

## **Cadre de Cohérence Technique**



## GENERALITES

### Contenu

- [01 - REFERENTIEL PRODUITS](#)
- [02 - REFERENTIEL DES REGLES D'IMPLEMENTATION](#)
- [03 - REFERENTIEL DES SERVICES SOCLES](#)
- [04 - REFERENTIEL DES PATTERNS D'ARCHITECTURE](#)
- [99 - Annexes](#)

### Périmètre du CCT

Le CCT s'intéresse à 6 domaines principaux, ou piliers :

1. L'utilisateur, – qu'il soit citoyen/usager, agent, entreprise, association – Ce domaine primordial adresse différents thèmes comme son identification / authentification / autorisation, l'environnement numérique de travail.
2. Les données et les API, patrimoine du SI de l'État et socle sur lequel se fonde le service rendu à l'utilisateur
3. La sécurité du service
4. La fabrique de code qui traite du "build" au travers des processus d'intégration et de déploiement continu
5. L'hébergement qui traite du "run" et des problématiques d'hébergement et d'exploitation
6. Les services transverses : services de confiance, gestion électronique de courrier, etc...

Dans ces domaines préférentiels,

Il édicte des règles et des recommandations, et il référence les composants et offres de services portés par les différents acteurs DNUM. Au-delà d'un référentiel de cadrage, le CCT se veut un outil de mise en relation entre les producteurs et consommateurs de ces composants et services. Le CCT produit un référentiel de composants et de leurs versions d'usages recommandés à un instant donné.

### La composition du CCT

Le CCT contient des référentiels pour un usage immédiat et opérationnel :

- Référentiels des produits et des versions
- Référentiels des exigences et recommandations.
- Référentiels des services transverses ou socle.

Le CCT propose des outils clés pour le développement des applications/produits :

- Des patterns d'architecture.
- Des concepts d'architecture (Cloud Native, Datas....)
- Un volet sécurité consistant.

Ce volet s'enrichit et évolue tout au long du cycle de vie du CCT

### Objectif du CCT

Le CCT s'applique à l'ensemble des acteurs du Ministère impliqués dans son offre numérique, qu'ils soient internes ou externes.

Les exploitants / hébergeurs : pour leurs exigences d'exploitabilité, les développeurs au sein de la DNUM ou avec des prestataires externes. Le CCT les aide à intégrer leur produit dans l'écosystème ministériel et interministériel (description des interfaces).

Les architectes et intégrateurs. Le CCT les aide à s'orienter vers des architectures à la fois maîtrisées par le ministère et les plus appropriées au devenir du SI de l'État  
les services accompagnant les passations de marché (au travers des clausiers et de la notation des offres proposés dans le guide mentionné plus haut)

Pour tous ces acteurs le CCT se veut, plus qu'un cadre normatif contraignant, un outil réellement utile dans l'exercice de leurs différentes fonctions.

Il est aussi une plate-forme :

- de discussion et mise en relation avec les communautés de compétences du ministère
- d'exposition des offres de service des différents acteurs de la DNUM.

### Gouvernance

La gouvernance du CCT s'appuie sur un comité animé par SMART au sein de la DNUM.



Le comité est collégial, constitué de référents mandatés par les principales sous directions de la DNUM.

Les décisions sont prises à la majorité des voix des référents présents (titulaire ou suppléant).

Au titre de son activité CCT, le comité d'architecture se réunit au moins deux fois par an pour valider la publication des mises à jour semestrielles du CCT.

En dehors de ces deux réunions annuelles, le comité a toute latitude pour organiser les travaux sous forme de groupes de travail ad-hoc. Ces groupes de travail peuvent intégrer des participants n'appartenant pas au comité.

### **Contribution du comité d'architecture au CCT :**

Il est en charge :

- du pilotage du cadre de cohérence technique ministériel ;
- de la préparation des réunions du comité CCT ;
- du suivi et de la prise en compte des normes et standards ;
- de la veille technologique sur les composants et produits référencés au CCT.

