

3.2.1. Gestion des socles ENT et des partenaires

Dans l'onglet *Communication > Gestion des identités > Délégation d'authentification*, l'Administrateur PRONOTE peut choisir le type de serveur du socle ENT auquel l'authentification a été délégué. Les utilisateurs rapprochés ou à rapprochés sont sélectionnables par type de public. Enfin, il soit saisir manuellement un identifiant unique, soit importer les identifiants uniques à partir d'un fichier texte (*.txt), soit importer un fichier XML de rapprochement d'identités.

Pour les applicatifs partenaires, l'Administrateur doit se rendre sur l'onglet *Communication > Partenaires* puis il sélectionne le type de partenaires (gestion financière ou restauration scolaire) et enfin le partenaire souhaité dans la liste. Il peut ensuite choisir le fichier XML à importer en cliquant sur le widget « Importer des identifiants » du volet « Interconnexion » ou en cliquant sur le bouton « Récupérer les identifiants » du volet « Rapprochement des identités ». Le flux de données est alors déchiffré grâce à la clé RSA privée d'Index-Education, puis les identifiants partenaires sont importés dans la base PRONOTE à partir de rapprochements automatiques basés sur les données d'identité (Nom, Prénom, Date de naissance, etc.) des individus contenus dans le fichier XML.

A l'issue de chaque action de rapprochement, un rapport d'import est affiché à l'Administrateur présentant le nombre d'individus de la base PRONOTE ayant pu être rapprochés. A noter que pour chaque nouvelle demande de rapprochement d'identités, un message de confirmation est affiché précisant que l'Administrateur peut soit conserver les identifiants rapprochés lors du précédent import auxquels seront ajoutés les nouveaux identifiants ayant pu être rapprochés, soit effacer tous les anciens identifiants de la base PRONOTE et réaliser un nouveau rapprochement.

[2] Emplacement de l'interface non garanti dans PRONOTE.

3.2.2. Gestion manuelle des échecs de reconnaissance

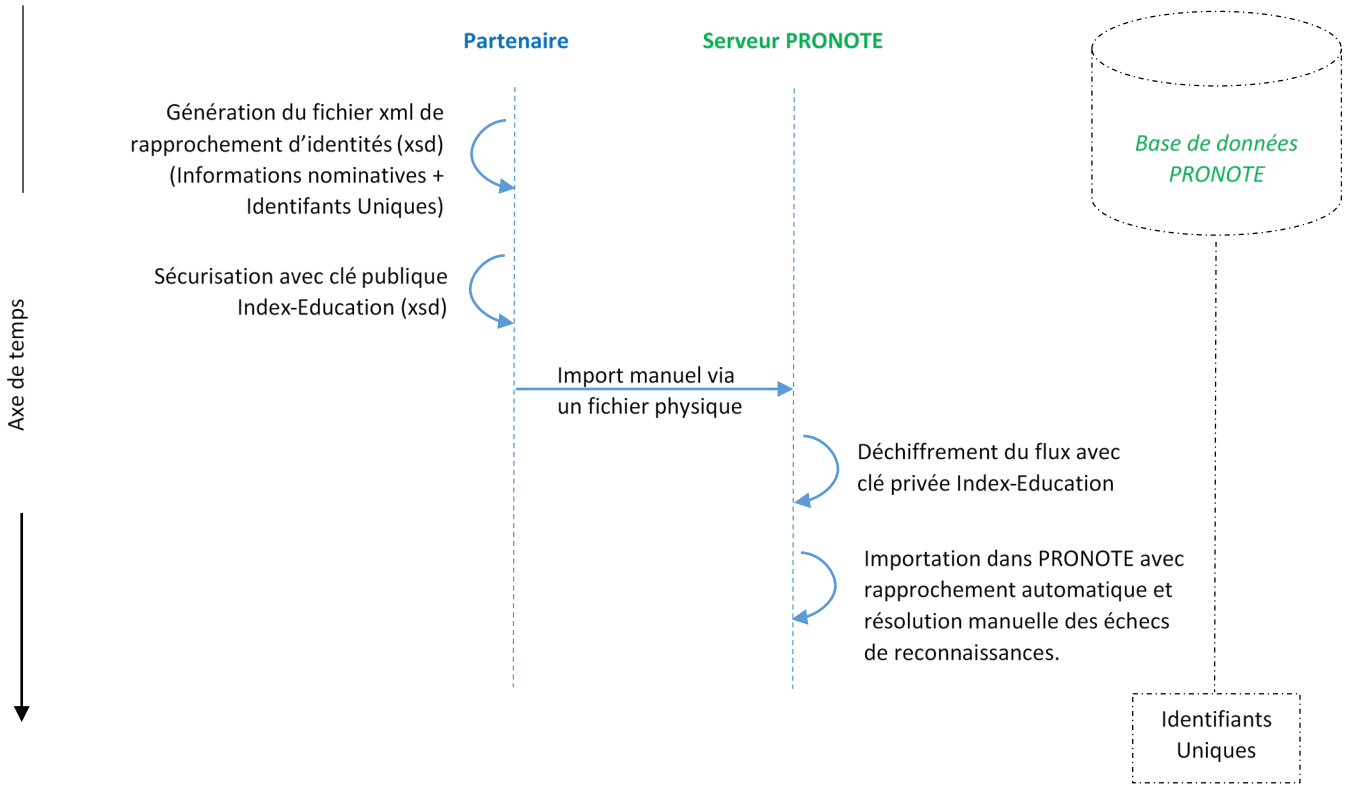
Après import des identifiants partenaires, l'Administrateur peut détecter les éventuels échecs survenus lors de la reconnaissance automatique d'identités. Ces erreurs résultant de la non-adéquation de données individus de la base du logiciel partenaire avec les données utilisateurs de la base PRONOTE de l'établissement. Dans ce cas, une interface de résolution manuelle des erreurs de rapprochements est mise à la disposition du superviseur dans PRONOTE.

