INDEX ÉDUCATION
CS 90001 13388 Marseille cedex 13
www.index-education.com
info@index-education.fr
Tél : (+33) 04 96 15 21 70
Fax : (+33) 04 96 15 00 06

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599



Authentification avec CAS sous PRONOTE et Pronote.net 2017

Version du mardi 11 avril 2017

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

Table des matières

1. Vocabulaire employé et documentation 3

1.1. SSO (Single Sign-On) 3

1.2. CAS (Central Authentication Service) 3

1.3. SAML (Security Assertion Markup Language) 3

2. Schéma général d'une authentification avec CAS 3

2.1. Un utilisateur se connecte à l'aide d'un navigateur au client CAS 3

2.2. Le client CAS répond en envoyant une redirection vers le serveur CAS 3

2.3. Le serveur CAS répond en envoyant une redirection vers le client CAS et en spécifiant un ticket de service 4

2.4. Le client CAS interroge le serveur CAS pour demander validation du ticket de service et reçoit en retour les informations d'authentification 4

2.5. Si le serveur CAS répond favorablement, le client CAS accepte l'authentification et commence à servir l'utilisateur 5

3. Client CAS de Pronote.net 2017 5

4. Délégation d'authentification du client lourd PRONOTE 2017 5

5. Les options pour la première connexion 6

6. Interfaces d'administration PRONOTE serveur et Pronote.net 7

6.1. Interface de paramètres de publication de Pronote.net 7

6.2. Interface de paramétrage d'intégration dans un ENT (avec CAS) 7

6.2.1. Configuration par sélection de modèle de votre ENT 9

6.2.2. Configuration manuelle 9

URL du serveur CAS : 9

URL à communiquer au socle ENT : 9

Autoriser l'authentification directe par Pronote.net ou PRONOTE : 9

6.3. Paramétrage avancé 9

6.3.1. Avec l'identité de l'utilisateur (par défaut) 11

6.3.2. Avec l'identifiant PRONOTE de l'utilisateur 11

Sécurité et aspects légaux : 12

Stockage d'un identifiant PRONOTE : 12

Plusieurs identifiants PRONOTE pour un même utilisateur CAS : 12

Utilisateurs multi-profils : 12

Changement d'année scolaire : 12

6.3.3. Via la page de connexion des Espaces Pronote.net ou depuis le client PRONOTE 13

6.3.4. Refuser l'accès si l'identifiant CAS n'est pas renseigné dans PRONOTE 13

6.4. Bouton « Tester l'authentification par le serveur CAS » 14

7. Informations à transmettre à l'administrateur du serveur CAS 14

8. Single Sign Out 14

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

1. Vocabulaire employé et documentation

1.1. SSO (Single Sign-On)

Single Sign-On est traduit en français par *Authentification Unique* ou *Identification Unique*. Il s'agit de permettre à un utilisateur de ne s'authentifier qu'une seule fois pour accéder à plusieurs applications.

Voir http://fr.wikipedia.org/wiki/Authentification_unique

1.2. CAS (Central Authentication Service)

CAS est une architecture pour implémenter un système d'authentification unique (SSO) en s'appuyant sur des systèmes d'authentification tiers comme LDAP, Active Directory, une base SQL, etc. L'architecture est générique et ne dépend pas du système d'authentification choisi.

CAS est un projet du groupe JASIG (Java Architectures Special Interest Group).

Pour plus d'informations, le lecteur peut se référer aux articles en ligne suivants :

http://fr.wikipedia.org/wiki/Central_Authentication_Service

https://www.apereo.org/projects/cas/

https://wiki.jasig.org/display/CAS/Home

1.3. SAML (Security Assertion Markup Language)

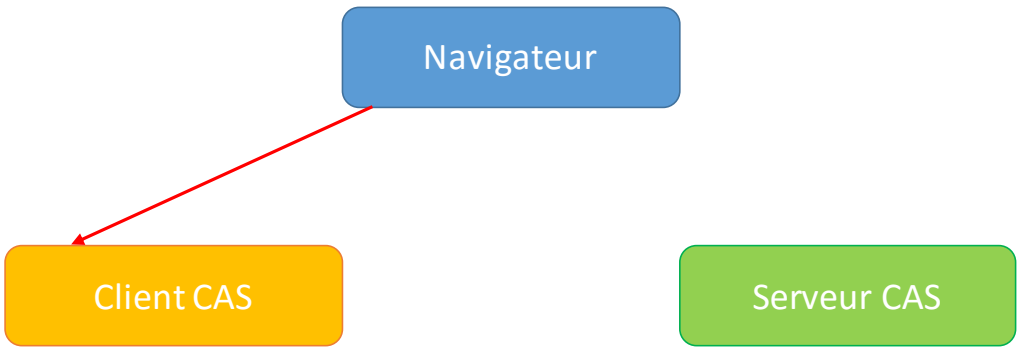
SAML est un langage XML pour échanger des informations de sécurité entre applications.

Voir https://fr.wikipedia.org/wiki/Security_assertion_markup_language

2. Schéma général d'une authentification avec CAS

Ce schéma décrit les échanges entre un navigateur, un client CAS et un serveur CAS.

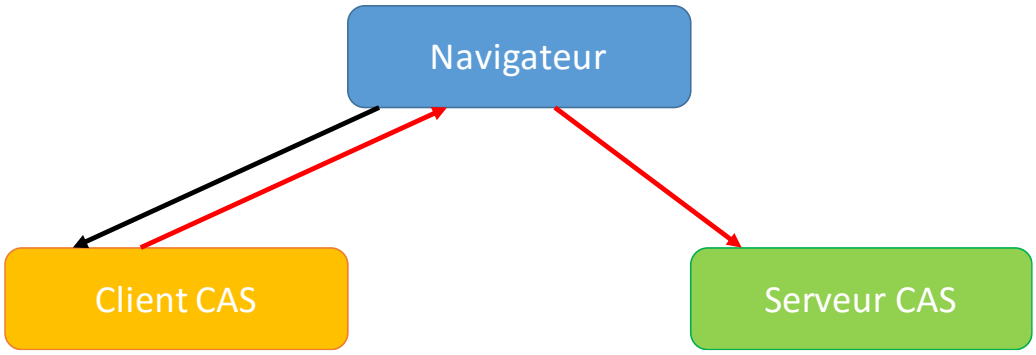
2.1. Un utilisateur se connecte à l'aide d'un navigateur au client CAS



2.2. Le client CAS répond en envoyant une redirection vers le serveur CAS

En paramètre de l'URL il passe sa propre adresse comme adresse de retour. L'adresse de redirection a la forme https://serveurcas/cas/login?service=https:%2F%2Fclientcas%2F

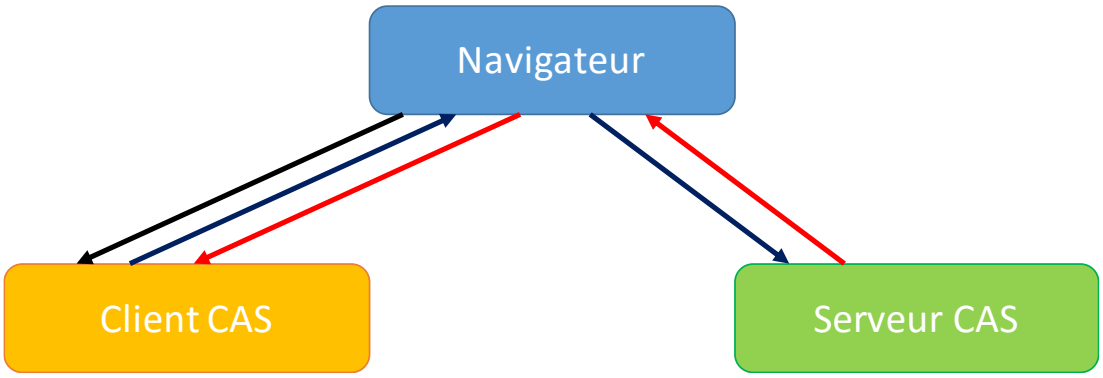
S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599



