

RAPPORT

Secrétariat général

Service des Politiques  
support et des  
Systèmes d'Information

Centre de prestations  
et d'Ingénierie  
Informatique

Département  
Opérationnel  
de l'Ouest

Février 2016

# DESCRIPTION DU PLUGIN D'AUTHENTIFICATION AVEC CAS POUR SPIP

C.Imberti – version modifiée le 01/02/2016



MINISTÈRE  
DE L'ÉGALITÉ DES TERRITOIRES  
ET DU LOGEMENT  
[www.territoires.gouv.fr](http://www.territoires.gouv.fr)

MINISTÈRE DE L'ÉCOLOGIE,  
DU DÉVELOPPEMENT DURABLE  
ET DE L'ÉNERGIE  
[www.developpement-durable.gouv.fr](http://www.developpement-durable.gouv.fr)

## Historique des versions du document

---

Version	Date	Commentaires
1	12/02/2010	
1.1	23/06/2010	Modification de l'annexe
1.2	19/12/2013	Ajout d'un chapitre dans l'annexe
1.3	01/02/2016	Ajout de la possibilité de créer un auteur à la volée. Ajout de la possibilité d'offrir à l'utilisateur le choix entre plusieurs serveurs CAS. Ajout d'une sécurité anti BOT (optionnelle).

## Auteur du document

---

Christophe IMBERTI - SG/SPSSI/CP2I/DO Ouest

## Sommaire

---

<b>1. PRESENTATION .....</b>	<b>4</b>
1.1 Rappel sur le Single Sign-On avec CAS .....	4
1.2 Les objectifs de ce plugin .....	4
1.3 Les fonctionnalités de ce plugin .....	4
1.4 Compatibilité.....	4
<b>2. CONFIGURATION .....</b>	<b>5</b>
<b>3. UTILISATION .....</b>	<b>6</b>
3.1 Authentification CAS .....	6
3.2 Authentification Hybride .....	6
<b>4. ANNEXE.....</b>	<b>7</b>
4.1 Installation .....	7
4.2 Offrir à l'utilisateur le choix entre plusieurs serveurs CAS .....	7
4.3 Fichier de paramétrage optionnel .....	10
4.4 Pouvoir utiliser une URL spécifique lorsque le plugin interroge le serveur CAS.....	11

# 1. Présentation

Le plugin « cicas » permet d'utiliser un serveur SSO (Single Sign-On), basé sur CAS (Central Authentication Service), pour s'authentifier dans SPIP 2.0.

## 1.1 Rappel sur le Single Sign-On avec CAS

Une présentation sur le Single Sign-On avec CAS a été rédigée, par les auteurs du client PHP pour CAS (phpCAS), à l'adresse suivante : <http://perso.univ-rennes1.fr/pascal.aubry/node/29>

## 1.2 Les objectifs de ce plugin

L'objectif est d'utiliser le login et le mot de passe stocké dans le serveur d'authentification au lieu de ceux qui sont stockés dans SPIP. Cela évite à l'utilisateur de gérer ses mots de passe dans plusieurs sites (ou applications) et cela lui évite de s'authentifier à nouveau lorsqu'il passe d'un site à un autre.

## 1.3 Les fonctionnalités de ce plugin

On peut paramétrer ce plugin pour offrir une **authentification CAS ou bien une authentification hybride** (SPIP ou CAS). Dans ce dernier cas, chaque fois qu'il souhaitera s'authentifier, l'utilisateur pourra choisir soit de s'authentifier comme d'habitude avec SPIP, soit de cliquer sur le lien « Utiliser l'authentification centralisée » pour s'authentifier avec CAS.

Par paramétrage on peut choisir de comparer l'identifiant renvoyé par le serveur CAS au contenu du champ de SPIP contenant l'email des auteurs, ou bien à celui contenant le login des auteurs.

Si plusieurs auteurs ont, dans SPIP, le même email, il est nécessaire de savoir lequel retenir. Aussi, parmi les auteurs disposant du même email, celui qui a le plus de droits dans SPIP sera retenu. Si deux auteurs ont les mêmes droits, le premier par ordre alphabétique de nom d'auteur dans SPIP, sera retenu. Les auteurs dont le statut est « à la poubelle » ne seront jamais pris en compte.

L'authentification sur le site public redirige ensuite vers la page en cours, idem lors de la déconnexion.

On peut configurer le plugin pour que, si l'authentification sur ce serveur CAS a réussi mais que l'auteur n'existe pas dans SPIP, l'auteur soit créé automatiquement (avec le statut "rédacteur" ou bien "visiteur").

