



**MINISTÈRES  
ÉDUCATION  
JEUNESSE  
SPORTS  
ENSEIGNEMENT  
SUPÉRIEUR  
RECHERCHE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général**

**Direction du numérique pour  
l'éducation**

**Délégation des services numériques  
pour l'administration centrale**

Bureau des opérations et du  
support des services de  
l'administration centrale  
DNE AC2

et

**Secrétariat général**

**Service de l'action  
administrative et des moyens**

**Sous-direction des achats**

**Bureau de la stratégie et de  
l'ingénierie des achats**

**SAAM B 1**

61-65 rue Dutot  
75732 Paris Cedex 15

## **CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

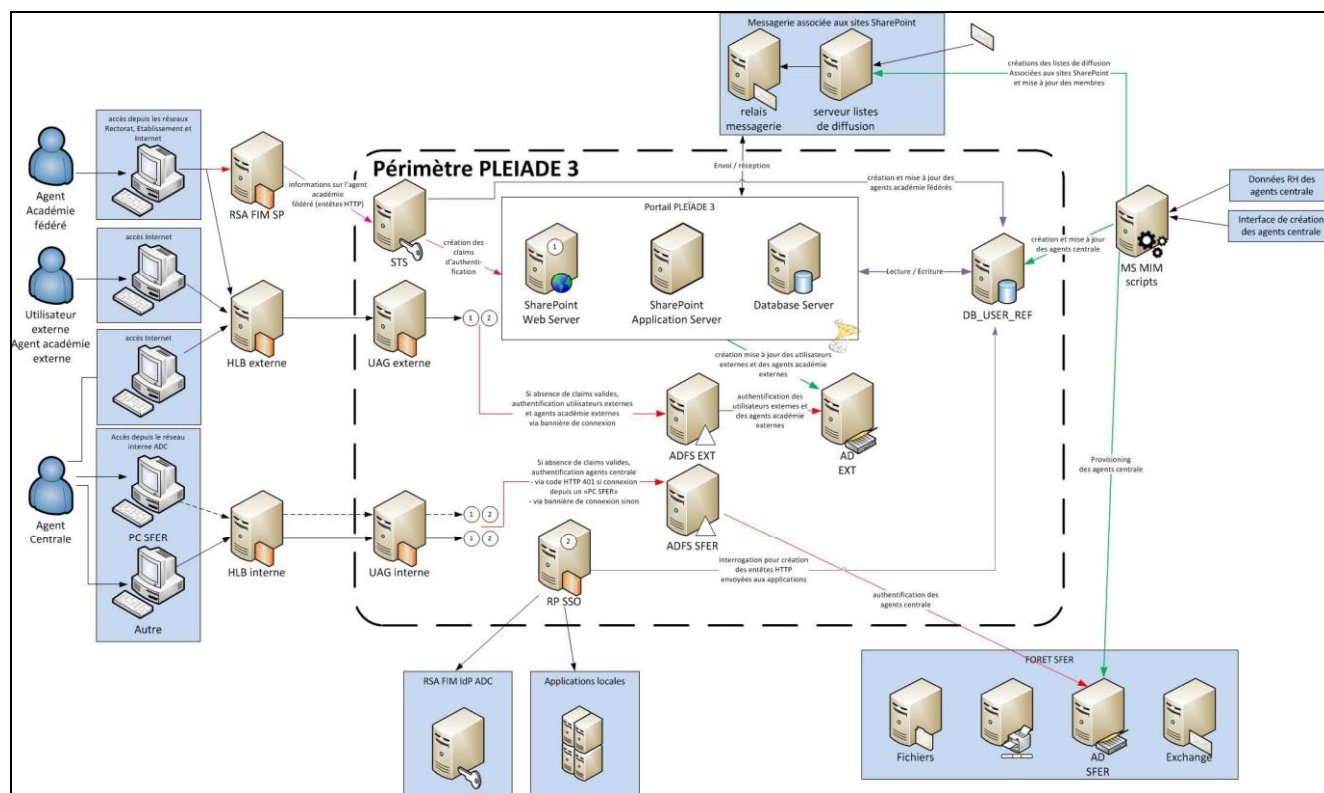
### **ANNEXE 2 :**

#### **ARCHITECTURE ACTUELLE DU PORTAIL PLEIADE**

### **Procédure n° MEN-SG-AOO-25028**

**Objet :** Réalisation de prestations de tierce maintenance applicative et de prestations associées pour le portail intranet national sécurisé "Pléiade" (technologies Microsoft SharePoint / SQL Server) pour le compte des ministères chargés de l'éducation nationale, de l'enseignement supérieur et de la recherche, des sports, de la jeunesse et de la vie associative.