2.3. Le serveur CAS répond en envoyant une redirection vers le client CAS et en spécifiant un ticket de service

Cette adresse de redirection a la forme https://clientcas/?ticket=ST-74-IrItJgBOoWHnkprmzWFp

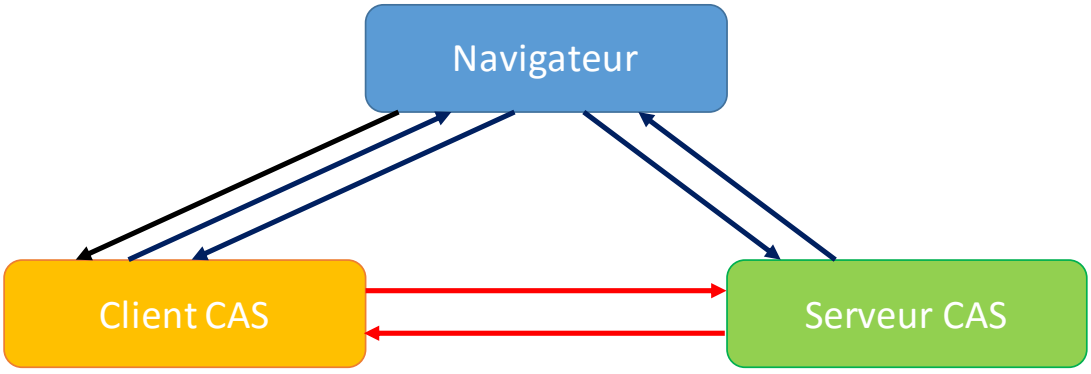
Si l'utilisateur est déjà authentifié auprès du serveur CAS (cookie dans le navigateur), le serveur CAS répond immédiatement. Sinon le serveur CAS propose une page d'authentification puis envoie la redirection.



2.4. Le client CAS interroge le serveur CAS pour demander validation du ticket de service et reçoit en retour les informations d'authentification

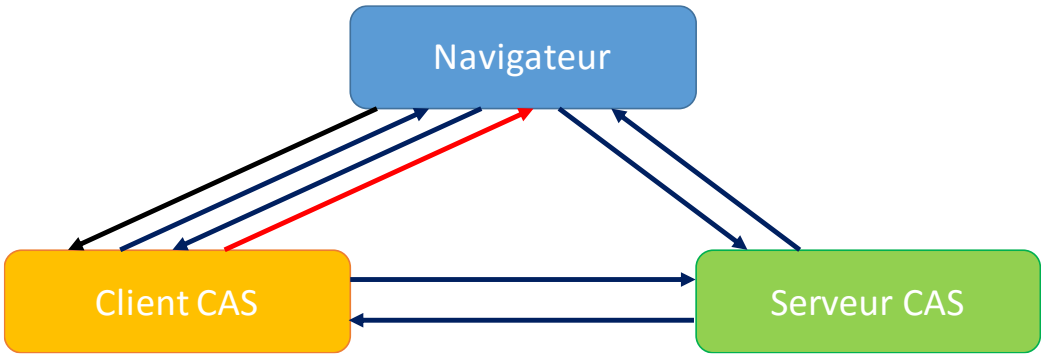
Typiquement le client CAS envoie une requête POST de la forme :

https://serveurcas/cas/samlValidate?TARGET=https:%2F%2Fclientcas%2F, le corps de la requête étant un bloc SAML. La réponse du serveur CAS est également un bloc SAML.



S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

2.5. Si le serveur CAS répond favorablement, le client CAS accepte l'authentification et commence à servir l'utilisateur



3. Client CAS de Pronote.net 2017

Pronote.net 2017 intègre un client CAS, toute la configuration d'interconnexion avec CAS s'effectue dans l'interface de l'application d'administration Pronote.net.

Le seul prérequis est un certificat dans le cas où le serveur Pronote.net est configuré pour utiliser HTTPS au lieu de HTTP.

Le serveur Pronote.net 2017 comprend nécessairement un serveur HTTP ou HTTPS pour le retour depuis le serveur CAS décrit au point 2.3. Mais attention : en mode HTTP, le ticket de service passe en clair sur le réseau. Si ce ticket est intercepté, celui qui l'intercepte a la possibilité de se connecter à Pronote.net et s'il le fait plus rapidement que le navigateur destinataire de ce ticket, il a accès à tout ce à quoi aurait pu accéder l'utilisateur qui s'est authentifié. C'est une faille de sécurité importante.

En mode HTTPS avec un certificat valide, cette interception n'est pas possible a priori[1].

Utiliser HTTPS avec un certificat auto-généré, c'est à dire non signé par une autorité de certification reconnue, n'offre pas plus de sécurité qu'utiliser HTTP : ceux susceptibles d'intercepter les communications peuvent eux-mêmes générer un certificat de même nom qui ne peut pas être différencié du vrai certificat par l'utilisateur.

Le mode HTTP est proposé en phase d'évaluation, ou si les utilisateurs n'accèdent pas à Pronote.net directement mais au travers d'un autre serveur HTTPS ou d'un proxy inverse.

Pour les établissements scolaires, il existe une autorité de certification *AC Education Nationale*, elle-même certifiée par le *Secrétariat Général de la Défense Nationale*, qui peut émettre des certificats valides.

Tous les établissements dont les serveurs sont hébergés chez Index Education utiliseront le même certificat **.index-education.net* certifié par *GoDaddy Secure Certification Authority*.

4. Délégation d'authentification du client lourd PRONOTE 2017

Cette fonctionnalité déjà présente dans PRONOTE 2016 permet l'authentification du client lourd à un serveur CAS. Cette fonctionnalité repose sur un principe technique proche que celui de Pronote.net présenté ci-dessus et nécessite une configuration dans la rubrique « *Déléguer l'authentification* » de l'interface graphique du serveur PRONOTE 2017.

Le principe de base est de considérer l'architecture CAS vue précédemment mais en considérant :

- Le serveur PRONOTE comme un serveur web en https hébergeant un client CAS,
- Le client lourd PRONOTE comme un navigateur web.

[1] Il y a pourtant eu une faille par le passé qui permettait de le faire. Voir http://www.microsoft.com/france/technet/security/Bulletin/MS09-056.mspx. Cette faille a été corrigée le 13 octobre 2009, et il est recommandé que les mises à jour Windows soient effectuées régulièrement pour plus de sécurité.

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

Comme pour Pronote.net, il est nécessaire de sécuriser les communications entre le client CAS et le navigateur, particulièrement lorsque le serveur CAS répond en envoyant une redirection vers le client CAS et en spécifiant le ticket de service. A la différence de l'authentification avec CAS sous Pronote.net qui utilise le protocole HTTPS au niveau de la couche application, la sécurisation des communications client lourd – serveur PRONOTE requiert un protocole d'authentification du serveur au niveau des couches session et transport.

