Cible de sécurité CSPN

JPLATFORM 10

A propos de ce document

Historique

Version	Date	Auteur	Commentaires
1.0	08/04/2020	JALIOS	Première version
1.1	22/07/2020	JALIOS	Mise à jour par rapport aux spec crypto et réunions OPPIDA
1.2	25/08/2020	JALIOS	Mise à jour des versions applicatives testées
1.3	21/12/2020	JALIOS	Mise à jour à la suite des remarques de l'ANSSI (document Référence : JALIOS.01 du 25/11/2020) Mise à jour des versions applicatives testées
1.4	04/01/2021	JALIOS	Mise à jour de la version produit

Contacts

Jalios SA
58 rue Pottier
78150 Le Chesnay

Si vous avez des questions ou souhaitez des éclaircissements sur ce document, vous pouvez nous contacter :

Service commercial

Jean-François Pellier
Tél : 01 39 23 31 15
E-mail : jean-francois.pellier@jalios.com

Service technique

Xavier Masia

Tél : 06 13 97 40 46
E-mail : xavier.masia@jalios.com

Sommaire

1 Identification du produit 6
2 Argumentaire du produit 7
2.1 Présentation générale du produit 7
2.1.1 Réseau Social d'Entreprise (RSE) 7
2.1.2 Espaces collaboratifs 7
2.1.3 Espace de travail (Digital Workspace) 8
2.1.4 Gestion documentaire collaborative 8
2.1.5 Social Learning 8
2.2 Architecture générale 9
2.3 Utilisateurs du produit 13
2.4 Hypothèses sur l'environnement d'utilisation du produit 14
2.4.1 Hypothèses sur l'environnement physique 14
2.4.2 Hypothèses sur les intervenants 14
2.4.3 Hypothèse sur l'environnement technique 14
3 Environnement technique de fonctionnement du produit 16
3.1 Environnement technique retenu pour l'évaluation 16
4 Biens sensibles devant être protégés 18
4.1 Liste des agents menaçants 18
5 Description des menaces 19
6 Spécification des fonctions dédiées à la sécurité 20
6.1 FDS_AUTH – Authentification locale des utilisateurs 20
6.2 FDS_ACL_Publi – Gestion des droits sur les publications 20
6.2.1 Droits de consultation des publications 20
6.2.2 Droits de contribution 20
6.2.3 Droits de dépôt des fichiers 21
6.2.4 Droits d'accès aux fichiers 21
6.2.5 Profils de consultation 21
6.2.6 Notion de Category Rights 21
6.3 FDS_ACL_Categorie – Gestion des droits sur les catégories 21
6.3.1 Droits de consultation 21
6.3.2 Droits d'usage 22
6.3.3 Droits de gestion 22

6.4 FDS_ADMIN_CENTRALE – Gestion des droits d'administration centrale 22
6.4.1 Droits d'administration centrale 22
6.4.2 Droits d'administration d'un espace de travail 22
6.5 FDS_ACL_Espace_Collaboratif 23
6.6 FDS_LOG - Fonction d'audit 23
6.7 FDS_NETTE Nettoyage des contributions par liste blanche 24
6.8 FDS_STOCK_CRED Fonction de stockage sécurisée des credentials des applications tierces (LDAP, ...) 24
6.9 FDS_GEST_FLOW Gestion des workflow (dans schéma consultation) 24
7 Argumentaires 25
7.1 Relation Biens / Menaces 25
7.2 Couverture des menaces par les fonctions 25

1 Identification du produit

Le présent document constitue la cible de sécurité CSPN pour le produit **JPlatform 10**.

Nom commercial du produit	JPlatform 10
Editeur	Jalios
Site web de l'éditeur	www.jalios.fr
Version du produit	SP4 10.0.4 patch 20201210

2 Argumentaire du produit

2.1 Présentation générale du produit

Solution tout-en-un, modulaire, complète et évolutive, **JPlatform 10** permet de créer une plateforme de Digital Workplace, d'intranet social et collaboratif ou encore de GED collaborative pour travailler ensemble efficacement.
Grâce à sa modularité et à son évolutivité, **JPlatform 10** peut être mise en œuvre de façon complète, progressive ou restreinte pour tenir compte des objectifs de l'entreprise, de sa maturité, et du rythme de son projet d'évolution digitale. **JPlatform 10** s'interconnecte aux suites bureautiques et aux services de messagerie mais aussi à d'autres outils ou services déjà déployés pour constituer un espace de travail unique et personnalisé.