Cette interface, accessible depuis l'onglet *Communication* > *Partenaires* pour les applicatifs partenaire et depuis l'onglet *Communication* > *Gestion des identités* > *Délégation* d'authentification de PRONOTE client[3], présente, pour chaque partenaire, les outils suivants :

- Un tableau récapitulant par type de profils utilisateurs, le nombre d'individus de la base PRONOTE, le nombre d'individus dans le fichier de rapprochements, le nombre d'individus rapprochés et le nombre d'individus restants à rapprocher.
- Un widget « Récupérer les identifiants » qui permet de refaire un rapprochement d'identités pour récupérer en mémoire les identifiants partenaires ou les identifiants CAS/ADFS contenus dans le fichier.
- Exposition sous ce widget du nom du fichier de rapprochement : le nom de fichier est exposé si un rapprochement d'identités vient d'être effectué ou si la mise en mémoire des identifiants vient d'être faite par le superviseur. Un rapprochement manuel ne peut être réalisé que si les identifiants partenaires ont été préalablement récupérés et stockés en mémoire.

Un tableau détaillant, pour chaque type d'utilisateurs supporté, la liste des utilisateurs présents dans la base PRONOTE d'une part et présents dans le fichier de rapprochement issu de la base de données partenaire d'autre part. L'Administrateur peut ensuite sélectionner un utilisateur (un élève par exemple) présent dans la base PRONOTE de l'établissement (respectivement dans le fichier de rapprochement d'identités), double-cliquer sur la colonne *Identifiant partenaire* (respectivement la colonne *Ressources Pronote*) afin d'ouvrir une interface graphique dédiée à la gestion manuelle des correspondances. L'Administrateur peut alors rechercher un individu parmi une liste d'utilisateurs de même profil provenant du fichier de rapprochements (respectivement de la base PRONOTE) et effectuer manuellement la correspondance (avec la possibilité de ne rechercher que les individus n'ayant pas d'identifiants partenaire). Une demande de confirmation est alors envoyée à l'Administrateur avant toute modification de la base de données PRONOTE.

3.3. Diagramme de séquence du rapprochement d'identités dans PRONOTE



[3] Configurations des menus et onglets non garantie dans PRONOTE client.

4. Conclusion

En proposant à ses partenaires ou aux fournisseurs d'identités la possibilité d'exporter un fichier XML sécurisé contenant les données nominatives des individus d'un établissement scolaire en vue de permettre le « rapprochement des identités » dans PRONOTE, Index-Education facilite la vie des différents acteurs :

- Chaque utilisateur authentifié à PRONOTE peut accéder sur demande et sans réauthentification à son espace personnel sur le site du partenaire ou à son compte PRONOTE si le rapprochement d'identités est réalisé car le serveur PRONOTE et/ou le serveur PRONOTE.net ont délégué leur authentification à un tiers fournisseur d'identités,
- Les personnels administratifs des établissements scolaires n'ont plus à leur charge de stocker ni de transmettre à chacune de ses ressources les paramètres de connexion vers les différents espaces personnels des usagers,
- Chaque partenaire autorisé à afficher ce lien vers son site en ligne dans PRONOTE s'exonère ainsi de la fourniture de logins / mots de passe et de toutes autres informations personnelles relatives à ses utilisateurs pour qu'ils s'authentifient à leurs espaces personnels
- Chaque fournisseur d'identités s'exonère de devoir importer un identifiant unique PRONOTE par utilisateur commun, identifiant qui servait à reconnaître l'individu dans l'annuaire du fournisseur d'identités après validation d'un ticket de service ou d'un jeton sécurisé.

Pour toute question relative à l'interconnexion : interconnexion@index-education.fr