Le serveur doit être configuré avec un certificat numérique X.509 délivré par une autorité de certification afin de garantir l'authentification du serveur PRONOTE et sécuriser le canal de communication client-serveur. Il est possible d'importer des certificats et de choisir le certificat à utiliser dans la partie « Gestion du certificat » de la rubrique « Déléguer l'authentification » de l'interface graphique du serveur PRONOTE 2017. Il est rappelé que, pour éviter toute faille de sécurité, un certificat serveur X.509 auto-généré ne sera pas accepté lors de la mise en service du serveur PRONOTE.

Lors du paramétrage dans l'interface graphique du serveur PRONOTE 2017, l'url de service (url du client CAS) nécessaire pour la validation du ticket CAS auprès du serveur CAS doit être conforme au certificat pour permettre la mise en service du serveur. **A noter que le serveur PRONOTE ne répond pas sur une requête sur cette url de service.**

La transmission du ticket CAS entre le client PRONOTE et le serveur CAS PRONOTE sera chiffrée sur un canal TLS à partir des algorithmes de chiffrement de la couche cryptographique de Microsoft Windows Secure Channel (Schannel).

Le client lourd doit vérifier que le certificat côté serveur est valide, que le serveur s'est avéré possesseur de la clé privée associée au certificat serveur X.509 et que l'identité du serveur est bien contenue dans le certificat.

Pour authentifier l'utilisateur, le client PRONOTE 2017 affiche la page de login de l'ENT dans un navigateur intégré. D'un point de vue fonctionnel, l'utilisateur administratif, enseignant ou personnel de l'établissement n'aura pas à changer ses habitudes de connexion et s'authentifiera auprès du serveur sans se soucier des considérations techniques sous-jacentes.

Tous les établissements dont les serveurs sont hébergés chez Index-Education utiliseront le même certificat serveur **.index-education.france* certifié par *GoDaddy Secure Certification Authority*.

5. Les options pour la première connexion

Ces options sont valables aussi bien pour le client lourd que pour le client léger.

Lorsque la réponse SAML du serveur CAS (étape 2.4) contient un identifiant d'utilisateur inconnu de la base PRONOTE, le comportement par défaut est d'analyser le contenu d'autres attributs, « nom », « prenom », « dateNaissance », « codePostal », et « categories » pour identifier l'utilisateur.

PRONOTE ou Pronote.net propose d'autres options permettant de retrouver l'utilisateur :

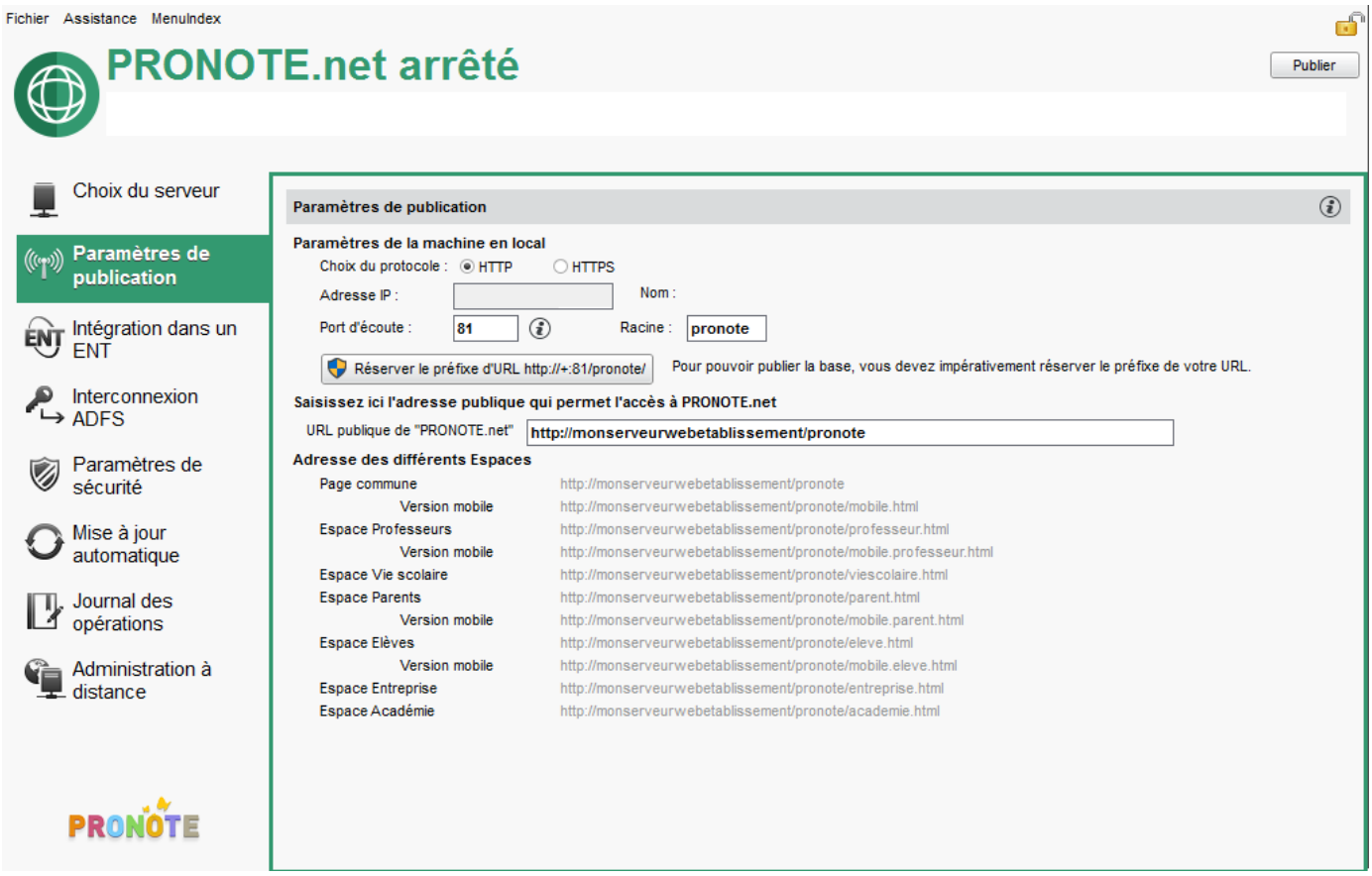
- Soit l'utilisation d'un attribut contenant l'identifiant PRONOTE, les identifiants PRONOTE étant exportés au préalable vers la base du serveur CAS,
- Soit une seconde authentification en utilisant l'identifiant et le mot de passe PRONOTE.

Dans tous les cas cela ne concerne que la première connexion à PRONOTE ou Pronote.net : une fois l'utilisateur identifié avec succès, son identifiant CAS est mis à jour dans la base et les connexions suivantes seront acceptées en n'utilisant que cet identifiant.

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

6. Interfaces d'administration PRONOTE serveur et Pronote.net

6.1. Interface de paramètres de publication de Pronote.net



URL publique de « Pronote.net » :

Afin que l'intégration dans un ENT puisse aboutir, il est nécessaire de renseigner l'url publique de votre Pronote.net qui est l'url telle qu'elle doit être saisie dans le navigateur d'un utilisateur qui se connecte à Pronote.net. Si l'utilisateur n'accède pas directement à Pronote.net mais au travers d'un autre serveur web, c'est ce dernier qui doit apparaître ici.