## Architecture Logique de Pléiade



**Architecture logique de PLEIADE 3.1** Les différents types d'utilisateurs de Pléiade sont listés dans le tableau suivant:

Type Utilisateur	Description
Agents de la Centrale	<ul style="list-style-type: none"> <li>Agents de l'administration centrale connus du SI RH</li> <li>Agents en activité à l'administration centrale non connus du SI RH Quelle que soit leur situation RH, tous les agents de l'administration centrale ont accès au portail intranet Pléiade.</li> </ul>
Agents en académie	<ul style="list-style-type: none"> <li>Agents en académie non enseignants et non personnels d'orientation ayant un accès au portail intranet Pléiade de fait Ils se connectent au portail via leur portail local Arena en fédération d'identité avec le portail Pléiade. Ils seront nommés « agents académie fédérés » dans la suite du document.</li> <li>Agents en académie enseignants et personnels d'orientation ayant accès au portail intranet Pléiade après inscription. Ils se connectent directement au portail Pléiade. Ils seront nommés « agents académie externes » dans la suite du document.</li> </ul>
Utilisateurs externes	<ul style="list-style-type: none"> <li>Utilisateurs Externes (Universités et établissements du supérieur, autres ministères, organismes sous tutelle, prestataires de service, ...) ayant accès au portail intranet Pléiade après inscription</li> </ul>

Les utilisateurs de Pléiade 3 utiliseront les mécanismes d'authentification suivants :

**Authentification Claims sur Active Directory + ADFS** : ce service ADFS est utilisé pour fédérer les annuaires SFER et EXT. D'une part, il active le mécanisme d'authentification intégrée à Windows et qui permet aux utilisateurs du domaine SFER (agent de la centrale) qui se connectent depuis un poste faisant partie du domaine SFER de bénéficier d'une connexion transparente (authentification Windows Intégrée) et de l'accès à l'ensemble des fonctionnalités liées à l'intégration du client Office. D'autre part, ce service ADFS assure l'authentification en mode formulaire pour les utilisateurs du domaine EXT (agents académie externes et utilisateurs externes) et les utilisateurs du domaine SFER (agent de la centrale) qui se connectent depuis un poste qui ne fait pas partie du domaine SFER.

**Authentification Claims au travers de la fédération d'identité académique RSA FIM + STS Custom** : il s'agit du mécanisme utilisé pour les agents en académie se connectant via le portail Arena (agents académie fédérés). L'accès se fait en fédération d'identité (RSA FIM). L'authentification est réalisée au niveau de l'académie. Des données issues du référentiel académique sont transmises à l'application finale sous forme d'entêtes http constituant le « Vecteur d'Identité ». Un service STS (Security Token Service) spécifique decode les informations du « vecteur d'identité » positionnés en tant que revendication SAML.

Pour son, référentiel utilisateurs, le portail intranet Pléiade s'appuie sur la base de données DB\_USER\_REF. Les utilisateurs y sont provisionnés à partir :

- des SIRH de l'administration centrale (agents de la centrale connus du SI RH)
- des SI RH des académies (agents académie fédérés)
- du vecteur d'identité transmis par la fédération d'identités RSA FIM (création à la volée d'agents académie fédérés)
- du formulaire d'inscription individuelle disponible dans le portail intranet Pléiade (agents académie externes et utilisateurs externes)
- du processus d'inscription par fichier disponible dans le portail intranet Pléiade (agents académie externes et utilisateurs externes)

Par ailleurs, la base de données DB\_USER\_REF contient notamment et selon le type d'utilisateurs :

- les informations relatives à l'activité, la messagerie, la téléphonie, la localisation des utilisateurs
- les attributs nécessaires aux vecteurs d'Identité pour les applications SSO
- l'appartenance et le niveau d'autorisation des utilisateurs aux sites de publication et aux sites collaboratifs

Une connexion vers les relais de messagerie est nécessaire pour l'émission des notifications et la réception de messages à destination des listes de diffusion associées à des groupes SharePoint. Afin qu'il n'y ait pas de pertes de messages, les relais de messagerie SMTP sont accessibles en haute disponibilité.

