Mise en place du SSO pour le produit **AIRS Dossier**

Digitech

Version 3.0, 05/04/2022

Sommaire

1. Introduction . . . 2
2. Paramétrage et mise en œuvre SSO Kerberos pour Dossier . . . 3
2.1. Création d'un compte Kerberos . . . 3
2.2. Association du compte Kerberos à un SPN . . . 4
2.3. Contrôle de l'existence des associations . . . 5
2.4. Création d'une association (ou d'un service) . . . 5
2.5. Génération du **"keytab"** . . . 6
2.6. Test du paramétrage . . . 6
2.7. Association avec l'application Dossier . . . 7
3. Activation Kerberos dans le navigateur des utilisateurs . . . 8
3.1. Internet Explorer . . . 8
3.2. Firefox . . . 8
4. Annexes . . . 9
4.1. Authenfication auprès d'un serveur Linux Kerberos MIT . . . 9
4.1.1. Sur le serveur . . . 9
4.1.2. Sur le poste client . . . 11
4.2. Erreurs courantes . . . 12
4.2.1. Failure unspecified at GSS-API level . . . 12

Table 1. Notes de suivi

Date	Version	Etat	Objet	Rédacteur	Validateur
02/11/2011	1.0	Validé	Création du document	Régis Krawezyk	
01/08/2019	2.0	Validé	Modification du document	Nicolas Félix	
05/04/2022	3.0	Validé	Dossier **8.0**	Nicolas Félix	

1. Introduction

L'authentification unique (en anglais **S**ingle **S**ign-**O**n ou SSO) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à son poste de travail ainsi qu'aux applications.

Sans SSO, à chaque accès à la page d'accueil de Dossier, l'utilisateur doit d'abord entrer ses **login** et **mot de passe**, que l'application utilise pour ouvrir une session Dossier.

Avec SSO, le navigateur transmet automatiquement à l'application le nom que l'utilisateur a saisi pour s'authentifier lors de l'ouverture de sa session Windows. Dès lors, l'application réceptionne le nom et vérifie sa validité auprès du serveur d'authentification,avant de l'autoriser ou non à accéder à l'application.

Ce document décrit le paramétrage nécessaire pour intégrer Dossier au sein d'un domaine géré par Active Directory (SSO de type Kerberos). En annexe est décrite la même procédure avec une authentification réalisée par un serveur Kerberos sous Linux.

2. Paramétrage et mise en œuvre SSO Kerberos pour Dossier

L'authentification unique (en anglais *S*ingle *S*ign-*O*n ou SSO) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à son poste de travail ainsi qu'aux applications.

Sans SSO, à chaque accès à la page d'accueil de Dossier, l'utilisateur doit d'abord entrer ses login et mot de passe, afin d'ouvrir une session Dossier. Avec SSO, le navigateur transmet automatiquement à l'application le nom que l'utilisateur a saisi pour s'authentifier lors de l'ouverture de sa session Windows. Dès lors, l'application réceptionne le nom et vérifie sa validité auprès du serveur d'authentification, avant de l'autoriser ou non à accéder à l'application.

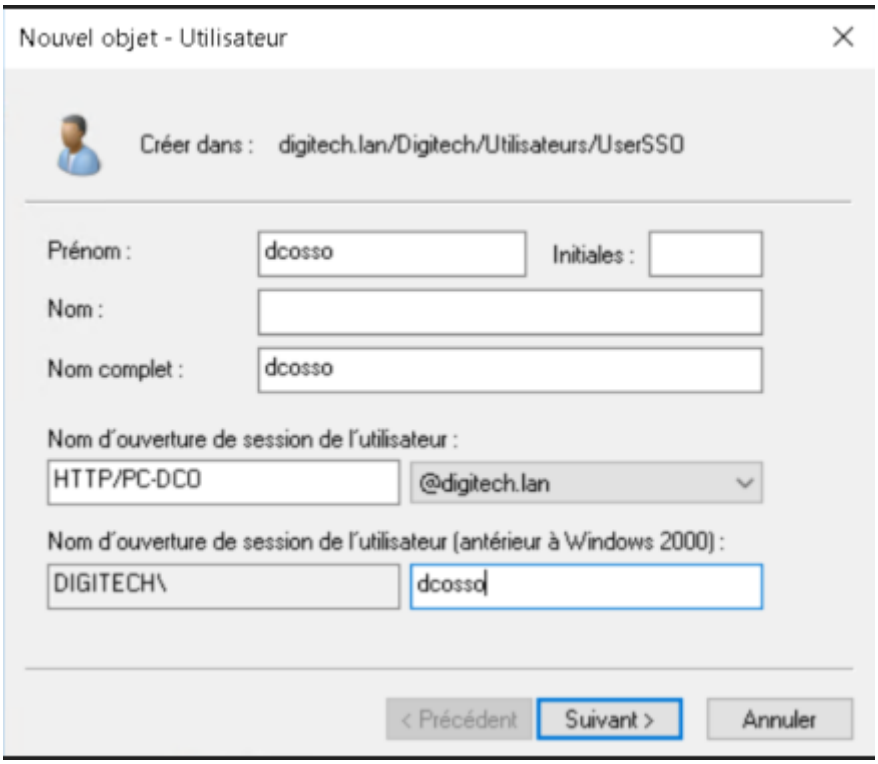
Ce document décrit le paramétrage nécessaire pour intégrer Dossier au sein d'un domaine géré par Active Directory (SSO de type Kerberos). En annexe est décrite la même procédure avec une authentification réalisée par un serveur Kerberos sous Linux.

