

Architecture et Outils pour les applications Expadon 2

AUTEURS

FRANCEAGRIMER/SI/U_SIAFT/Pôle Expadon 2

OBJET DU DOCUMENT

Document décrivant les différentes architectures physiques et techniques mises en place dans les applications Expadon 2. Ce document recense également la liste des outils, des composants et des documents d'aide au développement.

Sommaire

1	<i>Introduction</i>	3
2	<i>Objectifs et enjeux du programme Expadon 2</i>	4
3	<i>Les architectures</i>	5
3.1	Architecture de la sphère Agrément (avant refonte)	6
3.2	Architecture de la sphère Infocom	8
3.3	Architecture de la sphère Certificat	10
4	<i>Gestion des sources</i>	12
5	<i>Charte graphique</i>	12
6	<i>Authentification de l'utilisateur</i>	12
7	<i>Outils et composants</i>	13
7.1	Scan Antivirus de sécurité des documents et pièces jointes	13
7.2	Gestion électronique des documents	13
7.3	Plateforme d'échange	13
7.4	Signature électronique	14
7.5	Containerisation	14
7.6	Read Model et Event sourcing	14
7.7	Référentiel Externes	15

1 INTRODUCTION

Ce document a pour but de synthétiser les différentes architectures physiques ou techniques mises en place dans les applications Expadon 2. Cette architecture a évolué avec les applications, ce document précise donc l'architecture employée pour chaque application.

Les applications Expadon 2 sont réparties en 4 grands groupes :

- La Sphère Agrément constituée des applications Webapp, Webmin et Batches ainsi que la future application de refonte Agrément
- La sphère Infocom avec l'application Infocom
- La sphère Certificat comprenant les applications : Certificat, GMC, CPM, PEN, GUT
- Une nouvelle sphère en cours de construction contenant les applications transverses : Gestion utilisateurs et Référentiels

2 OBJECTIFS ET ENJEUX DU PROGRAMME EXPADON 2

Objectifs et enjeux du programme Expadon 2

Objectifs stratégiques

- ▶ **Accompagner** les exportations françaises et permettre une plus grande fluidité des procédures SPS.
- ▶ **Encourager** les entreprises françaises à l'export, et notamment les PME.

Organisation du programme

Investissement : portage du programme à 50% par la DGAL et à 50% par FranceAgriMer.
Fonctionnement : portage à 100% par FranceAgriMer depuis 2014.



Le programme Expadon 2 c'est quoi ?

- **Agrément** (mis en service en sept 2017) :
 - Information sur les modalités d'agrément
 - Téléprocédure de gestion et suivi des demandes
 - Gestion des listes par pays
- **Infocom** (mis en service en 2019) : Portail d'entrée unique sur tous les services autour de la certification sanitaire
- **Certificat** (mis en service partiellement en 2020) :
 - Téléprocédure (demande, instruction et signature)
 - Gestion et paramétrage des modèles
 - Plateforme d'échanges numériques pour les gros opérateurs
 - Serveur gouvernemental pour les autorités pays tiers



Principaux services ciblés dans Expadon 2

1. Gestion des demandes d'agrément
2. Gestion de la certification SPS
3. Information et Communication
4. Tableaux de bord.

Bénéficiaires du programme

Les utilisateurs finaux

- ▶ Les opérateurs demandeurs
- ▶ Les responsables de filières
- ▶ Les agents des services déconcentrés DD(ec)PP, DRAAF/DAAF, les services économiques des ambassades de France à l'étranger)
- ▶ Les services centraux de la DGAL
- ▶ L'UAEXP au sein de la MAEI à de FranceAgriMer

3 LES ARCHITECTURES

La plateforme « Expadon 2 » est conçue selon une approche orientée services (SOA) et respecte les principes d'une architecture n-tiers. Les tiers (niveaux) identifiés dans l'architecture d'Expadon 2 sont :

- Le tiers « Présentation » est responsable de la gestion de l'interaction homme-machine ;
- Le tiers « Service » est responsable de fournir les services au tiers « Présentation » (et aux autres modules) de manière fiable et sécurisée ;
- Un éventuel tiers « Back Office » est responsable des actions telles que l'exécution de tâches planifiées sans utilisateur connecté ;
- Le tiers « Services Partagés » est responsable de fournir
 - Les données aux tiers « Service » accessible « Back Office »
 - Les services partagés d'envoi d'email accessible « Back Office »
 - Les services partagés de gestion des documents accessible « Back Office » ;
- Une plateforme d'échange machine-à-machine vient compléter l'architecture de la plateforme afin de permettre de soumettre des demandes de certificat directement depuis le système d'information des exportateurs