Un **paramétrage par fichier est possible**. Il est prioritaire sur le paramétrage du plugin dans l'espace privé. Cela facilite le déploiement sur un grand nombre de sites.

Si un site est publié simultanément sur deux réseaux (par exemple intranet et internet) et que l'on veut pouvoir s'authentifier sur le site dans les deux cas, il peut être souhaitable que le serveur CAS soit accessible sur intranet et sur internet. Aussi, il convient de déterminer la provenance de l'auteur (intranet, internet, ...) et d'aiguiller automatiquement sur l'adresse corrélative du serveur CAS (intranet, internet, ...). Cette possibilité est offerte uniquement via le paramétrage par fichier.

Il est possible d'offrir à l'utilisateur le choix entre plusieurs serveurs CAS (cf. annexe).

Il est possible d'activer une sécurité anti BOT (cf. annexe).

## 1.4 Compatibilité

Le plugin est compatible avec SPIP 2.0, SPIP 2.1, SPIP 3.0 et SPIP 3.1. Il surcharge une seule fonction (« logout »).

Il est compatible avec PHP 5.4.

## 2. Configuration

La configuration s'effectue dans le menu [Configuration] de SPIP, sous menu [Configurer CAS] :

### Configuration du plugin cicas

#### Mode d'authentification

**ATTENTION** : Il est impératif sélectionner en premier (ci-dessous) le mode d'authentification intitulé "CAS ou SPIP" afin de vérifier, sans risque, le bon fonctionnement de l'authentification CAS. Une fois cette vérification effectuée on pourra alors sélectionner (ci-dessous) le mode d'authentification intitulé "CAS".

CAS  
 CAS ou SPIP  
 SPIP

Enregistrer

#### Configuration du serveur CAS

URL du serveur CAS

Repertoire du serveur CAS

Port du serveur CAS

Identifiant utilisateur fournit par le serveur CAS

Si l'authentification sur ce serveur CAS a réussi mais que l'auteur n'existe pas dans SPIP, faut-il le créer automatiquement ?

Enregistrer

Il est **impératif** sélectionner en premier le mode d'authentification intitulé "CAS ou SPIP" afin de vérifier, sans risque, le bon fonctionnement de l'authentification CAS.

Il convient de renseigner l'adresse du serveur CAS (sans la faire précéder de http://), le répertoire éventuel du serveur CAS (par exemple : /cas) et le port du serveur CAS (en général : 443).

Si l'identifiant renvoyé par le serveur CAS est l'email de l'auteur, il est **nécessaire** de s'assurer que, dans SPIP, l'email de chaque auteur est bien renseignée.

On peut configurer le plugin pour que, si l'authentification sur ce serveur CAS a réussi mais que l'auteur n'existe pas dans SPIP, l'auteur soit créé automatiquement avec le statut rédacteur ou visiteur. Il est possible d'offrir à l'utilisateur le choix entre plusieurs serveurs CAS (cf. annexe).

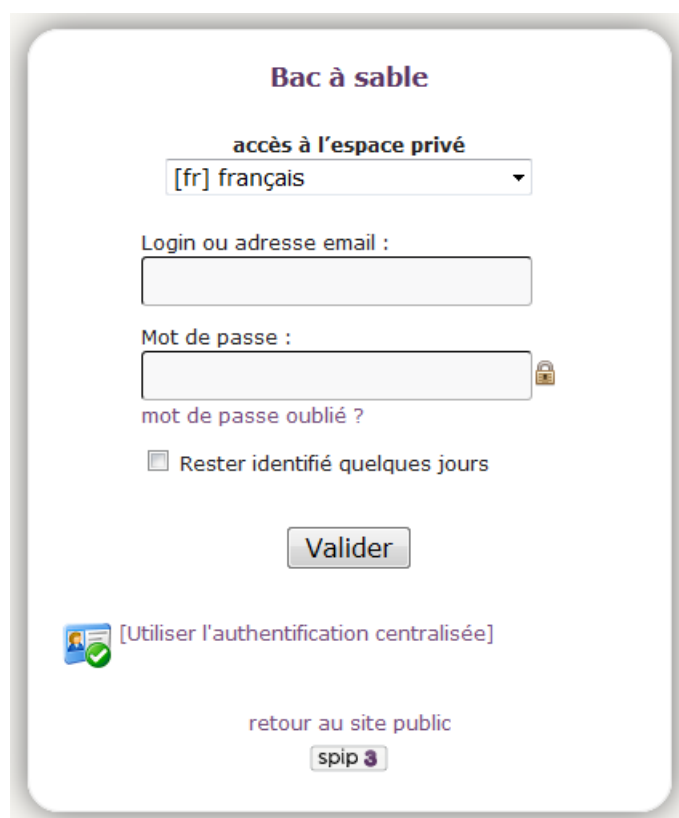
## 3. Utilisation

### 3.1 Authentification CAS

Au lieu d'accéder au formulaire d'authentification de SPIP, l'utilisateur est redirigé vers le formulaire d'authentification du serveur CAS.