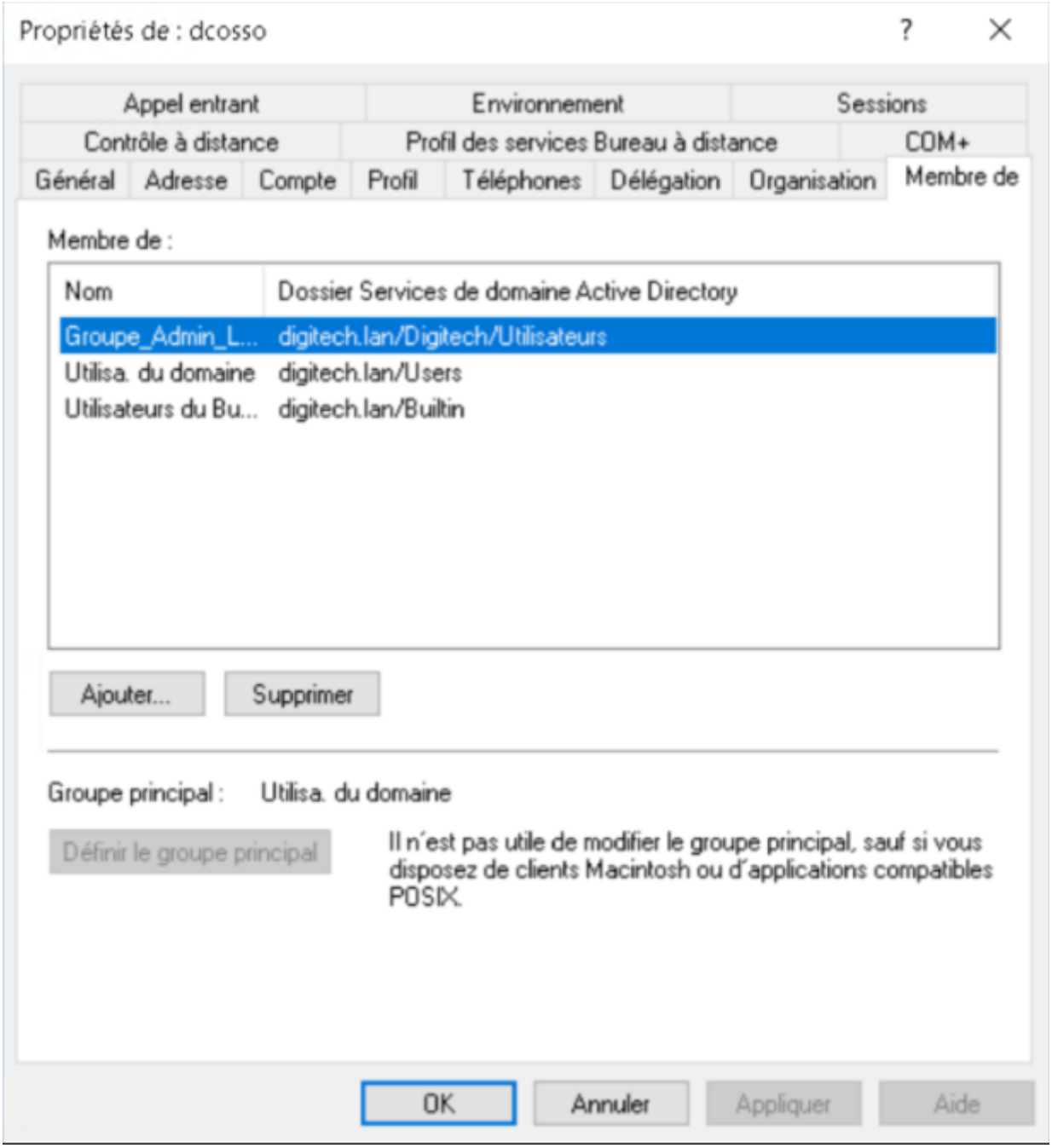
Ce chapitre se découpe en plusieurs parties qui sont liées à des types d'opérations distinctes nécessaires à la mise en œuvre de ce mode de fonctionnement.