JPlatform 10 permet aux entreprises de mettre en œuvre au sein d'un portail unique les fonctionnalités suivantes :

- Réseau social d'entreprise : espaces communautaires, profil riche déclaratif...
- Espaces collaboratifs : blog, wiki, calendrier partagé, planification...
- Portail d'entreprise et espace de travail personnalisé : intégration dans le SI, nombreux connecteurs, applications métiers...
- Gestion électronique documentaire : partage documentaire et édition collaborative, recherche avancée, gestion des versions…
- Social Learning : catalogue de savoirs, création de parcours, partage de savoir-faire, tableaux de bord...
- Gestion de contenu : espaces éditoriaux, workflow éditorial ou métier, gestion des droits…

2.1.1 Réseau Social d'Entreprise (RSE)

Le Réseau Social d'Entreprise (RSE) constitue un support aux communautés professionnelles pour :

- le partage des bonnes pratiques,
- la veille et la réflexion stratégique,
- l'émergence des initiatives et innovations,
- le transfert de connaissances.

2.1.2 Espaces collaboratifs

La solution **JPlatform 10** peut accueillir de multiples types d'espaces collaboratifs :

- espace collaboratif organisé autour de projets internes, transverses ou externes (partenaires, fournisseurs, clients...),
- espace collaboratif pour établir une proposition commerciale,
- espace collaboratif de veille ou de réflexion stratégique,
- espace communautaire organisé par thématiques ou par centres d'intérêts...
- club ou communauté extra-professionnelle.

2.1.3 Espace de travail (Digital Workspace)

L'espace de travail collaboratif permet de :

- disposer d'un point d'accès unique aux applications métiers,
- tirer le meilleur parti d'Office 365, G-Suite ou Libre office,
- mettre en œuvre sans développement des process métiers,
- permettre à chacun d'organiser son espace de travail,
- développer simplement des applications métiers.

2.1.4 Gestion documentaire collaborative

Le partage documentaire s'effectue dans un référentiel unique ou dans des espaces collaboratifs dédiés à un département, un projet ou une communauté.

Pour exploiter au mieux les documents, la solution **JPlatform 10** assure leur maîtrise durant toutes les phases du cycle de vie : création collective, validation, classement, diffusion avec limitation de droits, recherche, gestion de l'expiration, archivage.

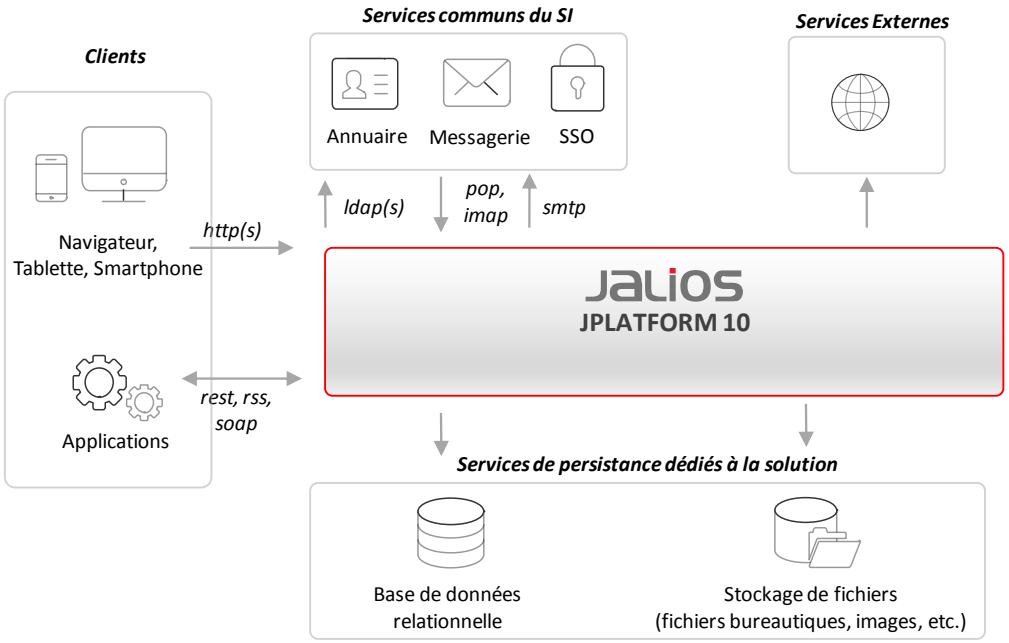
2.1.5 Social Learning

Le Social Learning fédère, via un point d'entrée unique, formation, communication et collaboration autour des objectifs d'apprentissage :