### 3.2 Authentification Hybride

Le plugin ajoute un lien « Utiliser l'authentification centralisée » dans le formulaire d'authentification de SPIP.



The screenshot shows a login form titled "Bac à sable". At the top, it says "accès à l'espace privé" with a dropdown menu currently set to "[fr] français". Below this are two input fields: "Login ou adresse email :" and "Mot de passe :". The password field has a lock icon on the right. Under the password field, there is a link "mot de passe oublié ?" and a checkbox labeled "Rester identifié quelques jours". A "Valider" button is centered below these options. At the bottom left, there is a link with a user icon and a green checkmark: "[Utiliser l'authentification centralisée]". At the bottom center, there is a link "retour au site public" and the SPIP logo.

Chaque fois qu'il souhaitera s'authentifier, l'utilisateur pourra choisir soit de s'authentifier comme d'habitude avec SPIP, soit de cliquer sur le lien « Utiliser l'authentification centralisée » pour s'authentifier avec l'authentification centralisée.

## 4. Annexe

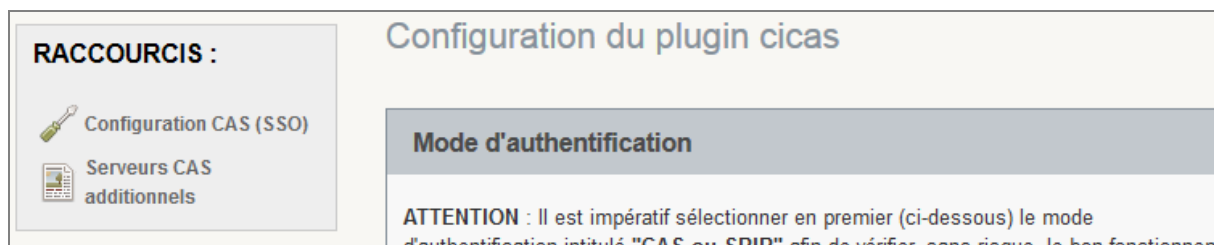
### 4.1 Installation

Le plugin « cicas » s'installe comme tous les plugins, cf. [http://www.spip.net/fr\\_article3396.html](http://www.spip.net/fr_article3396.html)  
Il contient le client phpCAS, ce qui évite de devoir installer ce dernier.

### 4.2 Offrir à l'utilisateur le choix entre plusieurs serveurs CAS

#### 4.2.1 Configuration d'un serveur CAS additionnel

Dans le menu [**Configuration**] de SPIP, sous menu [**Configurer CAS**], il convient de cliquer, dans la colonne de gauche, sur le lien "Serveurs CAS additionnels" :



La page suivante s'affiche :



En cliquant sur le bouton [Ajouter un serveur], on obtient le formulaire dont une copie d'écran figure page suivante.

## Serveur CAS additionnel

Retour

URL du serveur CAS

Repertoire du serveur CAS

Port du serveur CAS

Identifiant utilisateur fourni par le serveur CAS

Si l'authentification sur ce serveur CAS a réussi mais que l'auteur n'existe pas dans SPIP, faut-il le créer automatiquement ?

Supprimer ce serveur additionnel

La configuration d'un serveur additionnel s'effectue comme pour le serveur principal (cf. chapitre 2). Lorsque l'on clique sur le bouton [Enregistrer], le serveur apparaît dans la liste des serveurs CAS additionnels :

### Serveurs CAS additionnels

Il est possible d'ajouter des serveurs CAS additionnels. Si l'authentification sur le serveur CAS échoue, le plugin tentera l'authentification sur le premier serveur CAS additionnel (si elle échoue également, le plugin tentera l'authentification sur le second serveur CAS additionnel, etc.).

**Serveurs CAS additionnels**

Aucun serveur additionnel n'est présent

Ajouter un serveur

Pour modifier un serveur CAS additionnel, il suffit de cliquer dessus dans la liste ci-dessus.

Pour supprimer un serveur CAS additionnel, il convient de cliquer dessus dans la liste ci-dessus, puis de cliquer sur le bouton [Supprimer ce serveur additionnel].