### **Contribution du comité d'architecture au CCT : les référents contributeurs du CCT**

Dans le périmètre de leur entité de rattachement, ils sont chargés :

- du recueil des demandes d'évolution et de la préparation des dossiers présentés en comité ministériel ;
- du contrôle de l'application du CCT ;
- de l'information au sein de leur entité, et tout particulièrement de la sensibilisation des chefs de projets.



## 01 - REFERENTIEL PRODUITS

- Gestion du cycle de vie des produits
- Colonnes version et Disponibilité
- Identifier ou récupérer les produits
  - Référentiels Legacy :
  - Catalogue CAAS :
- Qui peut faire une demande d'une inscription de produit au référentiel
- Référentiel des produits
  - Comment lire le référentiel
    - Socle & hébergement
    - Base de données
    - Langages de développement
    - Serveur web
    - Middlewares
    - Produits - CMS
    - Produits - Mesure d'audience
    - Produits - Ged
    - Produits - Editique
    - Produits - BI
    - Produits - API Manager
    - Produits - Transfert de fichiers
    - Poste de travail
    - Sécurité - Gestion des certificats
    - Sécurité - Authentification et Identité
    - Fabrique du logiciel - socle de développement
    - Fabrique du logiciel - CI/CD
    - Fabrique du logiciel - Gestion de projet Test
    - Fabrique du logiciel - Performance
    - Fabrique du logiciel - Audit de Code
    - Fabrique du logiciel - Automatisation des Tests -IMT

## Organisation du référentiel

- Les composants de base : ce sont les briques de base d'un système d'information. Ils n'ont pas vocation à fonctionner seul et ne fournissent pas de services finaux aux utilisateurs métiers, mais sont très structurants pour le SI. Leur rôle est de fournir des services à d'autres composants ou applications.
- Les outils métier informatiques, qui permettent à la fois de créer le service (outils de génie logiciel) et de maintenir ce service (outils de sauvegarde, de supervision, de déploiement...etc)
- Les services applicatifs transverses. Ceux-ci font souvent l'objet d'une offre de service, comme les offres de SSO bâties sur le composant LemonLDAP::NG, LDAP etc...

Les produits non présent dans le CCT ne sont pas exclus de tout possibilité d'usage en production mais soit soumis à dérogation SMART ou B2SI ou utilisable dans un périmètre métier restreint (exemple Python pour le BI), et le support est de la responsabilité du demandeur.

## Gestion du cycle de vie des produits

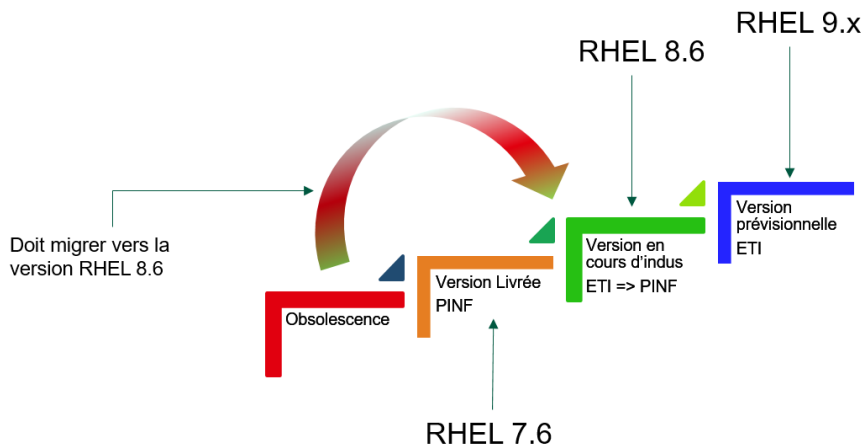
Chaque produit est porté par un ou plusieurs services ou acteurs du SNUM qui participent à la formalisation du cycle de vie du produit dans le CCT. Le maintien d'un produit au CCT doit être reconsidéré à interval régulier lors des Comités CCT. La sortie d'un produit du CCT doit notamment être envisagé dans les cas suivants :

- stagnation ou diminution significative du nombre de projet employant le produit depuis son inscription ;
- emploi du produit chez un seul acteur SNUM sans preuve de projet d'adoption par les autres ;
- impossibilité pour les membres du comité CCT d'identifier un porteur du produit ;
- obsolescence du produit.