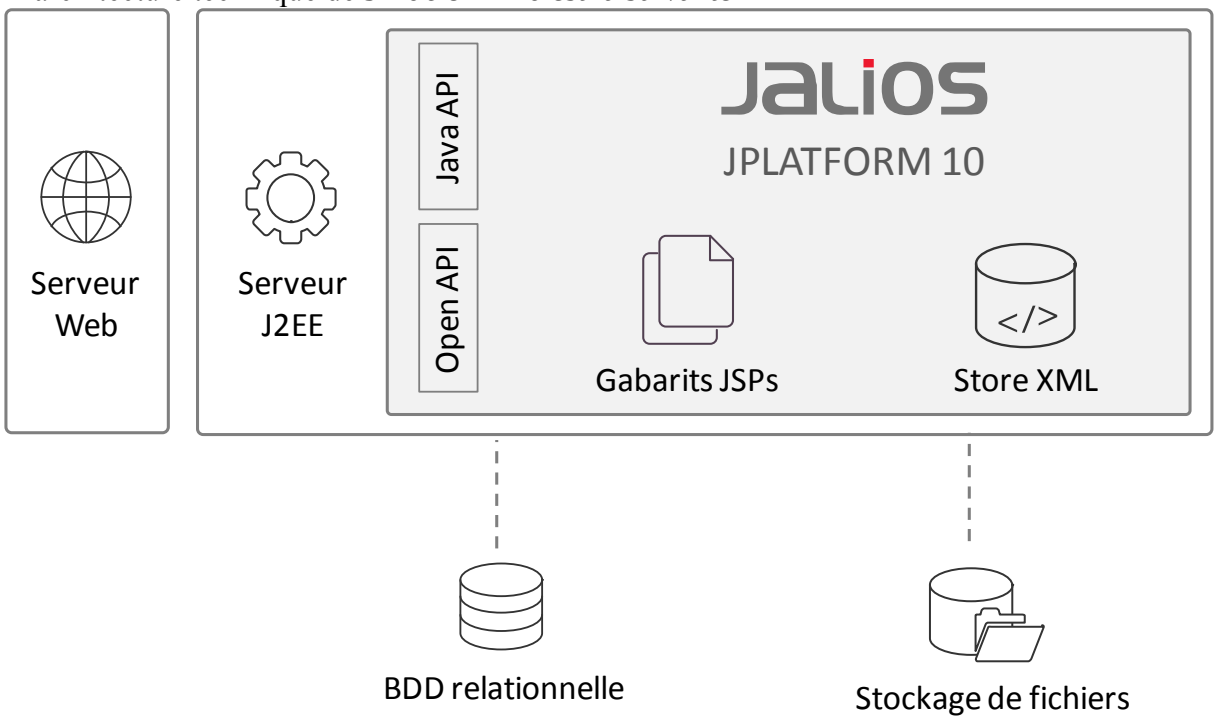
- publication de savoirs facile incitant au partage des connaissances et savoir-faire,
- espace collaboratif formateurs,
- quizz de validation de connaissances,
- gamification afin de dynamiser le dispositif et d'assurer un meilleur engagement,
- indicateurs de popularité basés sur les like et la participation,
- workflow de validation de contenu avant publication/partage,
- tableaux de bord.

2.2 Architecture générale

JPlatform 10 s'insère au sein du SI d'entreprise et permet également de s'interface avec des services web externes (par exemple Google G-Suite).