Concernant l'authentification des utilisateurs, le portail intranet Pléiade s'appuie sur :

- Le service RSA-FIM ECSADC : le portail en académie est responsable de l'authentification des agents académie fédérés. Ce composant transmet au portail intranet Pléiade l'identité de l'agent académie fédéré via des variables d'entête HTTP. Si l'utilisateur n'est pas connu dans la base DB\_USER\_REF, il est créé automatiquement.

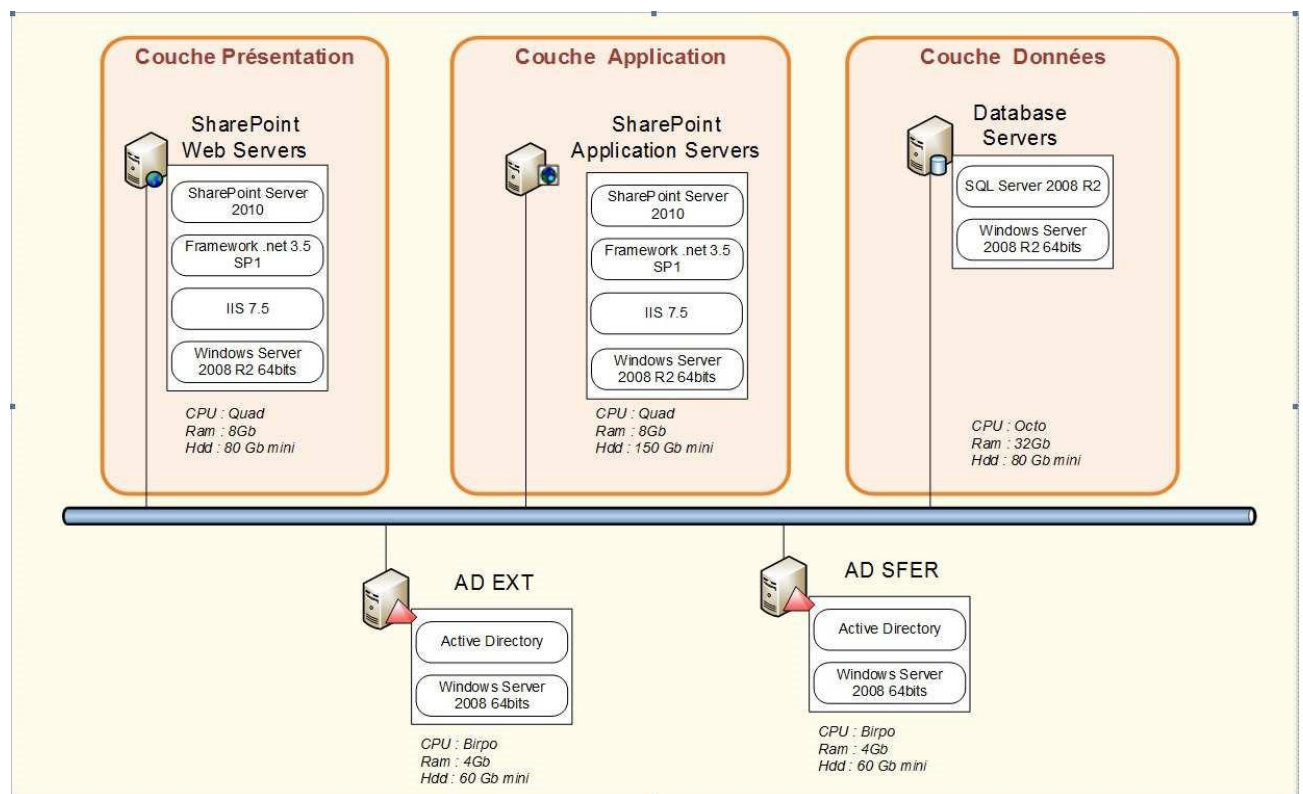
- Le domaine EXT : il est utilisé pour l'authentification des utilisateurs externes et des agents académie externes. (Remarque : une partie des utilisateurs qui fonctionnellement sont des utilisateurs académiques sont déclarés dans l'annuaire EXT).
- Le domaine SFER : il est utilisé pour l'authentification de l'ensemble des agents de la Centrale.

Les agents de la centrale, une fois authentifiés sur le portail intranet Pléiade, auront, en fonction de leurs droits, accès sans réauthentification à des applications locales (« SSOisées ») et à des applications nationales via l'utilisation du fournisseur d'identité (IdP) de RSA FIM.