6.2. Interface de paramétrage d'intégration dans un ENT (avec CAS)

6.2.1. Version hébergée chez Index-Education

Ce paragraphe concerne les établissements qui utilisent PRONOTE en mode hébergé chez Index-Education.

Pour le client léger : depuis la console d'hébergement, onglet *Intégration dans un ENT > Interconnexion*, et après avoir dépublié la base, activez la case à cocher « Activer l'interconnexion avec un ENT ».

Pour le client lourd : depuis la console d'hébergement, onglet *Déléguer l'authentification*, et après avoir dépublié la base, activez la case à cocher « Activer le SSO ».

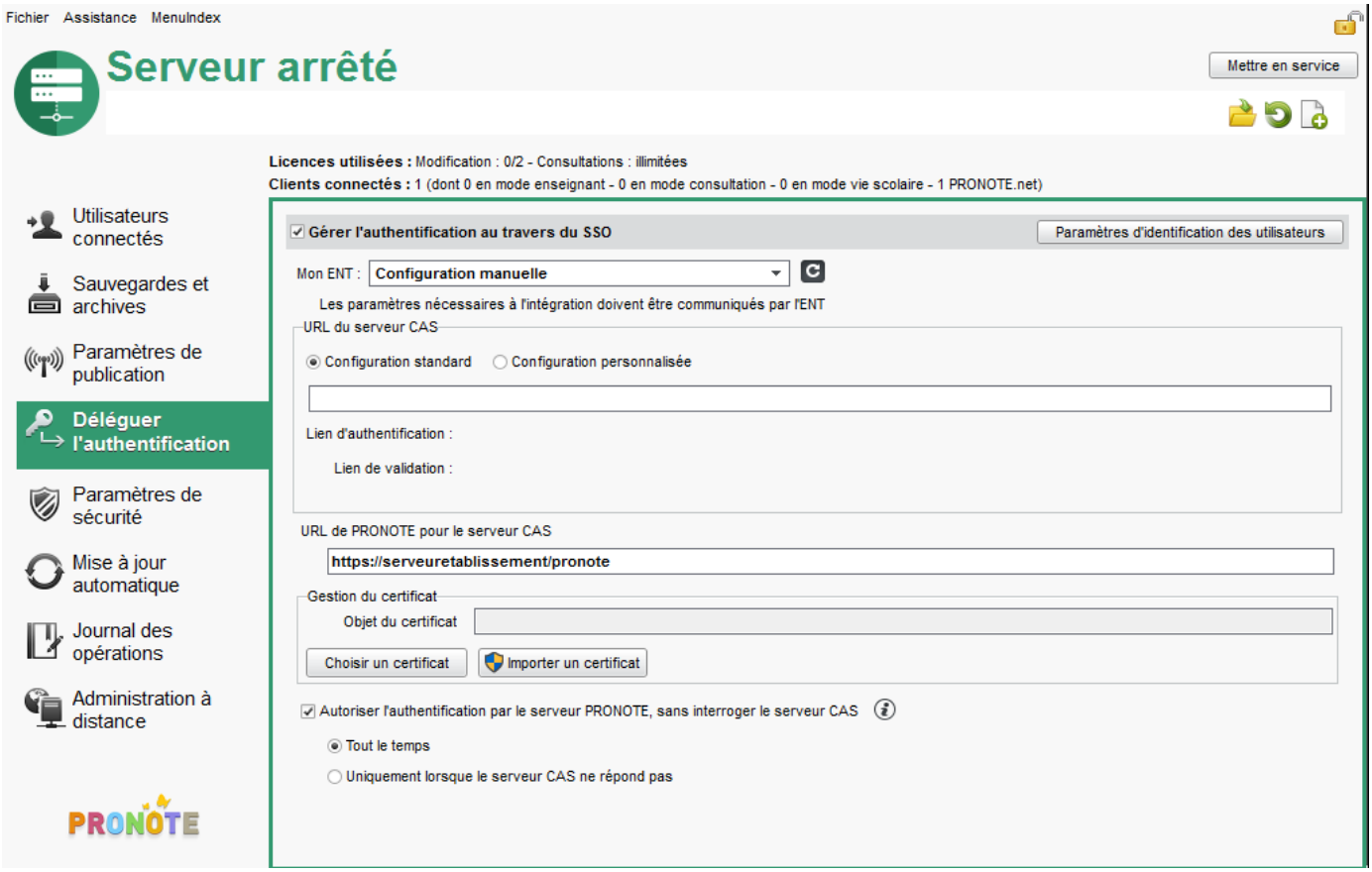
6.2.2. Version non hébergée

Pour le client léger : Depuis l'interface graphique de Pronote.net, onglet *Intégration dans un ENT > Interconnexion*, activez la case à cocher « Activer l'interconnexion avec un ENT ».

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599



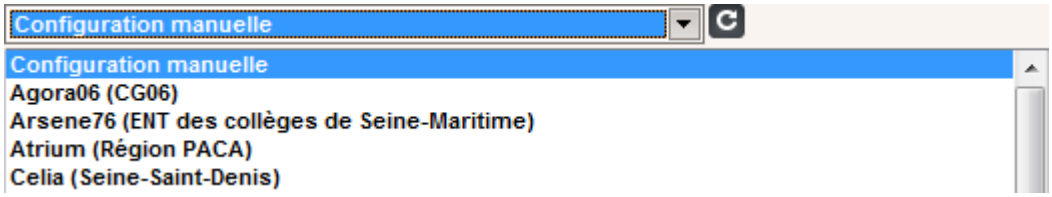
Pour le client lourd : Depuis l'interface graphique de PRONOTE serveur, onglet *Déléguer l'authentification*, activez la case à cocher « Activer le SSO ».



S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

6.2.3. Configuration par sélection de modèle de votre ENT

Désormais vous pouvez configurer l'interconnexion par sélection de votre ENT dans une liste si celui-ci a fourni à Index-Education les modèles de configuration CAS (voir documentation : http://www.index-education.com/contenu/telechargement/partenaires/DocumentationModelesConfigurationCAS-Pronote2017.pdf).

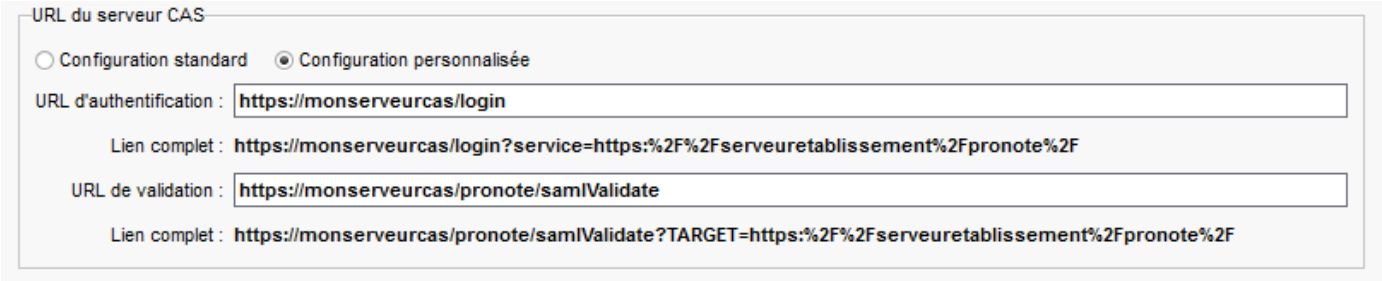


Ces modèles de configuration CAS sont communs à PRONOTE et à Pronote.net 2017.