Chaque tiers est hébergé sur un ensemble de serveurs distincts, chaque tiers n'ayant accès qu'aux tiers adjacents :

- L'accès à la plateforme Expadon 2 n'est accessible de l'extérieur du Datacenter qu'au travers de mécanismes de protection mis en place par l'hébergeur afin d'assurer la sécurité périmétrique de la plateforme : firewalls, reverse proxy, Web Application Firewall, serveur de rebond pour l'administration. Ces mécanismes assurent le routage des requêtes provenant de l'extérieur de la plateforme Expadon 2 vers le module adapté au traitement de la requête.
- Le tiers « Présentation » est hébergé sur un cluster de serveurs Front Office. Les applications sont récupérées par les navigateurs internet des utilisateurs, puis s'exécutent dans ces mêmes navigateurs. Elles accèdent ensuite au tiers « Services », via les frontaux, pour obtenir les données et réaliser les actions demandées par l'utilisateur.
- Le tiers « Services » est hébergé sur un cluster de serveurs Back Office. Il assure les services nécessaires au fonctionnement des applications utilisateur (accès aux données Expadon 2, traitement des actions demandées par l'utilisateur) provenant du tiers « Présentation », et au fonctionnement des applications « Back Office ». Il est accessible depuis le cluster de serveurs Front Office et depuis le « BackOffice ».
- Le tiers « Back Office » est hébergé sur des serveurs dédiés « Back Office ». Il assure des services internes à la plateforme Expadon 2. Ce tiers ne doit pas être accessible depuis l'extérieur de la plateforme Expadon 2.
- Le tiers « Services Partagés » est hébergé sur des serveurs de base de données ou de fichiers. Ce tiers est accessible depuis les tiers « Service » ou « Back Office », mais ne doit pas l'être depuis le tiers « Présentation » ou l'extérieur de la plateforme Expadon 2.

NB : La plateforme Expadon 2 est hébergée chez le prestataire d'infogérance Claranet.

3.1 Architecture de la sphère Agrément (avant refonte)

La téléprocédure « Agrément » est conçue avec une approche orientée service afin d'offrir une souplesse d'évolution, d'accessibilité et de déploiement.

À ce titre, les composantes « Interface Homme Machine » (Front Office), « Services Métier » (Middle Office) et « Service Batch » font l'objet de livrables séparés et sont déployés sur des environnements distincts. La partie Middle Office comprend des composants en charge de l'accès aux bases de données (Back Office).

Le Framework Orion, intégré et fourni par le MASA, a été retenu dès 2014 pour la réalisation de la partie front de l'application et c'est donc un composant essentiel pour la téléprocédure Agrément.

A titre informatif, la liste non exhaustive ci-dessous présente le contexte technologique actuel de l'application Agrément historique :

- Langages de développement et bibliothèques principales : Java/JEE, cadriciel ORION V5.1.3, JSF2, HTML, XHTML, Javascript (jQuery), CSS (Bootstrap), SQL ;
- OS : Linux CentOS 6 ;
- Base de données : PostgreSQL 9.3.3 configurée en réplication maître-esclave et surcouche PGPool ;
- Modélisation des données : DDD ;
- Serveurs d'application : Glassfish, Tomcat
- Protocoles/outils de communication : HTTP/HTTPS, SMTP/SMTPS, FTP/SFTP, LDAPs, SOAP, Rest;
- Gestionnaire de source : Git
- Gestion Documentaire : Alfresco ;
- Génération des éditions : JasperReport, LibreOffice, ORION Reporting System et PDFBox;
- Gestion des performances applicatives : APM Nudge ;
- Packaging et déploiement : livraison ftp Claranet