- Définition d'un compte Kerberos (Dans l'exemple ci-dessous, ce sera un compte AD)
- Association du compte Kerberos à un SPN (Service Principal Name)
- Association du service avec l'application Dossier

2.1. Création d'un compte Kerberos

Dans notre exemple, il s'agit d'ajouter un compte sur un **AD** :





Dans cet exemple a été créé l'utilisateur `dcosso` au sein de l'**Active Directory** (association avec une machine et un domaine) et son ajout comme membre de `Groupe_Admin_Local`.

2.2. Association du compte Kerberos à un SPN

Il est très déconseillé d'utiliser un compte Kerberos déjà existant afin de l'utiliser, sur une même machine, pour mettre en place le principe de connexion SSO sur une autre application telle que Dossier.

Nous conseillons donc, soit de définir un nouveau compte, soit de supprimer les associations existantes. À savoir que les opérations de création et/ou modification des associations existantes ne peuvent être réalisées que par l'administrateur système au sein de l'organisation.

2.3. Contrôle de l'existence des associations

Afin de s'assurer que de telles associations n'existent pas, vous avez la possibilité de vérifier via la commande ci-dessous, qui ne nécessite pas le statut d'administrateur du système.

```
setspn.exe -L $USER_AD_DOSSIER
```

où $USER_AD_DOSSIER désigne votre compte Kerberos

Si de telles associations existent sur une même machine, vous avez alors la possibilité de définir un autre compte Kerberos ou de supprimer toutes les références à ce compte sur cette machine en vous assurant qu'elles ne sont pas utilisées par d'autres configurations SSO. Pour supprimer les références, il suffit d'exécuter, pour chacune des lignes où apparaît ce compte, la commande ci-dessous sachant qu'une telle action nécessite d'être administrateur du système :

```
setspn.exe -D <ligne>
```

Par exemple, si vous avez les deux lignes suivantes pour le compte dossier_app (@setspn.exe –L dossier_app@) :

- HTTP/SRV_DOSSIER
- HTTP/SRV_DOSSIER.DOMAINE

Il faudra alors exécuter les deux commandes :

```
setspn.exe -D HTTP/SRV_DOSSIER dossier_app
setspn.exe -D HTTP/SRV_DOSSIER.DOMAINE dossier_app
```

2.4. Création d'une association (ou d'un service)

Pour cela, il suffit d'utiliser l'utilitaire setspn qui nécessite de disposer des droits d'administration système :

```
setspn.exe -A HTTP/$APP_SERVEUR.$DOMAINE $USER_AD_DOSSIER
```

où :

- **$APP_SERVEUR** par le nom du serveur qui contient le serveur d'applications Web au sein duquel est déployé l'application Dossier
- **$DOMAINE** par le nom de votre domaine, il doit correspondre avec le domaine auquel est associé le compte Kerberos

Toutes ces informations doivent être renseignées en majuscule (serveur et domaine). Quant à l'utilisateur, simplement respecter la casse utilisée lors de sa création.

Pour la vérification, vous pouvez exécuter la commande suivante :

```
setspn.exe -L $USER_AD_DOSSIER
```

2.5. Génération du "keytab"

Il apparaît ensuite indispensable de réinitialiser le mot de passe du compte $USER_AD_DOSSIER.