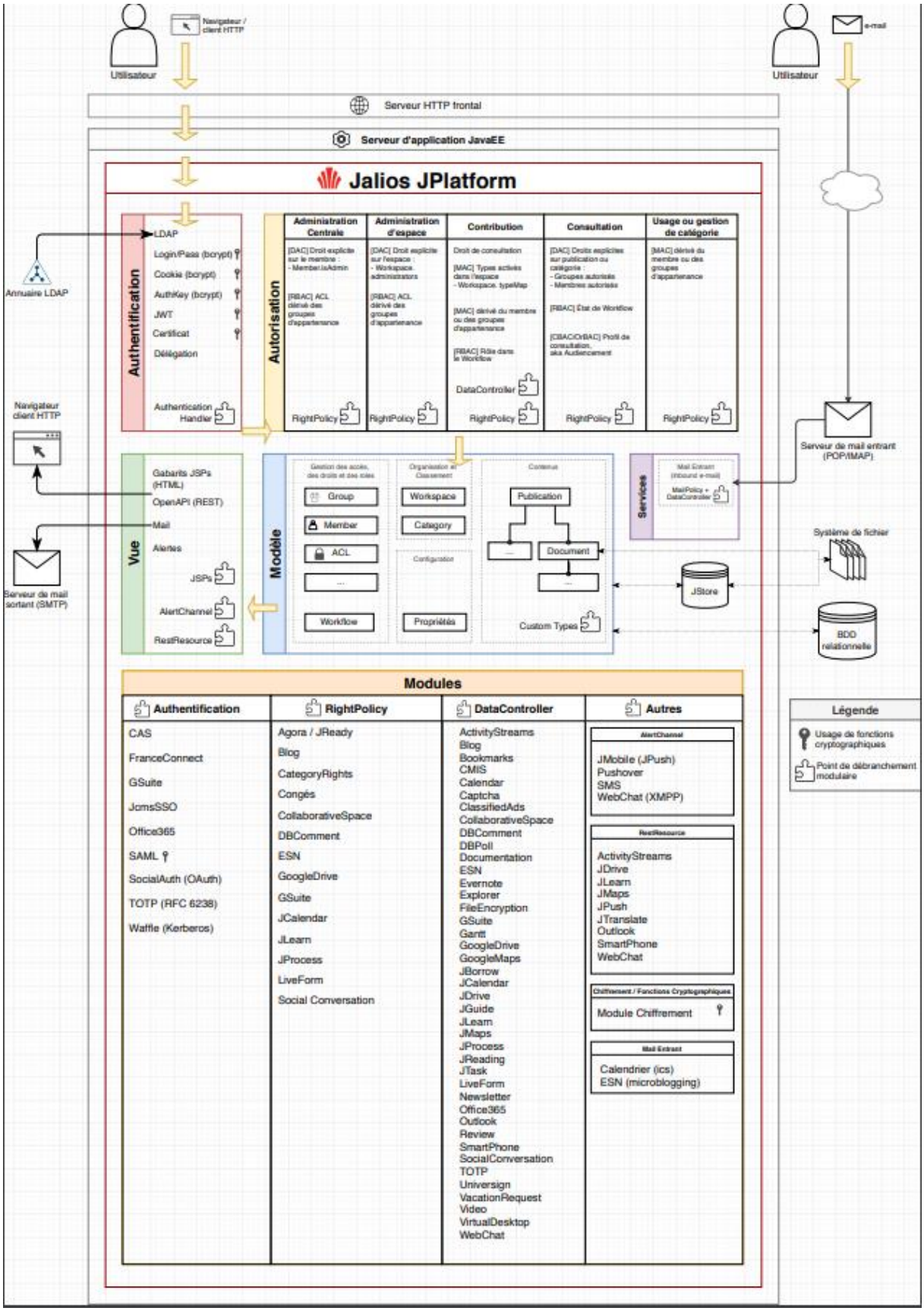


L'architecture technique de **JPlatform 10** est la suivante



- Serveur WEB : serveur frontal (optionnel) pouvant être installé devant le serveur d'application afin de mettre en place des fonctionnalités avancées (service de fichiers statiques, load balancing pour haute disponibilité ou failover, redirection spécifique, etc)
- Serveur Java EE : serveur d'application JavaEE (anciennement J2EE) permettant l'exécution de JPlatform
- Open API : endpoint REST permettant l'accès à distant aux APIs de JPlatform
- Java API : API interne Java dans le cœur de JPlatformGabarits JSPs :
- Gabarit de présentation des données. Définit les normes d'affichage des contenus. Dans JPlatform tout gabarit est représenté par un fichier JSP (Java Server Page : standard de page Web dynamique qui associe HTML avec du code Java).
- Store XML : Base de données interne de JPlatform. JStore est une base de données objets dont la persistance est assurée par la journalisation des opérations de modification. Au démarrage de l'application, l'ensemble des objets est chargé en mémoire en rejouant les opérations contenues dans le fichier store.xml . En cours d'exploitation, lorsqu'un objet est créé, modifié ou supprimé, l'opération décrivant cette écriture est ajoutée au journal. Seuls les attributs des objets sont chargés en mémoire et stockés dans store.xml .
- BDD relationnelle : JPlatform stocke une partie de ses données dans une base de données relationnelle, JcmsDB, gérée par un SGBDR
- Stockage de fichiers : le stockage des fichiers/document est réalisé sur le système de fichier du système d'exploitation hôte.

JPlatform 10 est une plateforme modulaire organisée autour de composants logiciels « core ». Les entreprises peuvent activer un certain nombre de modules complémentaires en fonction des besoins.



Les composants « Core » sont les suivants :

- Authentification,
- Autorisation,
- Vue,
- Modèle,
- Services.

Les modules activables dans **JPlatform 10** peuvent s'intégrer aux composants « core » grâce à des « points de débranchement » de type :

- Authentification,
- Right Policy,
- DataController,
- Autres.

2.3 Utilisateurs du produit

Administrateur système : il s'agit de l'administrateur qui installe le système d'exploitation et l'application **JPlatform 10**. Il s'agit d'un personnel du client final de la solution.

Utilisateurs **JPlatform 10** : il s'agit des utilisateurs qui possèdent des droits sur l'application. Chaque utilisateur se voit attribuer des droits selon des profils. Il est à noter qu'un utilisateur peut cumuler plusieurs profils.

Profil	Droits
Administrateur central	Gérer les comptes utilisateurs Gérer les groupes Gérer les espaces de travail Gérer les modèles de workflow Gérer les types de publications Effectuer les tâches d'exploitation (configuration, indexation des publications, gestions des caches, …) Effectuer les tâches de développement (définition des types de publication, gestion des changements, profiling, …)
Administrateur d'espace de travail	Gérer les groupes de l'espace de travail Affecter les membres aux groupes Gérer les affectations des rôles des workflows Gérer les propriétés des types (workflows, droits par défaut, onglet affichés, …) Consulter, éditer et supprimer toutes les publications et les catégories de l'espace de travail quelques soient leurs droits
Gestionnaire de catégories	Créer, modifier, déplacer et supprimer des catégories.
Contributeur	Consulter, créer, modifier ou supprimer des publications
Invité	Lecture, écriture de commentaire sur les publications, votes

En fonction de son profil, un utilisateur peut attribuer des droits d'accès aux autres utilisateurs. Ces droits peuvent concerner les publications ou la configuration. La matrice suivante indique qui peut affecter les droits.