6.2.4. Configuration manuelle

URL du serveur CAS :

Quand on saisit cette url, l'interface met à jour les adresses utilisées pour l'authentification et pour la validation (respectivement aux étapes 2.2. et 2.4. décrites ci-dessus). Ces valeurs peuvent être sélectionnées pour être copiées ailleurs. Au cas où les url de la page de login et de validation ne sont pas les mêmes, vous pouvez cocher l'option « Les adresses d'authentification et de validation sont différentes » puis saisir les deux url distinctes.



URL à communiquer au socle ENT :

Quand on change l'url publique de Pronote.net sur l'interface des paramètres de publication ou quand on change l'url de PRONOTE à communiquer au serveur CAS, l'interface met à jour l'url de Pronote.net ou de PRONOTE pour le serveur CAS. Cette valeur peut être sélectionnée et copiée ailleurs, et doit être communiquée à l'administrateur du serveur CAS (voir partie 7.). Les deux astérisques à la fin de l'url de service pour Pronote.net signifient que le serveur CAS doit accepter toutes les url de service commençant par ce qui précède ces deux astérisques (dans les implémentations publiques des serveurs CAS en tous cas).

Autoriser l'authentification directe par Pronote.net ou PRONOTE :

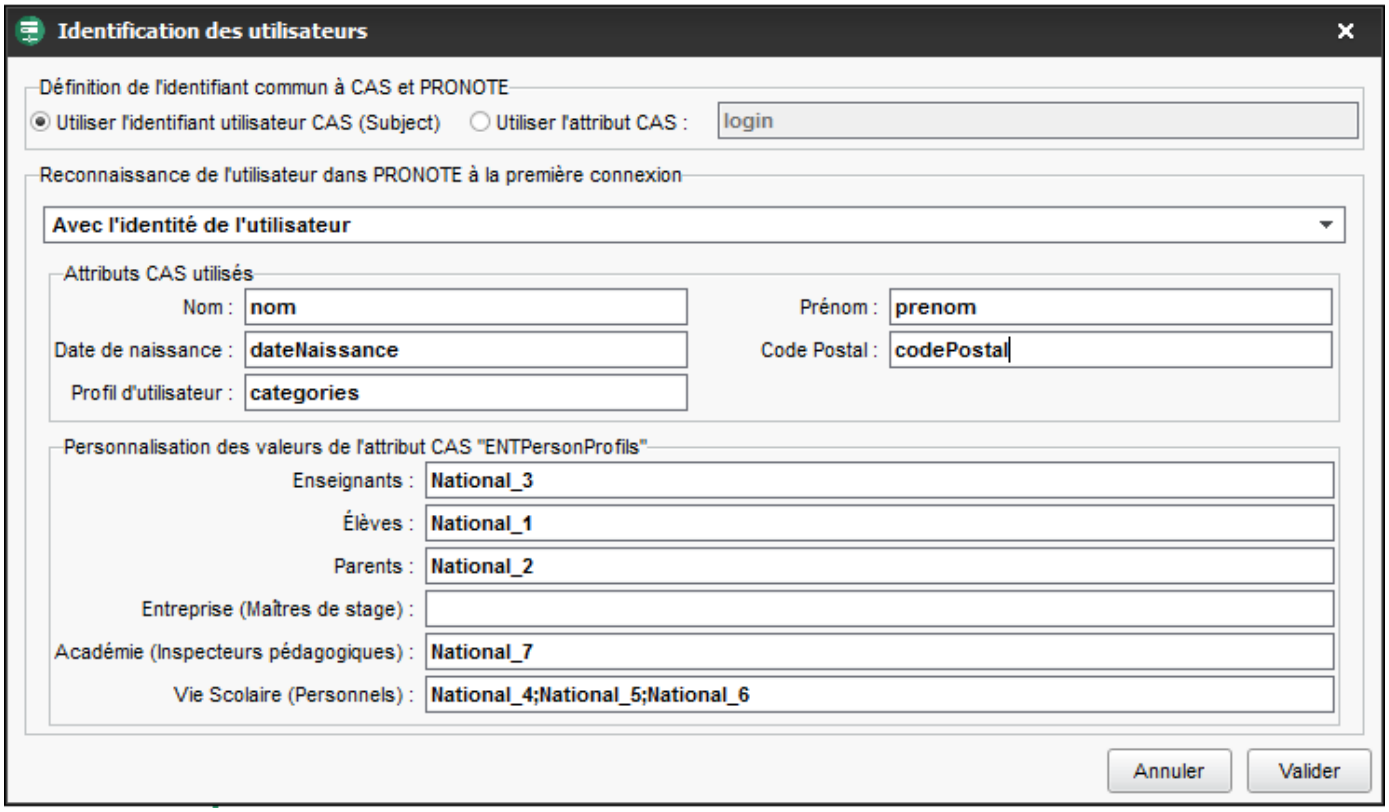
Si le serveur CAS n'était plus accessible ou si un utilisateur est connu de Pronote.net ou de PRONOTE mais pas du serveur CAS, l'accès à l'authentification sans interroger le serveur CAS peut être activé : cela permet d'accéder à Pronote.net comme si l'authentification avec CAS n'était pas activée.

6.3. Paramétrage avancé

Pour le client léger : Pour accéder au paramétrage avancé depuis l'onglet *Intégration dans un ENT > Interconnexion*, il faut cliquer sur le bouton « Paramètres d'identification des utilisateurs ».

Pour le client lourd : Pour accéder au paramétrage avancé depuis l'onglet *Déléguer l'authentification*, il faut cliquer sur le bouton « Paramètres d'identification des utilisateurs ».

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

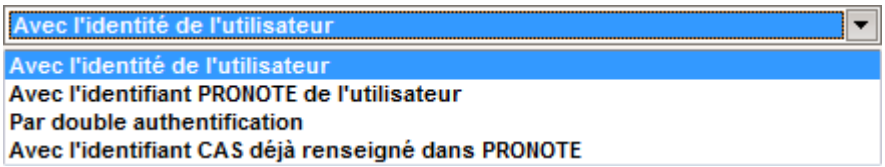


Cela ouvre la rubrique « Identification des utilisateurs » dans laquelle tous les champs sont pré-remplis par défaut (voir ci-dessus) et sont modifiables pour des configurations spécifiques.

Il s'agit d'informations que doit connaître le client CAS pour traiter la réponse SAML du serveur CAS à l'étape 2.4. et entamer l'étape 2.5. La réponse SAML du serveur CAS contient un sujet (« Subject ») et un certain nombre d'attributs, chaque attribut pouvant avoir une ou plusieurs valeurs.

La première information nécessaire est le nom de l'élément (sujet ou attribut CAS) contenant l'identifiant unique de l'utilisateur, l'identifiant CAS : si la réponse SAML spécifie un identifiant CAS connu dans la base PRONOTE, l'authentification se base sur cet identifiant seul.