## Colonnes version et Disponibilité

La colonne version indique le numéro de version, si une version supérieure est en préparation il convient de s'interroger d'attendre une date de disponibilité de la version plutôt que partir sur une version obsolète.





Les actions possibles sont indiqués dans la colonne Disponibilité MJ

Code	Actions
<b>A RETIRER</b>	Il est nécessaire que le projet upgrade le composant pour une version à jour et supporté.
<b>DISPONIBLE</b>	La version est disponible et qualifiée par et/ou pour le MJ,
<b>EN PRÉPARATION</b>	La version est en cours d'industrialisation ou de qualification, la version qui va être déployé dans un avenir proche.  Elle peut être demandée dans un mode dérogatoire dans des cas exceptionnels. (besoin éditeur).
<b>A QUALIFIER</b>	Demande d'étude ou de qualification d'une version (ou d'un produit nouveau). Cette demande peut être réalisée uniquement par les responsables du produit.

## Identifier ou récupérer les produits

La colonne Catalogue- Fournisseur indique où récupérer la version à jour du produit. Il est recommandé d'utiliser des produits qualifiés par le Ministère ou supportés par un éditeur référencé et dans la version déployable par les processus d'industrialisation du Ministère.

Si un produit ne figure pas dans le référentiel il est soumis à validation des architectes pour un usage limité au contexte projet avec un support spécifique.

Il n'est pas identifié au Ministère un catalogue unique mais la récupération des produits doit se conformer aux garanties offertes par le support d'éditeur ou la qualification MJ.

La colonne référence indique l'ID du produit, le champs n'est pas complet et est en construction, il fait référence à un catalogue futur référençant les composants du CCT par famille de produit ou d'usage.

- VM (ou legacy par abus de langage).
- CAAS ([CODEO](#) ou [ULJ](#)).
- Application.
- Fabrique.
- Infrastructure.

## Référentiels Legacy :

- Produits supportés par Redhat accessible dans les repository(ies) Redhat, RHSC, extra ou epel, la version du produit est corrélée avec la distribution RHEL. => le mot clé distrib indique l'origine du produit.
- Produits packagés et qualifié par le MJ, produits taggés mj\_ => mj indique que le produit est bien issu d'un package réalisé par le mj. [Midd leware](#) - [Provisionnement des infrastructures](#) - [CODEO](#) - [WIKI \(justice.gouv.fr\)](#) - [/shared/software](#)
- Produit éditeur validé en COMARCH et dont l'usage est répandu au sein du SNUM. => éditeur indique que le produit est issu des repo d'un éditeur, potentiellement sous licence.



## Catalogue CAAS :

Un produit déployé sur la plateforme CAAS est construit à partir d'une image qualifiée par le MJ. Il peut être délivré sous forme :

- D'une image sur laquelle il peut être ajouté un ou plusieurs composants.
- D'un chart Helm construit à partir de 1 ou plusieurs Images.
- D'un operator red hat ou fourni par un éditeur.

L'origine des produits est issu :

- Du catalogue Redhat et supporté par Redhat.
- Du catalogue VMWare Tanzu Application et supporté par Broadcom.
- D'un catalogue externe validé par le MJ et intégré dans la plateforme CAAS.
- d'un produit fabriqué et qualifié par le MJ.

## Qui peut faire une demande d'une inscription de produit au référentiel

Tout ajout d'un nouveau produit ou langage dans le CCT en particulier qui impacte la fabrication d'applications doit être évalué en COMARCH.

Les demandes de nouvelles versions peuvent être effectuée par :

- ETI et SMART pour le socle d'hébergement.
- SMART pour les langages.

Tout projet qui possède des licences d'un produit peut inscrire une nouvelle version de produit (VDR, SIGNA ...).

Pour les besoins éditeurs très spécifiques il peut être nécessaire de faire des demandes par anticipation, dans ce cas soit il y a une dérogation soit une priorisation à faire une demande.