	Contributeurs	**Gestionnaire des catégories**	**Administrateur d'espace de travail**	**Administrateur central**
Droits de consultation des publications	x		x	x
Droits de contribution	x		x	x
Droits de consultation des catégories		x	x	x
Droits d'usage des catégories			x	x
Droits de gestion des catégories			x	x
Droits d'administration d'espace de travail				x
Droits d'administration centrale				x

2.4 Hypothèses sur l'environnement d'utilisation du produit

2.4.1 Hypothèses sur l'environnement physique

H.LOCAUX_SECURISES — Les machines de **JPlatform 10** sont situées dans un local sécurisé à accès contrôlé.

2.4.2 Hypothèses sur les intervenants

H_ADMIN_SYS — L'administrateur système de **JPlatform 10** est considéré formé et de confiance

H_ADMIN_JPlatform — L'administrateur central de **JPlatform 10** est considéré formé et de confiance.

2.4.3 Hypothèse sur l'environnement technique

H.COMSEC — La protection des communications entre les postes clients et le serveur **JPlatform 10** est réalisée par le client final selon un guide de recommandations édité par JALIOS et qui concerne en particulier le paramétrage du serveur Web mis en place par le client final. Le chiffrement de ces communications doit être réalisé selon les préconisations de l'ANSSI en matière de mécanismes cryptographiques.

H.SAFE_INSTALL	L'installation des OS des machines de **JPlatform 10** est réalisé par le client final selon un guide de recommandation qui lui est propre. L'installation est réputée sécurisée et mise à jour régulièrement.
H.PUBLI_SAFE	Les publications mises en ligne sont réputées dépourvues de virus ou malware. Le client final de **JPlatform 10** doit mettre en œuvre des mécanismes d'anti-virus en amont de la publication.

3 Environnement technique de fonctionnement du produit

3.1 Environnement technique retenu pour l'évaluation

La plateforme évaluée est constituée des éléments suivants :

- JPlatform 10 SP4 - https://community.jalios.com/jplatform-10.0.4
- Système d'exploitation : Linux Server 64-bit
- Serveur Web frontal : Apache HTTP Server 2.4 (dans sa dernière version de maintenance)
- JVM Java : OpenJDK 11 (dans sa dernière version de maintenance)
- Serveur applicatif (JavaEE) : Apache Tomcat 9.0 (dans sa dernière version de maintenance)
- Navigateur des postes utilisateurs : Google Chrome (dans sa dernière version de maintenance)

Dans le cadre de la certification CSPN, le contexte d'emploi de **JPLATFORM 10** se limite à une configuration particulière de la plateforme :

- Site privé nécessitant une authentification
- 2 langues de contribution : français et anglais
- Utilisation de la base de données embarquée « Derby »
- Serveur de mail configuré
- Pas de proxy de sortie configuré
- OpenAPI activé

Les fonctionnalités suivantes sont désactivées :

- LDAP désactivé (Pas d'authentification, synchronisation des utilisateurs et des groupes avec un annuaire LDAP externe)
- WebDAV désactivé (Pas d'accès et de contribution de fichiers via le protocole WebDAV)
- JSync désactivé : La réplication JSync est désactivée
- Profil de consultation (aka « Audiencement ») désactivé
- Mail entrant désactivé

Les modules de **JPLATFORM 10** activés pour l'évaluation sont :

- Module PatchPlugin 10 SP4 - 10.0.4 - 20201210
- Module Espace collaboratifs 7.4 - https://community.jalios.com/plugin/collaborativespace
- Module CategoryRights 2.5 - https://community.jalios.com/plugin/categoryrights
- Module Explorer 4.2 - https://community.jalios.com/plugin/explorer
- Module Espace de conversations 5.3 - https://community.jalios.com/plugin/conversationspace
- Module Commentaire DB 6.2 - https://community.jalios.com/plugin/dbcomment
- Module Wiki 7.4 - https://community.jalios.com/plugin/wiki
- Module Conversion PDF 5.6 - https://community.jalios.com/plugin/pdfconverter
- Module Visionneuse de document 5.0 - https://community.jalios.com/plugin/documentviewer
- Module ESN 6.6 - https://community.jalios.com/plugin/esn
- Module JMobile 4.3 - https://community.jalios.com/plugin/jmobileplugin
- Module OnlyOffice 1.1 https://community.jalios.com/plugin/onlyoffice