#### 4.2.2 Utilisation avec de serveurs CAS additionnels

En mode "Authentification CAS", le serveur CAS principal et les serveurs CAS additionnels sont proposés à l'utilisateur lorsqu'il veut se connecter.

**Nom du site**

Vous pouvez vous authentifier avec l'un des serveurs d'authentification suivant (si vous ne savez pas lequel choisir, cliquer d'abord sur le premier) :

 [authentification-cerbere.application.i2] [Mémoriser ce choix](#)

 [identification.agriculture.gouv.fr] [Mémoriser ce choix](#)

[\[retour au site public\]](#)

En mode "Authentification Hybride", le serveur CAS principal et les serveurs CAS additionnels sont proposés à l'utilisateur dans le formulaire d'authentification de SPIP.

**Nom du site**

**accès à l'espace privé**

[fr] français ▼

Login ou adresse email :

Mot de passe :  
 

[mot de passe oublié ?](#)

Rester identifié quelques jours

Vous pouvez vous authentifier avec l'un des serveurs d'authentification suivant (si vous ne savez pas lequel choisir, cliquer d'abord sur le premier) :

 [authentification-cerbere.application.i2] [Mémoriser ce choix](#)

 [identification.agriculture.gouv.fr] [Mémoriser ce choix](#)

[retour au site public](#)



Remarque : Le lien "Mémoriser ce choix" pose un cookie qui évitera à l'utilisateur de choisir à nouveau lors de sa prochaine connexion.

### 4.3 Fichier de paramétrage optionnel

Un **paramétrage par fichier est possible**. Il est prioritaire sur le paramétrage du plugin dans l'espace privé. Cela facilite le déploiement sur un grand nombre de sites.

Nom du fichier : `racine_du_site/config/_config_cas.php`

Le fichier doit être situé dans le dossier « config » de SPIP.

Exemple de contenu du fichier :

```
<?php
/* -----
Paramètres de configuration pour CAS :

Exemple :
// pour une authentification avec CAS mettre 'oui',
// pour une authentification hybride CAS ou SPIP mettre 'hybride',
// sinon authentification SPIP
$GLOBALS['ciconfig']['cicas'] = 'hybride';

// si l'identifiant est stocké dans le champ login de la table auteur
// mettre 'login' (sinon la recherche sera effectuée dans le champs email)
$GLOBALS['ciconfig']['cicasuid'] = '';

// URL du serveur CAS (adresse utilisée par défaut)
// cet exemple est fictif car l'adresse urlcas.i2 n'existe pas
$GLOBALS['ciconfig']['cicasurldefaut'] = 'urlcas.i2';

// repertoire du serveur CAS (le cas échéant)
$GLOBALS['ciconfig']['cicasrepertoire'] = '/cas';

// port du serveur CAS (si non renseigne, la valeur par default est '443')
$GLOBALS['ciconfig']['cicasport'] = '443';

// Pour que l'auteur soit cree automatiquement (si l'authentification CAS a reussi
// mais que l'auteur n'existe pas dans SPIP), mettre 'lcomite' ou '6forum' (si la
// variable n'est pas declaree ou contient '', l'auteur ne sera pas cree)
$GLOBALS['ciconfig']['cicas_creer_auteur'] = '';

// tableau des autres URLs du serveurs CAS selon le type de terminaison de l'adresse
// d'appel du site SPIP. L'ordre donné dans cet exemple est important, car c'est
// l'ordre d'examen des terminaisons
$GLOBALS['ciconfig']['cicasurls'] = array('.ader.gouv.fr' => 'urlcas.ader.gouv.fr',
'.gouv.fr' => 'urlcas.ministere.gouv.fr',);

// compatibilité avec les anciennes adresses email
// domaine email dans la table des auteurs de SPIP => domaine email renvoye par CAS
$GLOBALS['ciconfig']['cicasmailcompatible'] = array('equipement.gouv.fr' =>
'developpement-durable.gouv.fr');

// Par default, l'ordre de recherche du HOST dans les variables HTTP est celui de
// phpCAS, c'est a dire : 'HTTP_X_FORWARDED_SERVER', 'SERVER_NAME', 'HTTP_HOST'
// Si l'hebergeur n'est pas compatible avec l'ordre de phpCAS, on peut definir
// l'ordre a prendre en compte.
$GLOBALS['ciconfig']['cicashostordre'] =
array('HTTP_X_FORWARDED_SERVER', 'SERVER_NAME', 'HTTP_HOST');

// Pouvoir utiliser une URL spécifique lorsque le plugin interroge le serveur CAS
$GLOBALS['ciconfig']['cicas_svu_url'] = 'urlcas.i2';
$GLOBALS['ciconfig']['cicas_svu_repertoire'] = '/cas';
$GLOBALS['ciconfig']['cicas_svu_port'] = '443';

// Pouvoir ajouter des serveurs CAS additionnels
$GLOBALS['ciconfig']['cicas_serveurs_additionnels']= array(
1=>array('cicasurldefaut' => 'url-cas-serveur-additionnel1', 'cicasrepertoire'=>
'/cas', 'cicasport'=>'443', 'cicasuid'=>'', 'cicas_creer_auteur'=>'6forum')
2=>array('cicasurldefaut' => 'url-cas-serveur-additionnel2', 'cicasrepertoire'=>
'/cas', 'cicasport'=>'443', 'cicasuid'=>'', 'cicas_creer_auteur'=>'6forum')
);
----- */
```

```

$GLOBALS['ciconfig']['cicas'] = 'hybride';
$GLOBALS['ciconfig']['cicasuid'] = '';
$GLOBALS['ciconfig']['cicasurldefault'] = 'urlcas.i2';
$GLOBALS['ciconfig']['cicasrepertoire'] = '/cas';
$GLOBALS['ciconfig']['cicasurls'] = array('.ader.gouv.fr' => 'urlcas.ader.gouv.fr',
'.gouv.fr' => 'urlcas.ministere.gouv.fr');
$GLOBALS['ciconfig']['cicasport'] = '443';
?>