Pour cela, vous devez générer un fichier **keytab** à l'aide de la commande suivante :

```
ktpass -out fichier.keytab -princ HTTP/$APP_SERVEUR@$DOMAINE -mapuser
$user_ad_dossier@$DOMAINE-pass password -crypto all -ptype KRB5_NT_PRINCIPAL
```

Le fichier `fichier.keytab` ainsi généré se trouve à la racine du répertoire de l'utilisateur connecté au serveur. Il sera utilisé afin de mettre en œuvre le mode SSO pour l'utilisation du produit Dossier.

2.6. Test du paramétrage

Ce chapitre a pour but de tester depuis le serveur applicatif le bon fonctionnement du SSO. Dans un premier temps (dans une ligne de commande) exécuter la ligne suivante (puis renseigner le mot de passe affecté au compte) :

```
kinit $USER_AD_DOSSIER
```

La réponse doit être du genre **New ticket is stored in cache file C:\Users..."**.

Si cette étape est **OK**, se placer dans le répertoire **\bin** du JDK. Nous allons ici avoir besoin du fichier **keytab** généré ci-dessus.

```
java -Dsun.security.krb5.debug=true sun.security.krb5.internal.tools.Kinit -k -t
<rep>\fichier.keytab HTTP/$APP_SERVEUR@$DOMAINE
```

Où <**rep**> est le nom complet du dossier contenant le fichier `fichier.keytab` précédemment généré

Cette commande ne doit pas présenter d'erreur et se terminer, elle aussi, par **New ticket is stored in cache file C:\Users...**

Suite à cette opération, les URL du type ci-dessous pourront être protégées par le filtre d'authentification Kerberos de l'application Web :

```
http://$APP_SERVEUR<:port>
http://$APP_SERVEUR<:port>/dossier
http://$APP_SERVEUR.$DOMAINE<:port>/dossier
```

où <:port> est la donnée du port de communication paramétré pour le serveur apache-Tomcat.

À ce stade, on peut considérer la connexion SSO depuis le serveur applicatif comme valide et procéder désormais au paramétrage de l'application Dossier.

2.7. Association avec l'application Dossier

Pour cette opération, il n'est pas nécessaire de disposer de droits d'administration comme pour les paragraphes précédents sinon de bonnes connaissances des fichiers et paramètres de l'application Dossier. Sera uniquement concerné le fichier config.xml présent au sein du sous-dossier Config/ des composants de l'application Dossier déployée.

Il faut alors ajouter la balise spnego entre les balises cfe (ou error si la balise cfe est absente) et la balise generation. Naturellement, ce paramétrage ne peut pas être ajouté ou combiné avec le paramétrage OpenId Keycloak (balise « IDP »).

3 attributs peuvent être renseignés :

- **debug** (paramètre optionnel pour augmenter les traces : true ou false),
- **keyTabLocation**
- **servicePrincipal**

La casse est importante !

3. Activation Kerberos dans le navigateur des utilisateurs

Reste ensuite à autoriser l'utilisation de ce mode de fonctionnement au sein des divers navigateurs du client. En fonction de la version du navigateur, des sites déjà référencés, ce paramétrage peut ne pas être nécessaire. Il convient de réaliser un test sans avant de les ajouter.

3.1. Internet Explorer

Aller dans **Outils › Options Internet › Sécurité › Intranet local › Sites... › Avancé..** et indiquer le domaine **http://$DOMAINE** comme étant dans l'intranet.

3.2. Firefox

L'authentification Kerberos est activée par défaut pour les versions récentes de **Firefox**. Entrer `about:config` dans la barre d'adresse et restreindre la liste des options en entrant **negotiate** dans le filtre de recherche rapide. Double-cliquer sur l'entrée **network.negotiate-auth.trusted-uris**, puis entrer **.$DOMAINE** pour limiter l'authentification Kerberos à ce *domaine*.

Cette entrée peut être laissée vide pour une autorisation sans restriction (non recommandée)

4. Annexes

4.1. Authenfication auprès d'un serveur Linux Kerberos MIT

4.1.1. Sur le serveur

1. Installer les packages `krb5-libs`, `krb5-server` et `krb5-workstation`.
2. Editer les fichiers de configuration /etc/krb5.conf et /var/kerberos/krb5kdc/kdc.conf afin qu'ils reflètent le nom du domaine correct (dans le cadre d'un domaine simple, il suffit de remplacer **EXAMPLE.COM** et **example.com** en respectant la casse et de remplacer **kerberos.example.com** par le nom du serveur Kerberos).
3. Créer la base de données au moyen de la commande :

```
/usr/kerberos/sbin/kdb5_util create s
```