4 Biens sensibles devant être protégés

B.CREDENTIALS_USERS	Mots de passe des utilisateurs de la ToE. Besoin de sécurité : Confidentialité, Intégrité
B.PUBLICATIONS	Les publications sont toutes les contenus qui peuvent être publiées sur la ToE (fichiers, commentaires, blogs, wiki,…). Besoin de sécurité : Confidentialité, Intégrité
B.CATEGORIES	Hiérarchie de termes permettant de caractériser et d'organiser les contenus. Besoin de sécurité : Intégrité
B.DROITS_ACCES_Publication	Droits d'accès associés aux publications et attribués aux utilisateurs de la ToE. Besoin de sécurité : Intégrité
B.DROITS_ACCES_Catégorie	Droits d'accès associés aux catégories et attribués aux utilisateurs de la ToE. Besoin de sécurité : Intégrité
B.DROITS_ADMIN	Droits d'administration centrale attribués aux utilisateurs de la ToE. Besoin de sécurité : Intégrité
B.DROITS_ESPACES_COLLAB	Droits d'accès spécifiques aux espaces collaboratifs (public, privé, secret). Besoin de sécurité : Intégrité
B.LOGS	Evènements de sécurité enregistrés par la ToE. Besoin de sécurité : Confidentialité, Intégrité, Disponibilité
B.CREDENTIALS_TIERS	Ensemble de mots de passe permettant à la ToE de se connecter à des applications tierces (LDAP, serveur de mail,…). Besoin de sécurité : Confidentialité, Intégrité

4.1 Liste des agents menaçants

Les agents menaçants pour la ToE peuvent être externes ou internes.

Externes : il s'agit d'attaquants n'ayant aucun droit sur la TOE mais pouvant accéder au réseau sur lequel elle est installée. Leur objectif est d'obtenir des droits d'accès à la ToE.

Internes : il s'agit d'utilisateurs de la ToE (hors administrateur système et administrateur central) disposant de droits restreints. Leur objectif est d'usurper des droits ou d'augmenter leurs privilèges sur la ToE.

5 Description des menaces

M.USURP_USER	Un attaquant externe ou interne tente d'usurper l'authentification d'un utilisateur de la ToE afin de disposer de droits d'accès particuliers sur le ToE.
M.ALTER_RIGHTS	Un attaquant externe ou interne tente de modifier les droits d'accès pour visualiser/modifier des publication, des catégories ou des droits d'administration.
M.PRIV_ECALADE	Un attaquant externe (exemple : compte invité) ou interne profite de ses droits d'accès pour tenter d'en obtenir des supérieurs ou de disposer d'un profil plus privilégié.
M.DECLOISONEMENT	Un attaquant interne, tente d'accéder à des publications qui ne lui sont pas destinées.
M.ALTER_LOGS	Un attaquant externe ou interne tente de modifier les journaux d'évènements de sécurité.
M.ALTER_PUBLI	Un attaquant externe ou interne provoque une altération des publications pour tenter d'introduire des commandes malveillantes.

6 Spécification des fonctions dédiées à la sécurité

6.1 FDS_AUTH – Authentification locale des utilisateurs

Cette fonction de sécurité repose sur une authentification des utilisateurs par mot de passe. Les mots de passe sont (stockés dans la base de données JCMSDB ou dans JSTORE) à l'aide de l'algorithme BCRYPT. Il est possible au travers de la configuration de cette fonction de définir une politique de mot de passe conforme aux recommandations de l'ANSSI en termes de complexité.

Une fois l'utilisateur authentifié, un cookie de session est généré et permet le maintien de la session pour l'utilisateur.

Il est à noter que la fonction d'authentification permet un mécanisme de délégation.

6.2 FDS_ACL_Publi – Gestion des droits sur les publications

Cette fonction de sécurité permet la gestion des droits d'accès aux publications.

Dans **JPlatform 10** les droits sont affectés soit individuellement à des membres soit à des groupes. Un membre qui appartient à un sous-groupe appartient automatiquement à tous les groupes parents de ce groupe (et aux parents des parents). Ainsi en affectant un droit à un groupe c'est non seulement les membres de ce groupe qui en bénéficient mais aussi tous les membres des sous-groupes de ce groupe.

6.2.1 Droits de consultation des publications

Ce droit contrôle qui peut consulter un contenu ou visualiser une portlet. Ce droit est défini contenu par contenu en indiquant les groupes et les membres autorisés. Si aucun droit n'est défini, la publication est visible de tous. Il est possible d'affecter des droits de consultation par défaut (par type de publication ou par espace de travail).

Le droit de consultation est conditionné :

- à l'état du workflow dans lequel se trouve la publication : une publication hors de l'état publié n'est visible que dans le back-office de son espace de travail,
- au rédacteur : quelques soient les droits de consultation, un membre a toujours accès aux contenus dont il est le rédacteur.