## Référentiel des produits

### Comment lire le référentiel

#### Socle & hébergement

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
VM	Red Hat Enterprise Linux	Redhat	RHEL < 7.6	NON DISPONIBLE	<b>HORS SUPPORT ÉDITEUR</b>  Socle OS pour le déploiement de VM pour des projets standard.
VM	Red Hat Enterprise Linux	Redhat	RHEL 7.6	NON DISPONIBLE	<b>HORS SUPPORT ÉDITEUR</b>  Socle OS pour le déploiement de VM pour des projets standard.  Plus disponible au 31 /11/2024.
VM	Red Hat Enterprise Linux	Redhat	RHEL 7	A RETIRER	<b>HORS SUPPORT ÉDITEUR</b>  Socle OS pour le déploiement de VM pour des projets standard.  Indisponibilité envisagé le 31/12/2024



VM	Red Hat Enterprise Linux	Redhat	RHEL 8	DISPONIBLE	<p>Socle OS pour le déploiement de VM pour des projets standard.</p> <p>Version minimale 8.10 à partir de nov 2024.</p> <p>Version mineur RHEL 8.8 annoncé en COPIL dette technique 23 mai 2024.</p>
VM	Red Hat Enterprise Linux	Redhat	RHEL 9	EN PRÉPARATION	Socle OS pour le déploiement de VM pour des projets standard.
VM	Windows	Microsoft	Windows < 2016	A RETIRER	Socle OS pour le déploiement de VM pour des projets standards nécessitant un serveur Windows
VM	Windows	Microsoft	Windows 2022	DISPONIBLE	Socle OS pour le déploiement de VM pour des projets standards nécessitant un serveur Windows
VM	Windows	Microsoft	Windows 2025	A QUALIFIER	Socle OS pour le déploiement de VM pour des projets standards nécessitant un serveur Windows
CAAS	Openshift	Redhat	OCP 3	A RETIRER	<p><b>HORS SUPPORT ÉDITEUR</b></p> <p>Orchestrateur de Container pour la solution Container As A Service du Ministère.</p> <p>Arrêt envisagé le 31/12 /2025</p>
CAAS	Openshift	Redhat	OCP 4 min 4.14	DISPONIBLE	Orchestrateur de Container pour la solution Container As A Service du Ministère.
IAAS	VSphere	VMware	min 8.0u3	DISPONIBLE	
	VCenter	VMware	min 8.0u3	DISPONIBLE	

## Base de données

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
VM	Postgresql	mj - Postgresql	< 14	A RETIRER	Moteur SGBD recommandé pour les projets standards requérant une base de données relationnelles.
VM	Postgresql	mj - Postgresql	14	DISPONIBLE	Moteur SGBD recommandé pour les projets standards requérant une base de données relationnelles.
VM	Postgresql	mj - Postgresql	15	DISPONIBLE	Moteur SGBD recommandé pour les projets standards requérant une base de données relationnelles.



VM	Postgresql	mj - Postgresql	16	DISPONIBLE	Moteur SGBD recommandé pour les projets standards requérant une base de données relationnelles.
VM	Oracle	mj - Oracle	< 12g	A RETIRER	Moteur SGBD recommandé pour les projets critiques dont les besoin requèrent une base de données relationnelles avec des fonctions avancées.
VM	Oracle	mj - Oracle	19c	DISPONIBLE	Moteur SGBD recommandé pour les projets critiques dont les besoin requèrent une base de données relationnelles avec des fonctions avancées.
VM	SQL Server Standalone	mj - Microsoft	2017 (RHEL)	DISPONIBLE	Moteur SGBD recommandé pour les projets dont les besoin requèrent une base de données relationnelles SQL Server.
VM	SQL Server / Windows - mutualisé	mj - Microsoft	2017 (Windows)	DISPONIBLE	Moteur SGBD recommandé pour les projets dont les besoin requèrent une base de données relationnelles pour le BI.
VM	SQL Server / Windows - mutualisé	mj - Microsoft	2022 (Windows)	A QUALIFIER	Moteur SGBD recommandé pour les projets dont les besoin requèrent une base de données relationnelles pour le BI.
VM	MariaDb	mj - MariaDb	10.3	DISPONIBLE	Moteur SGBD pour les projet utilisant un progiciel incompatible avec Postgresql.
VM	MariaDb	mj - MariaDb	10.11	A QUALIFIER	Moteur SGBD pour les projet utilisant un progiciel incompatible avec Postgresql.
VM	MongoDb	editeur - mongodb	4	A RETIRER	Base NoSQL orientés document.
VM	MongoDb	editeur - Mongodb Enterprise	6	DISPONIBLE	Base NoSQL orientés document.