Editer le fichier /var/kerberos/krb5kdc/kadm5.acl. Ce fichier est utilisé par `kadmind` pour déterminer les personnes qui ont le droit d'administrer la base de données Kerberos et leur niveau d'accès. On peut se contenter de laisser une ligne unique (remplacer **EXAMPLE.COM**) :

```
*/admin@EXAMPLE.COM*
```

4. Créer le premier utilisateur par la commande (remplacer **username**) :

```
/usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
```

5. Lancer les services suivants par la commande :

```
/sbin/service krb5kdc start
/sbin/service kadmin start
```

6. Ajouter un par un chaque poste de travail du réseau (remplacer **pc-sso.digitech.lan** par le nom du poste au sein du réseau) :

```
addprinc -pw PASSWORD -e des-cbc-crc:normal host/pc-sso.digitech.lan
```

7. Ajouter chaque nouvel utilisateur autorisé à ouvrir une session par la commande (remplacer **L.LOGIN** par le login de l'utilisateur) :

```
addprinc -pw PASSWORD -e des-cbc-crc:normal L.LOGIN
```

8. Ajouter de la même manière un compte de pré-authentification pour l'application Dossier, dont nous reporterons les login et mot de passe dans le fichier **sso .properties** (cf. référence plus haut).
9. Editer le fichier /etc/krb5.conf qui doit refléter les paramètres du réseau (cf. référence plus haut, identique au fichier **krb5.conf** nécessaire au paramétrage de JAAS). Cette étape n'est pas nécessaire si les postes de travail sont situés sur le même domaine que le serveur.
10. **Redémarrer** Kerberos.

Vous trouverez des explications complètes de cette procédure à l'adresse suivante

4.1.2. Sur le poste client

1. Configurer Kerberos par les commandes suivantes au moyen de l'utilitaire `ksetup` qui fait partie lui-aussi des supports tools de Windows.

Il faut remplacer respectivement **$DOMAINE**, **$KER_SERVEUR** et **$PASSWORD** au sein de l'exemple ci-dessous par:

- le nom du domaine
- le nom du serveur Kerberos
- le mot de passe utilisé par apache Tomcat pour consulter le serveur d'authentification (cf. compte dossier créé précédemment)

```
ksetup /setdomain $DOMAINE
ksetup /addkdc $DOMAINE $KER_SERVEUR.$DOMAINE
ksetup /setcomputerpassword $PASSWORD
```

2. **rebooter**
3. Exécuter la commander suivante

```
ksetup /mapuser * *
```

4. Vérifier que le nom du domaine de la machine a bien été modifié en ouvrant les **propriétés du poste de travail › Nom de l'ordinateur › Modifier › Autres**.
5. Décocher également l'option **Modifier le suffixe DNS principal**.
6. Créer le compte utilisateur correspondant à l'un des comptes déjà ouverts sur le serveur Linux. A partir de maintenant, l'utilisateur devrait être en mesure de s'authentifier en sélectionnant le bon domaine dans la liste déroulante lors de la prochaine ouverture de session Windows.

Vous trouverez des explications complètes sur cette procédure à l'adresse suivante

4.2. Erreurs courantes

4.2.1. Failure unspecified at GSS-API level

Suite du message :

```
Mechanism level: Encryption type AES256 CTS mode with HMAC SHA1-96 is not supported/enabled)
```

La configuration par défaut prévoit une clé aes de 128 (aes128-cts) il apparait ici un défaut de configuration car la clé du client est aes sur 256 bits . Il est donc nécessaire ici de faire évoluer la configuration de Dossier est de modifier dans le fichier krb5.conf présent dans le répertoire xml :

Listing 1. Configuration par défaut

```
[libdefaults]
default_realm = <CLIENT_REALM>
  default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
  default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
  des-cbc-crc permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
```

Listing 2. Nouvelle configuration

```
[libdefaults]
default_realm = <CLIENT_REALM>
  default_tkt_enctypes = aes256-cts aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
  default_tgs_enctypes = aes256-cts aes128-cts rc4-hmac
  des3-cbc-sha1 des-cbc-md5 des-cbc-crc permitted_enctypes = aes256-cts aes128-cts rc4-hmac
des3-cbc-sha1 des-cbc-md5 des-cbc-crc
```