6.2.2 Droits de contribution

Ce droit contrôle qui peut créer, modifier ou supprimer des publications. Ce droit est défini par type de publication. Il est affecté pour un groupe ou pour membre.
Il est possible de définir un droit spécifique d'édition pour un contenu. Ceci permet à certains membres ou groupes n'ayant pas ce droit d'en bénéficier pour ces contenus.
Le droit de contribution est conditionné :

1. au droit de consultation : un utilisateur ne peut pas éditer ni supprimer une publication à laquelle il n'a pas accès ;

2. à l'espace de travail : le contributeur ne bénéficie de son droit de contribution sur le type T dans un espace de travail que si cet espace utilise le type T ;
3. au workflow :
    1. un membre ne peut créer une publication que si il est autorisé à travailler dans l'état initial du workflow de la publication.
    2. un membre ne peut éditer ou supprimer une publication que si elle se situe dans un état de workflow où le membre peut agir ; c'est-à-dire un état pour lequel le membre occupe au moins un rôle de l'une des transitions sortantes de cet état.

6.2.3 Droits de dépôt des fichiers

Ce droit contrôle qui peut déposer des fichiers sur le site. Il s'agit en fait d'un droit dérivé du droit de contribution sur le type Document. Le membre doit avoir le droit de contribution sur le type Document.
En standard, **JPlatform 10** permet de contrôler le type et la taille des fichiers déposés.

6.2.4 Droits d'accès aux fichiers

Le droit d'accès aux fichiers déposés est régi par les publications qui les pointent. Lorsqu'un utilisateur accède à l'un de ces fichiers, **JPlatform 10** vérifie qu'il peut accéder à au moins une des publications qui référence ce fichier.

6.2.5 Profils de consultation

JPlatform 10 propose également une autre approche pour la gestion des droits de consultation : les profils de consultation.
Le principe consiste à déterminer les droits de consultation en croisant les catégories d'un contenu et les catégories du membre qui accède au contenu. Pour cela, les membres doivent être catégorisés sur les mêmes branches que les contenus. Les rédacteurs n'ont plus à déclarer explicitement les droits de consultations mais simplement à quelles catégories sont rattachés les contenus.

6.2.6 Notion de Category Rights

Le module Category Rights, inclus dans le périmètre d'évaluation propose une nouvelle politique de droit d'accès pour les publications. Cette politique propage les droits de catégories aux contenus qui s'y rattachent. Une publication catégorisée sur des catégories protégées est visible par un membre uniquement si le membre peut accéder à au moins une des catégories protégées.

6.3 FDS_ACL_Categorie – Gestion des droits sur les catégories

Cette fonction de sécurité permet la gestion des droits d'accès aux catégories.

6.3.1 Droits de consultation

Ce droit contrôle qui peut consulter une branche de catégories. Il est défini branche par branche pour un membre ou un groupe. Si un membre peut consulter la catégorie C, alors il peut aussi consulter toutes les sous-catégories de C.

Ce droit porte sur l'affichage des catégories (typiquement pour une Portlet Navigation). Il n'affecte pas les contenus situés sous ces catégories. En d'autres termes, un membre peut consulter les contenus référencés sous la catégorie C même s'il n'a pas le droit de consulter C.

6.3.2 Droits d'usage

Ce droit contrôle qui peut référencer un contenu sous une branche de catégories. Il est défini branche par branche pour un membre ou un groupe. Si un membre peut référencer la catégorie C, alors il peut aussi référencer toutes les sous-catégories de C. Ce droit est conditionné au droit de contribution des publications.

6.3.3 Droits de gestion

Ce droit contrôle qui peut gérer une branche de catégories, c'est-à-dire créer, modifier, déplacer et supprimer des catégories. Il est défini branche par branche pour un membre ou un groupe. Si un membre peut gérer une catégorie C, alors il peut aussi gérer toutes les sous-catégories de C

6.4 FDS_ADMIN_CENTRALE – Gestion des droits d'administration centrale

6.4.1 Droits d'administration centrale

Ce droit donne accès à toutes les fonctionnalités de **JPlatform 10.** En plus des droits précédents, il permet de :

- Gérer les comptes utilisateurs ;
- Gérer les groupes ;
- Gérer les espaces de travail ;
- Gérer les modèles de workflow ;
- Gérer les types de publications ;
- Effectuer les tâches d'exploitation (configuration, indexation des publications, gestions des caches, …) ;
- Effectuer les tâches de développement (définition des types de publication, gestion des changements, profiling, …).

6.4.2 Droits d'administration d'un espace de travail

Ce droit contrôle qui peut administrer un espace de travail, c'est-à-dire :

- Gérer les groupes de l'espace de travail;
- Affecter les membres aux groupes ;
- Gérer les affectations des rôles des workflows ;
- Gérer les propriétés des types (workflows, droits par défaut, onglet affichés, …) ;
- Consulter, éditer et supprimer toutes les publications et les catégories de l'espace de travail quelques soient leurs droits.