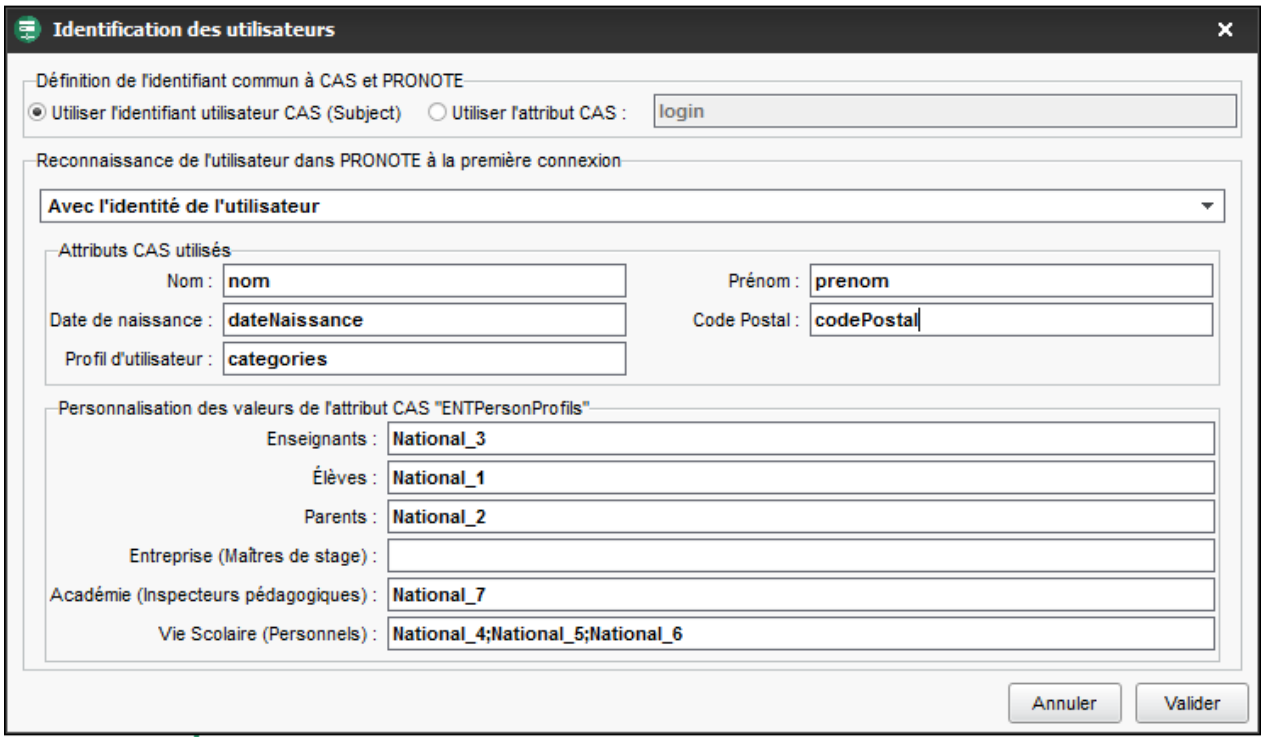
Ensuite il y a le cas particulier de la première connexion à Pronote.net ou à PRONOTE client car il faut mettre en correspondance l'utilisateur tel qu'il est connu du serveur CAS avec un utilisateur de la base PRONOTE[2]. Pour cela, quatre options sont disponibles :



[2] CAS est un système d'authentification unique dit à approche coopérative, c'est à dire que chaque application définit sa propre politique de sécurité.

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

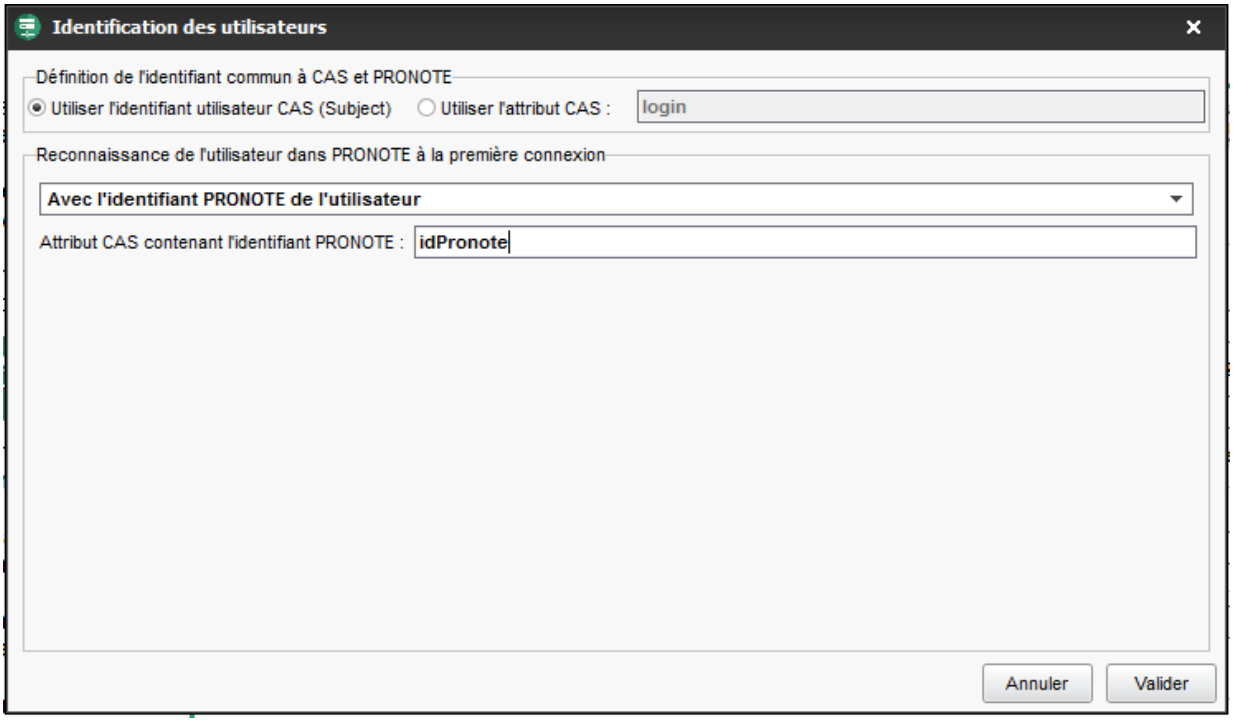
6.3.1. Avec l'identité de l'utilisateur (par défaut)



Pronote.net ou PRONOTE essaie de retrouver l'utilisateur en utilisant d'autres attributs comme le nom, le prénom et la date de naissance.

Le profil d'utilisateur désigne l'attribut qui contient les informations pour déterminer de quel type est l'utilisateur qui demande à se connecter : professeur, élève, parent, etc. C'est typiquement un attribut ayant plusieurs valeurs. Les champs sous *Personnalisation des valeurs de l'attribut CAS [...]* permettent de spécifier l'utilisation de cet attribut : pour chaque espace (Professeurs, Élèves, etc.) est définie une liste de valeurs séparées par des points-virgules. Si l'une des valeurs fait partie des valeurs de l'attribut profil d'utilisateur, alors l'utilisateur peut accéder à l'espace en question. La recherche des utilisateurs dans la base est limitée aux espaces auxquels il peut se connecter.

6.3.2. Avec l'identifiant PRONOTE de l'utilisateur



S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

Ce mode peut être utilisé dans le cas où l'intégrateur a une limitation légale à l'envoi d'informations personnelles qui ne l'autorise pas à communiquer ces informations dans les réponses SAML.

Pour cela, l'échange d'informations personnelles est inversé, c'est PRONOTE qui exporte préalablement les informations sur les utilisateurs avec les identifiants PRONOTE correspondants : l'intégrateur CAS peut ainsi importer les identifiants PRONOTE et les intégrer plus tard dans les réponses SAML, ce qui permet à Pronote.net de retrouver les utilisateurs dès la première connexion.