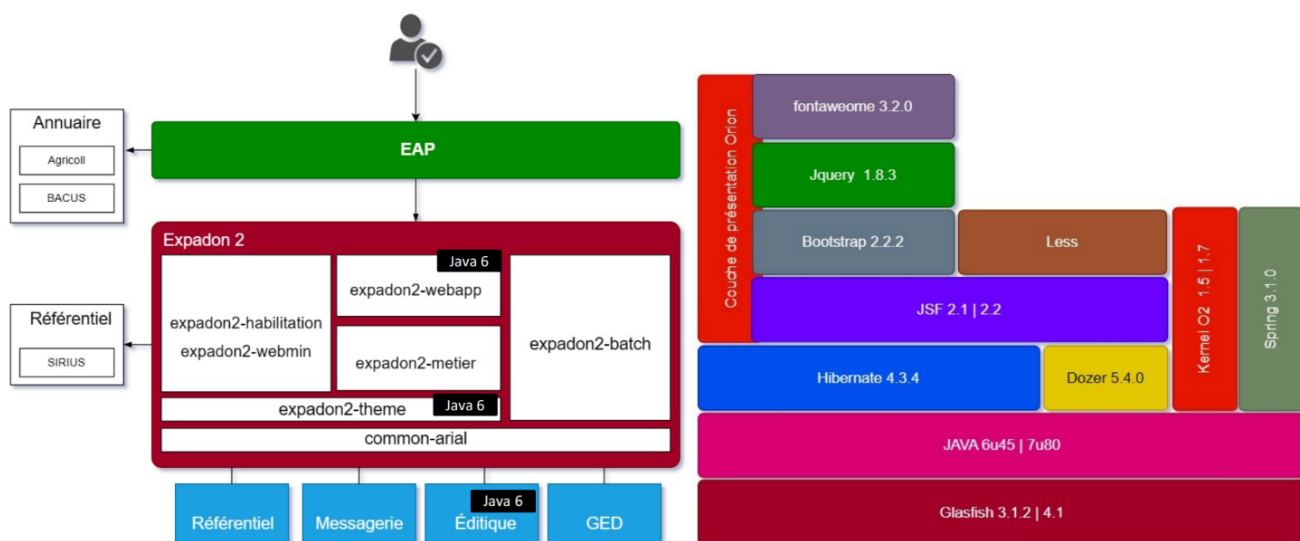


Figure 3 : Modules et technologies de l'application Agrément

Une étude est en cours pour lancer la refonte de cette application Agrément. Cette refonte sera effectuée sur le socle Nudle Java8/Angular avec application de la charte SDE.

3.2 Architecture de la sphère Infocom

Le portail « Information et Communication » (InfoCom) développé à partir de 2018 s'appuie sur le système de gestion de contenu de la société Jahia. Une personnalisation du module a été réalisée par des développements en langage Java.

Le portail « Information et Communication » permet, par le biais d'un site internet :

- de mettre à disposition tout un ensemble d'informations (base documentaire) sur l'exportation et l'importation ;
- de fournir un accès simple aux téléprocédures « Agrément pour l'exportation » ou « Certificat pour l'exportation » ;
- de publier des articles et des listes de liens internet ;
- d'informer et d'alerter les utilisateurs sur les sujets traités qui les concernent via une page d'accueil et une lettre d'information.