Ce droit est nominatif. Il est donné espace par espace par l'administrateur central.

6.5 FDS_ACL_Espace_Collaboratif

Cette fonction de sécurité permet la définition de droits spécifiques aux espaces collaboratifs (Espace **public**, **privé** ou **secret)**.
Le module Espace Collaboratif introduit le ***compte invité,*** un compte utilisateur avec des droits restreints.

Seuls les membres qui appartiennent à un espace privé ou secret peuvent en lire les contenus.

Les espaces privés sont visibles par tous les membres. En revanche, un membre qui n'appartient pas à un espace secret n'aura même pas connaissance de l'existence de cet espace.

La politique d'inscription est asservie sur la politique d'accès.

	Public	Privé	Secret
Inscriptions libres	x	x	
Demandes d'inscriptions validées par les animateurs	x	x	
Inscriptions gérées par les animateurs	x	x	x

6.6 FDS_LOG - Fonction d'audit

Cette fonction permet l'audit des évènements de sécurité suivants :

- Authentification
  - Délégation d'un compte à un autre
  - Authentification en échec plus de 3 fois
  - Tentative de réinitialisation de mot de passe avec un token invalide
  - Tentative d'authentification avec un compte désactivé ou un contact
- Accès
  - Tentative d'accès à un document sans les autorisations requises
  - Tentative d'export XML d'une publication sans les autorisations requises
- Contribution
  - Refus de dépôt de document provoqué suite à une limite quelconques (antivirus, taille, type, ...)
- Administration
  - Désactivation ou activation des écritures sur le site
- Divers :
  - Accès au portail avec des paramètres invalides
  -
  - Tentative d'accès à un JSP interdit

JPlatform 10 utilise la librairie Apache log4j 1.2 pour sa gestion d'évènements. Les évènements sont stockés dans un fichier du serveur applicatifs. Les cinquante derniers logs émis peuvent être visualisés directement dans l'interface d'administration centrale. Pour les autres, il est possible de les afficher en mode texte dans le système d'exploitation de la ToE. La protection des fichiers d'évènements est faite est faite via des droits d'accès du système d'exploitation. Enfin, il y a un système de rotation journalière défini au niveau fichier de

configuration de l'application (limité à 100MB par fichier, les précédents fichiers étant compressés au format gzip et avec un maximum de 50 fichiers)

6.7 FDS_NETTE Nettoyage des contributions par liste blanche

Cette fonction effectue un nettoyage des balises dans une publication par exemple dans wiki. Le nettoyage s'effectue sur la base d'une liste blanche qui autorise uniquement les balises déclarées.

6.8 FDS_STOCK_CRED Fonction de stockage sécurisée des credentials des applications tierces (LDAP, ...)

Cette fonction de sécurité permet le stockage des mots de passe utilisés par la ToE pour se connecter à des services tiers (LDAP, Serveur de mail). Les mots de passe sont stockés dans un fichier de configuration sur le système de fichiers de la ToE (protégé par le contrôle d'accès du système d'exploitation).

Note : l'évaluation ne concerne pas le stockage externe de credentials.

6.9 FDS_GEST_FLOW Gestion des workflow (dans schéma consultation)

Cette fonction permet la gestion des états d'une publication. En fonction de son état, une publication est accessible ou visible à son propriétaire uniquement. La gestion des workflow permet également de donner des droits de changement d'état à des utilisateurs.

7 Argumentaires

7.1 Relation Biens / Menaces

	M.USURP_USER	M.ALTER_RIGHTS	M.PRIV_ECALADE	M.DECLOISONEMENT	M.ALTER_LOGS	M.ALTER_PUBLI
B.CREDENTIALS_USERS	X		X			
B.PUBLICATIONS				X		X
B.CATEGORIES				X		X
B.DROITS_ACCES_Publication		X		X		
B.DROITS_ACCES_Catégorie		X		X		
B.DROITS_ADMIN		X	X			
B.DROITS_ESPACES_COLLAB		X		X		
B.LOGS					X	
B.CREDENTIALS_TIERS	X		X			

7.2 Couverture des menaces par les fonctions

	M.USURP_USER	M.ALTER_RIGHTS	M.PRIV_ECALADE	M.DECLOISONEMEN	M.ALTER_LOGS	M.ALTER_PUBLI
FDS_AUTH	X		X			
FDS_ACL_PUBLI		X	X	X		X
FDS_ACL_CATEGORIE		X	X	X		X
FDS_ADMIN_CENTRALE					X	
FDS_ACL_ESPACE_COLLAB		X	X	X		X
FDS_LOG					X	
FDS_NETTE		X	X	X		X
FDS_STOCK_CRED	X					
FDS_GEST_FLOW		X	X	X		X