L'export peut être fait manuellement (depuis le client PRONOTE en mode Administratif). Le schéma de spécifications des données XML exportées (avant chiffrement, voir ci-dessous) est accessible ici :

http://www.index-education.com/contenu/telechargement/partenaires/EchangesIdentifiantsCas.xsd

Sécurité et aspects légaux :

[Pour certains intégrateurs uniquement : Un code de rapprochement fourni par l'intégrateur CAS complète le numéro établissement pour éviter qu'un tiers exporte des données pour un établissement sans en avoir le droit. Les données exportées ne sont lisibles que par l'intégrateur destinataire de ces données. Pour ce faire elles sont chiffrées : le destinataire génère un couple de clés RSA 2048 bits et communique à la société Index-Education la clé publique pour qu'elle soit intégrée au code de PRONOTE. Les données exportées sont alors chiffrées par PRONOTE par la méthode de chiffrement symétrique AES avec une clé AES aléatoire qui est-elle même chiffrée par la méthode RSA avec la clé publique. Le destinataire qui est le seul à détenir la clé privée est le seul à pouvoir lire les données exportées.]

L'intégrateur partenaire s'engage par écrit à ne créer aucun compte mais seulement à établir des correspondances et importer les identifiants PRONOTE.

Le chef d'établissement est le seul responsable juridique des données contenues dans PRONOTE, que PRONOTE soit en mode local ou en mode hébergé. La société Index-Education garantit, en mode hébergé, la stricte confidentialité des données qui lui sont confiées et s'interdit, par contrat de licence d'hébergement, tout accès à ces données.

Stockage d'un identifiant PRONOTE :

L'identifiant PRONOTE est une chaîne dont la taille varie de 5 à 32 caractères (il est éditable dans le client PRONOTE en mode SPR). Quand l'identifiant est généré automatiquement, il fait 16 caractères.

Plusieurs identifiants PRONOTE pour un même utilisateur CAS :

Il peut y avoir des utilisateurs qui apparaissent une fois dans la base de l'intégrateur CAS mais plusieurs fois dans plusieurs bases PRONOTE de plusieurs établissements. L'intégrateur qui décide d'utiliser ce mode doit donc faire en sorte que différents identifiants PRONOTE puissent être associés au même utilisateur pour des établissements différents (table de relation pour une base SQL ou attribut multiple pour une base LDAP).

Dans ce mode, Pronote.net rappelle automatiquement à la requête samlValidate (étape 2.4.) le paramètre CODE_ETABLISSEMENT déjà spécifié à l'export des identifiants PRONOTE afin de permettre au serveur CAS de déterminer quel identifiant PRONOTE renvoyer.

Utilisateurs multi-profils :

De même un utilisateur peut apparaitre une fois dans la base de l'intégrateur CAS mais plusieurs fois dans une même base PRONOTE (c'est le cas d'un enseignant qui est aussi parent d'élève). Il faut alors qu'un administrateur se connecte à la base PRONOTE en SPR et affecte le même identifiant PRONOTE aux différents utilisateurs PRONOTE.

Les identifiants PRONOTE générés automatiquement par PRONOTE sont uniques dans toute la base. Les utilisateurs multi-profils sont le seul cas où les identifiants PRONOTE sont partagés et cela ne peut résulter que d'une opération manuelle d'un administrateur de la base de données de l'établissement.

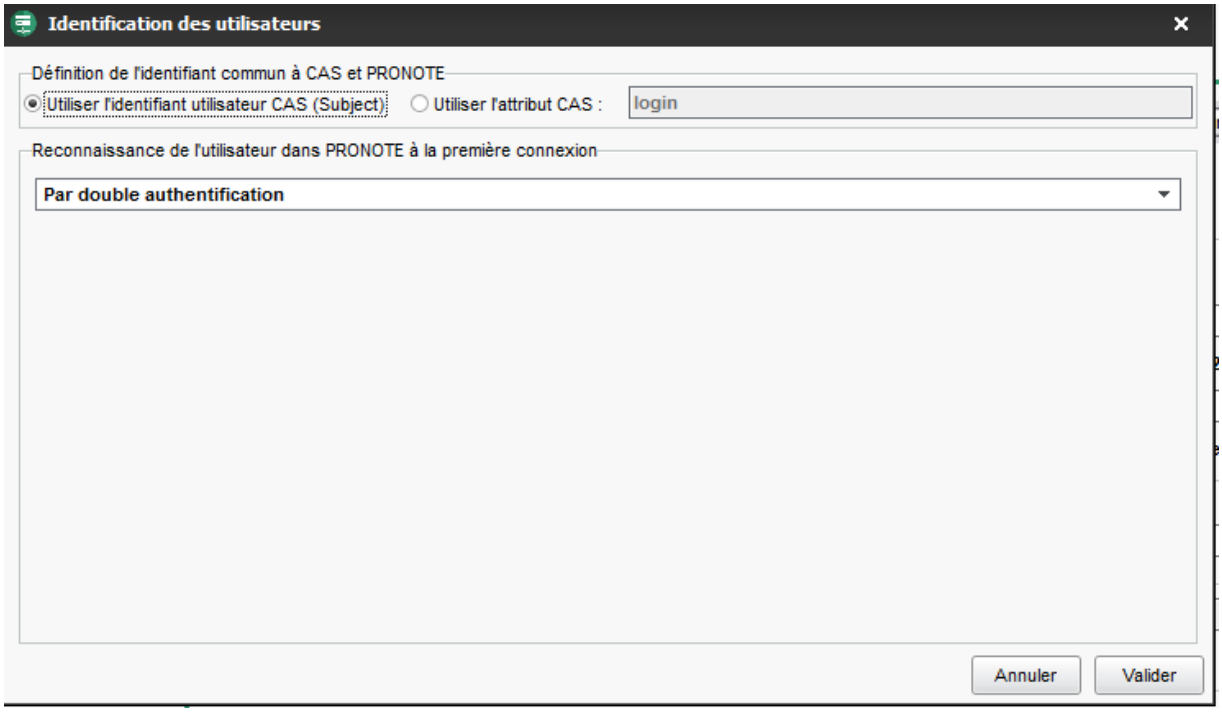
Changement d'année scolaire :

Au changement d'année scolaire, on ne peut pas présumer que les identifiants PRONOTE seront conservés : certains clients modifient la base de l'année précédente, d'autres partent d'une nouvelle base vide et ceux qui utilisent également notre logiciel d'emploi du temps EDT peuvent créer une nouvelle base à partir d'EDT.