## Composants applicatifs de Pléiade 3.1

Les composants applicatifs de PLEIADE sont :

- SharePoint 2010 Web Server : composante serveur qui gère la partie présentation
- SharePoint 2010 Application Server : Serveur d'application SharePoint qui assure les rôles applicatifs nécessaires au fonctionnement de Pléiade (exemple : recherche ou index)
- Database Server : Serveur de base de données qui héberge les bases de données Sharepoint 2010 de configuration, des applications de service et de contenu ainsi que DB\_USER\_REF, la base de données de référence de tous les utilisateurs de Pléiade 3.
- Active Directory SFER : la forêt SFER intègre les serveurs de l'infrastructure Pléiade 3.1 et assure l'authentification des agents de l'administration centrale via une brique ADFS
- Active Directory EXT : la forêt EXT assure l'authentification des utilisateurs externes et des agents académiques externes via une brique ADFS
- DB\_USER\_REF : Base de données de références de tous les utilisateurs de Pléiade 3.1
- UAG : Frontal d'authentification et de répartition de charge Sharepoint
- Serveurs et services connexes :
  - Composant STS : solution spécifique basée sur IIS en charge de l'augmentation des jetons d'authentification pour les agents académiques
  - Composant SSO composé de serveurs IIS 2008 R2 qui assurent le reverse-proxy des applications et la publication dans les entêtes http d'élément d'identification pour les applications



Architecture technique de Pléiade 3.1

## **COUCHE PRESENTATION**

Les serveurs web sont des serveurs avec le rôle SharePoint Web. Ils sont au nombre de quatre : 2 sur chaque site (Dutot, Descartes).

Les UAG assurent la répartition de charge (affinité par cookie).

Ces serveurs ont les composants logiciels suivants installés :

- Windows Server 2008 R2 x64 – Composants Windows : – IIS 7.5
  - Service SMTP
  - Framework .net 3.5 SP1
- SharePoint 2010 Enterprise x64 SP1 – rôle : web

## **COUCHE APPLICATION**

Les serveurs d'applications sont des serveurs qui hébergent les rôles applicatifs de SharePoint.

Ces serveurs ont les composants logiciels suivants installés :

- Windows Server 2008 R2 x64 – Composants Windows
  - IIS 7.5
  - Framework .net 3.5 SP1
- SharePoint 2010 Enterprise x64 SP1 – rôles : application/query/index

## **COUCHE DONNEES**

Les bases de données de la ferme SharePoint sont hébergées dans un cluster SQL Server, sur chaque site géographique (Dutot, Descartes) et un miroir entre les deux sites, avec un quorum (witness) sur un troisième site.

Ces serveurs ont les composants logiciels suivants installés :

- Windows Server 2008 R2 – Composants Windows
  - Distributed transactions
  - Framework .net 3.5 SP1
  - Failover clustering
- SQL Server 2008 R2 Entreprise version x64 SP2

## **LES CONTROLEURS DE DOMAINE SFER PHYSIQUES ET VIRTUELS**

La Forêt mono-domaine SFER dispose de quatre contrôleurs de domaine hébergés sur deux sites géographiques du ministère (Dutot, Descartes).

Les composants logiciels suivants sont installés :

- Windows Server 2008 R2 (en cours de migration vers Windows Server 2012 R2)
- AD DS (Active Directory Directory Services)

## **LES CONTROLEURS DE DOMAINE EXT VIRTUELS**

La Forêt mono-domaine EXT dispose de deux contrôleurs de domaine hébergés sur deux sites géographiques du ministère (Dutot, Descartes).

Les composants logiciels suivants sont installés :

- Windows Server 2008 R2
- AD DS (Active Directory Directory Services)

## **LE REFERENTIEL UTILISATEUR DB\_USER\_REF**

La base de données DB\_USER\_REF est le référentiel utilisateur sur lequel s'appuie le portail intranet Pléiade 3.1 et elle est utilisée également par d'autres projets ou applications. Elle contient les informations d'identification et d'autorisation pour les agents de la Centrale, les agents en académie ainsi que pour les utilisateurs externes. Les informations relatives aux trois types d'utilisateurs (centrale, académie, externe) sont stockées dans trois tables SQL distinctes.

Le projet Pléiade 3.1 s'appuie également sur cette base pour le fonctionnement du people picker ainsi que pour gérer ses autorisations.

Cette base de données est en technologie Microsoft SQL Server 2008 R2. Cette base de données contient également les groupes d'utilisateurs, les informations utilisateurs ainsi que la composition des groupes Sharepoint, c'est-à-dire l'appartenance des groupes d'utilisateurs à un ou plusieurs groupes Sharepoint.