```

#### 4.4 Sécurité anti BOT

Lorsqu'un BOT souhaite accéder au formulaire d'authentification, il est possible de le rediriger vers la page "403" (accès interdit). Pour cela, il convient de placer la constante `_CICAS_ANTI_BOT` dans un fichier d'options (le fichier `config/mes_options.php` ou bien le fichier d'options d'un autre plugin), avec la valeur 'oui', comme ci-dessous :

```
define('_CICAS_ANTI_BOT', 'oui');
```

Remarque : C'est le détecteur de robot d'indexation de SPIP qui est utilisé (et qui est personnalisable dans le fichier `mes_options.php`).

#### 4.5 Pouvoir utiliser une URL spécifique lorsque le plugin interroge le serveur CAS

Prenons le cas d'un site Internet sur lequel on souhaite que des Internautes puissent s'authentifier.

Lorsqu'un Internaute veut s'authentifier, il est redirigé vers formulaire d'authentification sur le serveur CAS. Lors de la validation du formulaire d'authentification, l'Internaute est redirigé vers SPIP (avec un ticket dans l'URL) et SPIP va (via le client phpCAS qui est livré avec le plugin CICAS) interroger le serveur CAS (avec ce ticket) afin de savoir si l'utilisateur s'est authentifié et, si c'est le cas, obtenir l'identifiant de l'utilisateur.

Pour plus de détails sur le fonctionnement de CAS : <http://perso.univ-rennes1.fr/pascal.aubry/node/29>

Aussi, dans le cas précité, SPIP est amené à interroger l'adresse Internet du serveur CAS.

Si on souhaite éviter que cette interrogation passe par Internet et si le serveur CAS dispose également d'une adresse INTRANET accessible par SPIP, il peut être intéressant d'utiliser cette adresse INTRANET pour cette interrogation.

Le client PHP pour CAS (phpCAS), qui est livré avec le plugin, offre la possibilité d'utiliser une adresse pour le serveur CAS et une autre adresse lors de la validation du ticket, c'est-à-dire lorsque SPIP va interroger le serveur CAS.

La version 1.6 du plugin CICAS permet d'exploiter cette possibilité, via trois variables à ajouter dans le fichier de paramétrage (cf. chapitre 4.3). Ces trois variables sont les suivantes :

```

// URL spécifique lorsque le plugin interroge le serveur CAS
$GLOBALS['ciconfig']['cicas_svu_url'] = 'urlcas.i2';

// Répertoire de l'URL spécifique (le cas échéant)
$GLOBALS['ciconfig']['cicas_svu_repertoire'] = '/cas';

// Port de l'URL spécifique (si non renseigné, la valeur par défaut est '443')
$GLOBALS['ciconfig']['cicas_svu_port'] = '443';

```

Remarques :

- **Cet exemple est fictif** car l'adresse `urlcas.i2` n'existe pas.
- L'acronyme « svu » signifie « `service_validate_url` » qui est une expression utilisée par phpCAS.
- Pour éviter de perturber la plupart des administrateurs de site, le paramétrage de cette URL spécifique est possible uniquement dans le fichier de paramétrage, et pas dans le formulaire de configuration du plugin.