S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

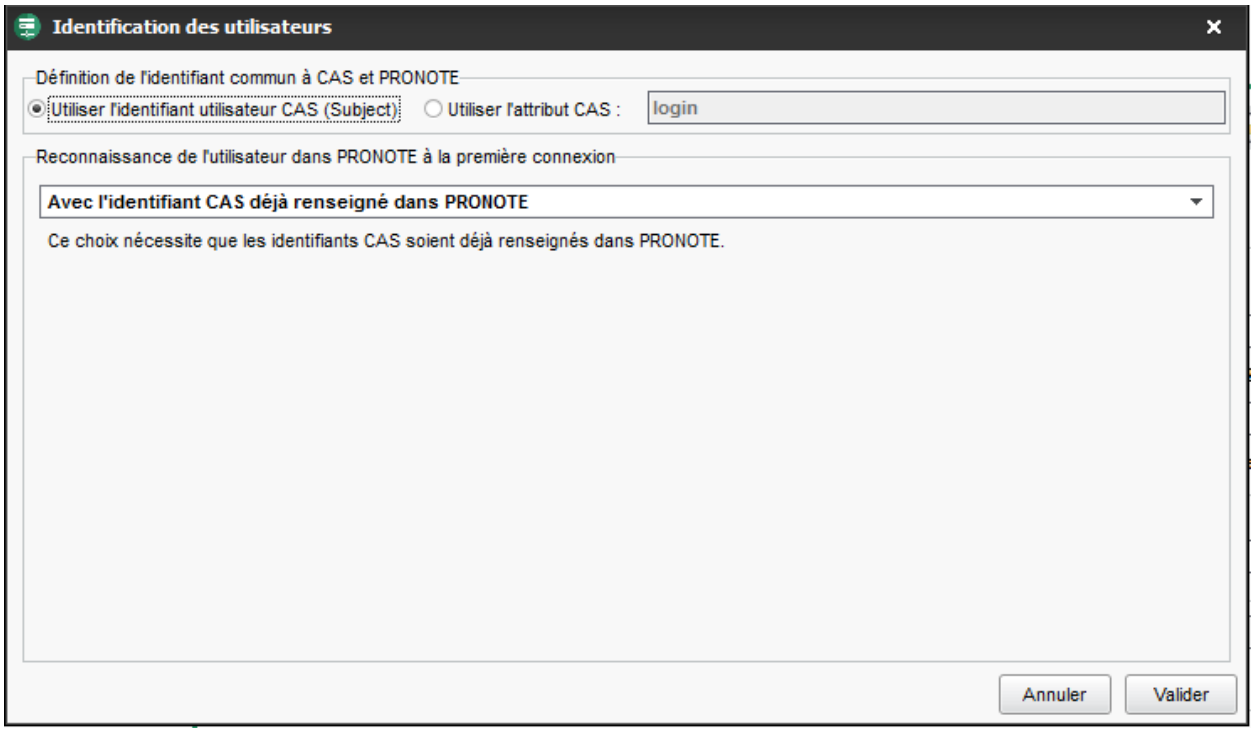
Dans la nouvelle base, les identifiants PRONOTE peuvent donc être différents. Il est recommandé aux intégrateurs CAS de supprimer de leur base à la rentrée scolaire tous les identifiants PRONOTE importés l'année précédente. À noter que si la base est créée à partir de celle de l'année précédente, les identifiants CAS des utilisateurs qui se sont déjà connectés sont conservés et l'authentification avec CAS doit fonctionner directement.

6.3.3. Via la page de connexion des Espaces Pronote.net ou depuis le client PRONOTE



Il y a alors double authentification à la première connexion : authentification par le serveur CAS puis authentification par Pronote.net ou par le client lourd PRONOTE. Cette option, plus compliquée pour l'utilisateur, permet d'éviter tout échange d'informations personnelles entre le serveur CAS et Pronote.net ou PRONOTE.

6.3.4. Refuser l'accès si l'identifiant CAS n'est pas renseigné dans PRONOTE



S.A.S au capital de 292 000 € / RCS Marseille B 384 351 599 / Siret 384 351 599 00079 / CODE APE 5829 C / TVA Intracommunautaire FR 95 384 351 599

Dans ce mode, il n'y a aucune tentative pour trouver l'utilisateur si l'identifiant CAS reçu est inconnu dans la base. Les identifiants CAS doivent être préalablement renseignés par l'utilisateur SPR dans la base PRONOTE, soit par import soit par saisie dans PRONOTE client[3].

6.4. Bouton[4] « Tester l'authentification par le serveur CAS »

Ce bouton fait apparaître une nouvelle interface avec un navigateur embarqué (un objet WebBrowser qui est en fait Internet Explorer dont la disponibilité n'est prévue que lorsque le serveur Pronote.net est publié). Il permet d'effectuer les étapes 2.1. à 2.4. décrites ci-dessus en affichant le détail de toutes les navigations et redirections qui se produisent, ce qui permet de résoudre les problèmes de configuration et/ou de connexion. Il est possible de sélectionner le résultat pour le copier ailleurs.

7. Informations à transmettre à l'administrateur du serveur CAS

Il y a deux informations à transmettre à l'administrateur CAS :

- L'url de Pronote.net ou de PRONOTE client pour le serveur CAS, cette url peut être copiée depuis l'onglet *Intégration dans un ENT > Interconnexion* de l'interface graphique d'administration du serveur Pronote.net ou depuis l'onglet Déléguer l'authentification de l'interface graphique d'administration du serveur PRONOTE (= url à communiquer au socle ENT).
- Le nom des attributs attendus dans la réponse SAML. Dans le mode par défaut *Reconnaissance de l'utilisateur dans PRONOTE à la première connexion = Avec l'identité de l'utilisateur*, il s'agit de « nom », « prenom », « dateNaissance », « codePostal », et « categories ». Si en retour l'administrateur signale que dans son architecture ces attributs ont des noms différents, il faut les spécifier dans l'interface de paramétrage avancé décrite à la section 5.3.1. Attention aux différences majuscules/minuscules : l'attribut « codePostal » ne sera pas reconnu s'il est écrit « CodePostal ».

8. Single Sign Out

Dans les protocoles CAS 1.0 et 2.0 (http://www.jasig.org/cas/protocol), il n'existe pas de requête de déconnexion issue du serveur CAS vers les clients CAS connectés. Il n'y a d'ailleurs jamais de connexion ouverte par le serveur CAS vers les clients CAS. Ainsi, les clients ne sont pas notifiés d'une déconnexion effectuée auprès du serveur CAS, c'est juste qu'il n'y a plus les paramètres d'authentification unique, de sorte que, lorsqu'une nouvelle authentification est nécessaire, la page d'authentification du serveur CAS est affichée.

Mais à côté du protocole CAS, il existe un autre protocole appelé *Single Sign Out* (https://wiki.jasig.org/display/CASUM/Single+Sign+Out) implémenté par la plupart des clients CAS récents, et qui permet au serveur CAS de leur notifier une déconnexion.

PRONOTE et Pronote.net n'implémentent pas ce protocole et la société Index-Education a décidé qu'il ne le sera pas. En effet, ni PRONOTE ni Pronote.net ne sont en soi des modules CAS mais bien des applications tierces pouvant être intégrées dans un environnement CAS pour la phase initiale d'authentification.

Ainsi, si un utilisateur se déconnecte du serveur CAS après l'ouverture de la session PRONOTE ou Pronote.net, la session n'est pas interrompue. Par contre, pour Pronote.net seulement, si à un moment donné l'utilisateur appuie sur F5 pour mettre à jour son navigateur ou fait quelque action nécessitant un rechargement de la page, il y aura bien une nouvelle demande d'authentification. À noter que la façon la plus sûre de mettre fin à tous les clients CAS d'une session CAS est de fermer le navigateur. La page de déconnexion des serveurs CAS présente d'ailleurs souvent un message demandant à l'utilisateur de fermer le navigateur pour plus de sécurité.

[3] Les identifiants CAS sont modifiables au travers de PRONOTE client pour l'utilisateur SPR à condition d'activer la gestion des identifiants PRONOTE et CAS dans les préférences d'affichage.

[4] Fonctionnalité de test uniquement disponible dans l'interface graphique du serveur Pronote.net.