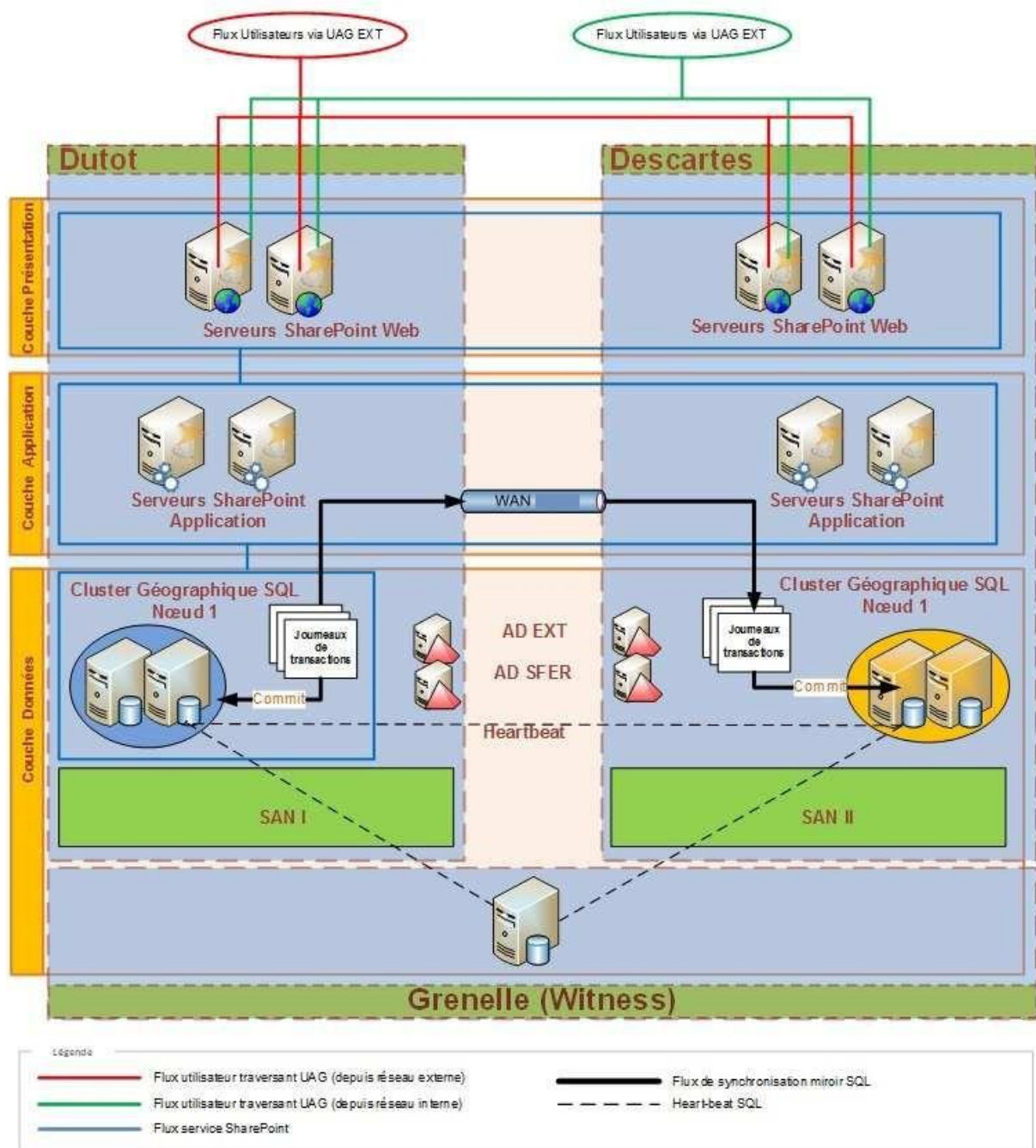
Cette base de données est installée sur l'environnement SQL utilisé par l'environnement SharePoint.

Les composants logiciels suivants sont installés :

- Windows Server 2008 x64 SP2
- SQL Server 2008 R2 x64 SP2



L'architecture physique de la solution Pléiade répartie sur les sites de Dutot, Descartes et Grenelle pour le « witness » est la suivante :



**Architecture physique de Pléiade 3.1**

Deux environnements techniques sont mis en œuvre au sein du ministère :

- Une plateforme de production,
- Une plateforme de pré-production iso-production destinée à la recette et aux tests d'intégration,
- Une plateforme de recette mono-serveur (un serveur d'application, un serveur frontal et un serveur de bases de données) hébergée au ministère et administrée par le titulaire.