## Langages de développement

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Application	JAVA	distrib - OpenJDK	8	A RETIRER	Langage de développement essentiellement pour le backend des applications du Ministère de la Justice
Application		distrib - OpenJDK	11	DISPONIBLE	
Application		distrib - OpenJDK	17	DISPONIBLE	
Application		distrib - OpenJDK	21	EN PRÉPARATION	
Application	PHP	distrib - php	< 8.2.x	A RETIRER	Langage de développement pour les applications /produits du Ministère



Application		distrib - php	8.2.x	DISPONIBLE	requérant le php. (CMS, produit et solution, POC, ...).
Application	Angular		>=17.x	DISPONIBLE	Framework de développement essentiellement pour le frontend des applications du Ministère de la Justice  Angular est le framework à <b>utiliser en priorité 1</b> .
Application	React		>=18.x	DISPONIBLE	Langage de développement frontend pour les applications/produits du Ministère.
Application	Python		>= 3.12.2	DISPONIBLE	Langage de développement <b>réservé exclusivement</b> pour <ul style="list-style-type: none"> <li>les travaux relatifs au domaine big data.</li> <li>aux domaines de l'intelligence artificielle (IA) et de l'ingénierie et de l'analyse de données, y compris avec l'utilisation de jeux de données et de grands modèles de langage ou <i>large language models</i> (LLM) <i>open source</i> hébergés</li> </ul>

## Serveur web

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Application	httpd	distrib - apache	2.4	DISPONIBLE	Serveur web, reverse proxy ou composant d'exécution pour les fpm php.
Application	NGINX	distrib - nginx	<1.18	DISPONIBLE	Serveur web, reverse proxy ou composant d'exécution pour les fpm php.
Application	NGINX	distrib - nginx	1.22		Serveurs web, performant. Exposition des Front Office.

## Middlewareas

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Application	tomcat	mj - apache	< 8	A RETIRER	Container d'exécution des applications métiers java.
Application	tomcat	mj - apache	9.x, 10.0	DISPONIBLE	Container d'exécution des applications métiers java.



Application	jboss	editeur - Redhat	< 8	A RETIRER	Serveur d'application java, uniquement pour les applications existantes.
Application	jboss	editeur - Redhat	8.0	DISPONIBLE	Serveur d'application java, uniquement pour les applications existantes. Pas de nouveaux projets utilisateurs de JBOSS.
Application	Redis	distrib - redis	6	DISPONIBLE	Base de données clé-valeur Disponible sur VM
Application	Redis	distrib - redis	7.4	DISPONIBLE	Base de données clé-valeur Disponible en conteneur
Application	Varnish	distrib - Varnish	6	DISPONIBLE	Service de cache statique.
Application	Elasticsearch	mj - elastic	7	A RETIRER	Moteur d'indexation standard pour les applications du Ministère.
Application	Elasticsearch	mj - elastic	8.x	DISPONIBLE	Moteur d'indexation standard pour les applications du Ministère.
Application	Artemis AMQ	editeur - Redhat	< 7.10	A RETIRER	MOM pour les échanges asynchrones
Application	Artemis AMQ	editeur - Redhat	7.10	A RETIRER	MOM pour les échanges asynchrones. Possède des failles de sécurité corrigées sur la 7.11
Application	Artemis AMQ	editeur - Redhat	7.11	DISPONIBLE	MOM pour les échanges asynchrones
CAAS - ULJ	Apache	VMware Tanzu Application Catalog - CODEO, ULMJ	2.4	DISPONIBLE	Image de conteneur basée sur UBI8
CAAS - ULJ	Apache Tomcat	VMware Tanzu Application Catalog - CODEO, ULMJ	10.1	EN PRÉPARATION	Image de conteneur basée sur UBI8
CAAS - ULJ	Elasticsearch	VMware Tanzu Application Catalog - CODEO, ULMJ	8.12	EN PRÉPARATION	Chart Helm basé sur UBI8
CAAS - ULJ	Java	VMware Tanzu Application Catalog - CODEO, ULMJ	17	EN PRÉPARATION	Image de conteneur basée sur UBI8
CAAS - ULJ	NGINX Open Source	VMware Tanzu Application Catalog - CODEO, ULMJ	1.25	EN PRÉPARATION	Image de conteneur basée sur UBI8
CAAS - ULJ	PHP-FPM	VMware Tanzu Application Catalog - CODEO, ULMJ	8.1	EN PRÉPARATION	Image de conteneur basée sur UBI8
CAAS - ULJ	PostgreSQL	VMware Tanzu Application Catalog - CODEO, ULMJ	16	EN PRÉPARATION	Image de conteneur basée sur UBI8, Chart Helm basé sur UBI 9