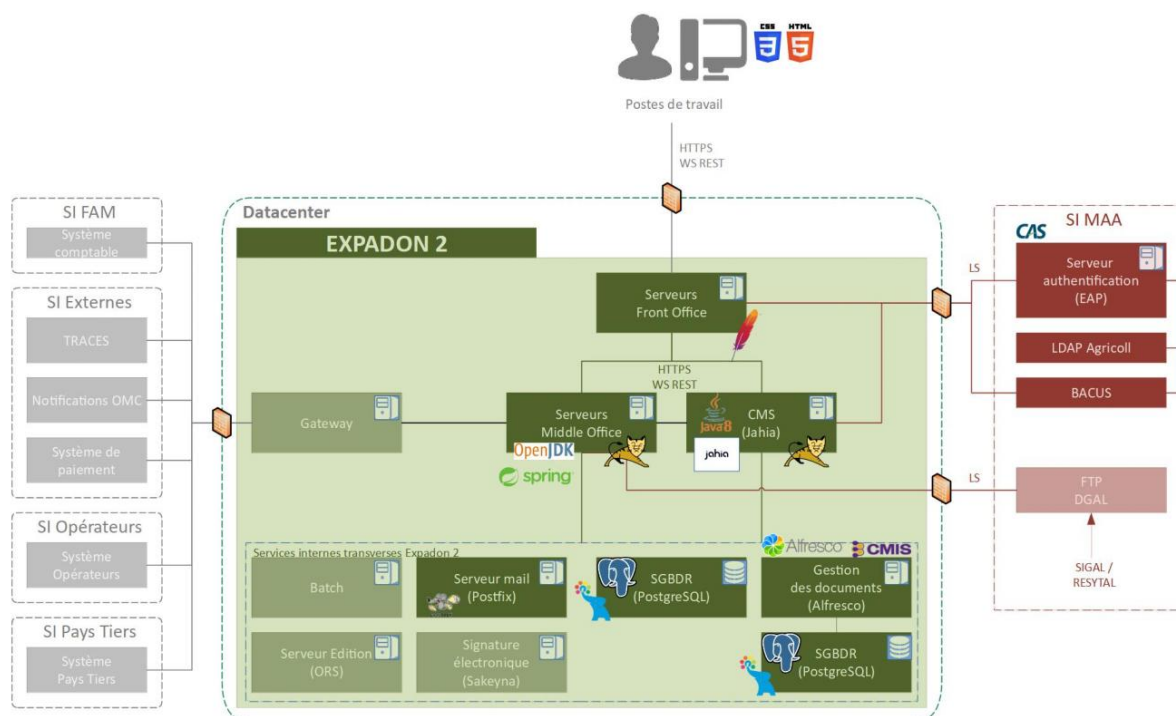


Figure 4 : Schéma architecture technique InfoCom

A titre informatif, la liste non exhaustive ci-dessous présente le contexte technologique actuel du système Infocom :

- Langages de développement et bibliothèques principales : Java/JEE, Jahia, Javascript;
- OS : Linux CentOS 7;
- Base de données : BDD interne Jahia + accès à la BDD PostgreSQL Agrément ;
- Serveurs d'application : Glassfish, Tomcat ; CMS Jahia Dx 7.2.2
- Protocoles/outils de communication : HTTP/HTTPS, LDAPs, SOAP, Rest;

- Gestionnaire de source : Git
- Gestion Documentaire : Alfresco 4.2 ;
- Packaging et déploiement : livraison ftp Claranet
- Vérification des PJ : ClamAV

Technologies utilisées



Figure 5 : Schéma des technologies InfoCom

3.3 Architecture de la sphère Certificat

La sphère Certificat est composée de 7 applications interconnectées entre elles et avec les autres applications Expadon 2 :

- Application Certificat (Back et front)
- Application Référentiel (Back)
- Application CPM (Front)
- Application Gestion des Modèles GMC (Back et Front)
- Application Gestion des utilisateurs GUT (Back et Front)
- Application PEN (Back)
- Application Serveur gouvernemental (Back et Front)

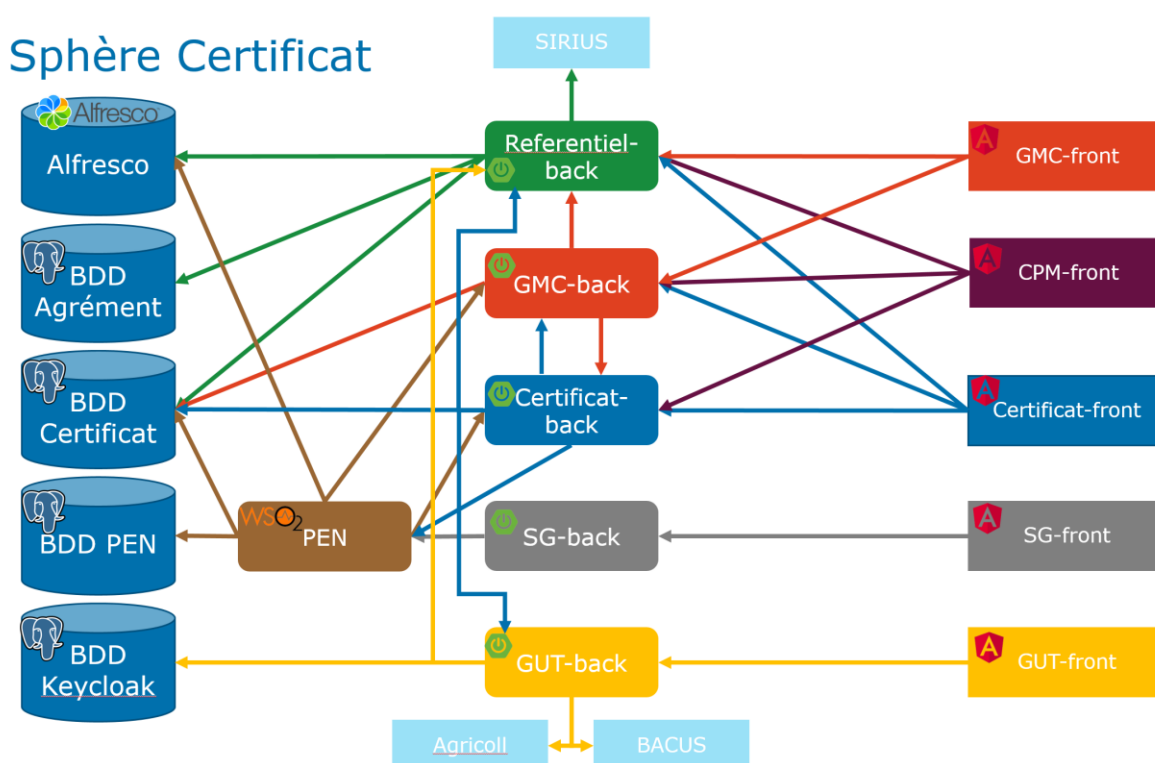


Figure 6 : Schéma architecture logique Certificat

Le socle technique retenu pour la plateforme Expadon 2 sphère « Certificats » se base sur les éléments suivants :

- Système d'exploitation CentOS 7.5 64bit.
- Base de données PostgreSQL.
- Serveur d'application Tomcat (embarqué par Spring Boot dans le cas des applications développées avec).
- EndOR. Un nouveau cadre de développement, EndOR, est mis en place par le BMSQ en 2018, en remplacement d'Orion, dont la dernière version disponible reposait sur des composants majeurs anciens, en limite de fin de vie pour certains. Ce nouveau cadre de développement s'accompagne de l'abandon du cadriciel Orion en tant que tel pour utiliser à une pile de

développement Spring, sans sur-couchage par le cadrage, accompagnée de services et de connecteurs propres au MAA. Les premiers développements de la sphère « Certificats » pourront être entrepris sur la base de ce socle de développement Spring classique, avec prise en compte des recommandations de développement du BMSQ.

- Java OpenJDK 8;
- Angular 9 pour le développement des interfaces homme-machine. Angular est un Framework d'application Web frontend open-source basé sur Typescript et JavaScript, principalement géré par Google et par une communauté de particuliers et de sociétés pour résoudre de nombreux problèmes rencontrés dans le développement d'applications single-page.
- Hibernate ORM pour la couche d'accès aux données. Hibernate ORM est un outil de mapping objet-relationnel pour le langage de programmation Java. Il fournit un cadre pour mapper un modèle de données orienté objet vers une base de données relationnelle. Hibernate est un logiciel libre qui est distribué sous la licence GNU LGPL 2.1.
- Spring Framework 5.x est un framework d'application pour la plateforme Java. Les principales fonctionnalités peuvent être utilisées par n'importe quelle application Java, mais il existe des extensions pour la création d'applications Web au-dessus de la plateforme Java EE. Le Spring Framework est distribué sous Licence Apache 2.0.
- Spring Security est un projet associé à Spring Framework qui permet de gérer les aspects sécurité d'une application.
- Keycloak 6.0.x comme solution IAM supportant l'architecture microservices. L'outil est compatible avec Spring-Security, Angular 9. Par ailleurs il supporte le protocole CAS d'identification utilisé par le Ministère, de même que des protocoles plus récents.
- Spring Boot 2.x est un projet associé à Spring Framework qui permet de simplifier la création d'applications Java indépendantes, ainsi que le déploiement de ces applications en production. Le projet Spring Boot est distribué sous Licence Apache 2.0.
- HikariCP est un outil permettant de gérer des pools de connexion à la base de données.
- Flyway est un outil permettant de faciliter la gestion des versions du schéma de la base de données.
- Swagger est un outil permettant de documenter les API.

4 GESTION DES SOURCES

Les sources sont gérées sous GIT depuis l'intégration de Expadon 2 dans le SI FranceAgriMer.

L'historique complet des versions et tags n'a pas pu être repris lors de la réintégration au sein du SI FranceAgriMer

5 CHARTE GRAPHIQUE

Les applications Expadon 2 ne respectent pas une charte graphique unique. Chaque application a défini une charte graphique lors de sa construction : en 2017 pour Agrément, 2019 pour Infocom et 2020 pour Certificat.

Dans le cadre de la refonte Agrément et la mise en place des briques transverses Gestion des habilitations et Référentiel, la charte graphique SDE sera appliquée.

6 AUTHENTIFICATION DE L'UTILISATEUR

L'authentification des utilisateurs sur la plateforme www.expadon.fr pour les applications principales est déléguée à la brique technique CAS SSO EAP V2 déployée sur le SI du MASA. Cette brique technique externe gère entièrement le dialogue utilisateur d'authentification (saisie de l'identifiant du compte utilisateur et du mot de passe...).

L'authentification s'appuie sur les annuaires suivants pour l'identification des utilisateurs :

- Compte Agricoll pour les agents du MAA ;
- Compte BACUS pour les utilisateurs externes au MAA.

La gestion des habilitations des utilisateurs est découplée entre les sphères « Agrément pour l'exportation » et « Certificat pour l'exportation ».

- La partie gestion des habilitations de la téléprocédure « Agrément pour l'exportation » et du portail Info.Com est implémentée avec le socle Orion dans l'application WebMin ;
- La gestion des habilitations pour la sphère « Certificats s'appuie sur le logiciel IAM Keycloak

7 OUTILS ET COMPOSANTS

Ce chapitre présente l'architecture des différents modules transverses utilisés par la plateforme « Expadon 2 », un chapitre dédié par module. Chaque chapitre présente les choix d'architecture spécifiques au module concerné.

7.1 Scan Antivirus de sécurité des documents et pièces jointes

La plateforme « Expadon 2 » est une plateforme ouverte aux utilisateurs internes du ministère ainsi qu'aux utilisateurs externes (i.e. les opérateurs et exportateurs). Il est possible de déposer des documents en provenance de ces utilisateurs. Par conséquent, il est nécessaire de mettre en place une solution vérifiant que ces documents ne constituent pas le vecteur d'une attaque cyber à l'aide d'un outil de scan antivirus.

La solution sélectionnée est basée sur l'outil ClamAV, installé sur toutes les VMs hébergeant les images des applications.

Pour la sphère « Certificats », les VMs « VM certificat X » et « VM Integration X » doivent avoir l'outil ClamAV installé sur chacune d'elle. La solution sera démarrée en mode daemon, en attente d'appel par les services applicatifs de « Certificats ».

Le scan sera déclenché via la librairie « clamav-client » par l'application Certificats, aussi bien pour les demandes faites par téléprocédure que via la plateforme d'échange (PEN).

Pour rappel, InfoCom doit également suivre le même principe.

La base de connaissance de ClamAV locale sur chaque VM doit être mise à jour de manière régulière par l'hébergeur.

7.2 Gestion électronique des documents

Une gestion transverse de l'ensemble des documents électroniques manipulés (notices d'information, modèles de certificats, certificats, pièces justificatives...) est mise en œuvre pour la plateforme Expadon 2. Les accès aux documents conservés s'effectuent uniquement via les applications de la plateforme Expadon 2, et non par des accès manuels dans l'interface proposée par le logiciel de GED. Cette possibilité est désactivée dans la GED.

La solution Alfresco existante de la sphère Agréments a été réutilisée dans le cadre de l'application InfoCom (sans impact sur le fonctionnement de la sphère Agréments) tandis que pour Certificat, il a été décidé de stocker les documents directement en base de données, ce pour limiter les adhérences et aussi le risque lié à la très grosse volumétrie estimée sur Certificat.

7.3 Plateforme d'échange

Une plateforme supportant les échanges avec les SI exportateurs est mise en œuvre qui permet d'accéder aux fonctionnalités d'Expadon 2 de façon automatisée.

La solution retenue est basée sur l'outil WSO2. L'analyse comparative de plusieurs outils a été nécessaire afin de retenir la meilleure solution sur la base des contraintes fonctionnelles et non-fonctionnelles.

Les principales caractéristiques de la plateforme d'échange sont les suivantes :

- WSO2 API Manager : écosystème complet intégrant la gestion d'identité, le contrôle d'accès, la publication des API, la supervision au runtime, le portail de développement et la documentation de l'environnement
- WSO2 Enterprise Integrator : solution permettant de réaliser la médiation des protocoles métiers et techniques.

7.4 Signature électronique

Un module de signature électronique a été mis en œuvre dans le cadre de la sphère « Agréments ». Ce module est basé sur le produit Sakeyna NetSigner de Thales. Il implémente une validation et une signature au format XADES en mode détaché avec manifeste (création d'un manifeste XML contenant une référence pour chaque document et signature enveloppante du manifeste XML ainsi produit). Il permet de signer n'importe quel document ou groupe de documents avec un cachet serveur, et de vérifier ensuite les signatures ainsi produites.

Ce module est développé en Java (testé avec OpenJDK 7, et Oracle Java 8), et fonctionne actuellement sous environnement CentOS. Il propose des API REST pour la signature et pour la vérification de signature.

7.5 Containerisation

Afin de simplifier et améliorer les processus d'installation, de configuration et de mise à jour des systèmes sur les différentes plateformes, les modules développés pour la partie Certificat (i.e. hors InfoCom et Agrément) sont livrés sous forme d'images Docker pour être installées sur les différents environnements. Les mêmes images sont utilisées sur les différentes plateformes, seule la configuration diffère.

Les points suivants sont pris en compte lors de création des images Docker des différents modules :

- La configuration est externe à l'image Docker, afin de disposer des mêmes images Docker sur les différentes plateformes, et de simplifier la mise à jour des images sur les plateformes. Une configuration pertinente doit néanmoins être présente par défaut dans les images Docker pour limiter la configuration externe aux seuls éléments spécifiques à l'instance.
- Les journaux et logs produits par les images Docker sont conservés, même en cas d'arrêt prévu ou non d'une image, ils ne doivent donc pas être stockés dans l'image Docker dont les contenus sont transients. Ces journaux sont automatiquement transférés sur le serveur ELK pour archivage, transformation et mise à disposition des logs à travers l'interface Kibana.

7.6 Read Model et Event sourcing

Un système de Read Model a été mis en place dans la sphère Certificat adossé à une version simplifiée d'event sourcing.

Un Read Model est une vue différente d'un objet :

- optimisé pour l'affichage sur la couche présentation
- sans dépendance sur d'autre table

Dans Expadon2, c'est représenté par un JSON stocké en base de données.

L'évent sourcing est un modèle de conception qui permet à partir d'une suite d'évènements et d'un état initial de calculer l'état final d'un objet.

La file d'évènements est stockée dans un event store ce qui facilite les reprises après erreur et les analyses.

Sur Certificat et CPM, des évènements sont issus pour mettre à jour les ReadModel mais il n'y a pas d'event store

7.7 Référentiel Externes

Interface avec système BACUS et Agricoll

Le système BACUS est le référentiel centralisé du ministère de l'Agriculture pour l'identification des personnes physiques. L'annuaire Agricoll est le référentiel des agents du ministère. Ils sont tous deux utilisés directement par le système EAP :

- Compte annuaire Agricoll pour les agents du MASA ;
- Compte annuaire BACUS pour les utilisateurs externes au MASA.

Ces deux référentiels sont interrogés par Expadon 2 grâce à une API mise à disposition par le MASA.

Interface avec le système SIRIUS

Le système SIRIUS du MASA, adossé aux services de l'INSEE, permet de fournir le référentiel des entreprises et personnes morales et est utilisé par Expadon 2 notamment pour la récupération et la mise à jour des SIRET/SIREN.

Ce référentiel est interrogé par Expadon 2 grâce à une API mise à disposition par le MASA.

Interface avec les systèmes SIGAL et RESYTAL

Les systèmes SIGAL et Resytal du MASA, permettent la mise à jour des référentiels des agréments CE, des identifiants, des numéros phytopass et des approbations des établissements d'Expadon 2.

Ces référentiels sont chargés dans Expadon 2 à partir de fichiers déposés par le MASA sur un serveur ftp puis traités par un batch Expadon 2 Agrément.