CAAS - ULJ	RabbitMQ	VMware Tanzu Application Catalog	3.10	DISPONIBLE	Image de conteneur basée sur UBI8
		- CODEO, ULMJ	3.12		
			3.13		
CAAS - ULJ	RabbitMQ	VMware Tanzu Application Catalog	3.12	DISPONIBLE	Chart Helm basé sur UBI8
		- CODEO, ULMJ	3.13		

Produits - CMS

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	Drupal	MJ	V10.x	DISPONIBLE	Gestion de contenu
Progiciel	Drupal	MJ	V9.x	A RETIRER	Gestion de contenu

Produits - Mesure d'audience

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	Matomo	MJ	V4.x	DISPONIBLE	Statistique de l'utilisation des applications (mesure d'audience)

Produits - Ged

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	Alfresco	Editeur - Hyland	7.1	DISPONIBLE	Gestion documentaire

Produits - Editique

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	BDOC	Editeur - Business Document (Inetum)	V6 et v7	A RETIRER	Production éditique.
Progiciel	Archimed	MJ		A RETIRER	Production éditique.
Progiciel	Opentext	Editeur - Open Text xstream CN	22.4	DISPONIBLE	Production éditique.



## Produits - BI

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	SAP BI	Editeur - SAP	4.1	A RETIRER	Solution pour l'analytique et restitution des indicateurs .
Progiciel	SAB BI	Editeur - SAP	4.2	DISPONIBLE	Solution pour l'analytique et restitution des indicateurs.
Progiciel	SAP BODS	Editeur - SAP	4.2	DISPONIBLE	Solution pour le traitement de la donnée pour l'alimentation des infocentres.
Progiciel	SAP BODS	Editeur - SAP	4.3	DISPONIBLE	Solution pour le traitement de la donnée pour l'alimentation des infocentres.

## Produits - API Manager

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	Kong - Control Plane	Editeur - Kong	3.6	DISPONIBLE	Console de management (GUI)
Progiciel	Kong- Data Plane	Editeur - Kong			API d'administration de la plateforme
Progiciel	Kong-Developer-Portal	Editeur - Kong			API Gateway
					Portail développeur de l'API Manager.

## Produits - Transfert de fichiers

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	SecureTransport Core	Editeur - Axway	5.5	DISPONIBLE	Plateforme d'échange sécurisé des fichiers
	SecureTransport Edge				
	Sentinel	Editeur - Axway			Supervision des échanges

## Poste de travail

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
-----------	-----------	-------------------------	---------	--------	--------------



Desktop	Edge Chromium	Editeur - Microsoft	120.x et ultérieures	DISPONIBLE	Mise à jour continue du navigateur recommandé des postes de travail des agents.
Desktop	Windows	Editeur - Microsoft	Windows 10 Enterprise 22H2 ou Windows 11 Enterprise	DISPONIBLE	Build OS MJ.
Desktop	Reader DC	Adobe	22.002	DISPONIBLE	Outil de lecture de pdf.
Desktop	Jabber	Editeur - Cisco		DISPONIBLE	Outil de visio conférence.
Desktop	Office 2021 Standard	Editeur - Microsoft		DISPONIBLE	Suite Office (word, excel, outlook ...)
Desktop	Libre Office Mimo	Editeur - The Document Foundation		DISPONIBLE	Suite libre Office.
Desktop	Gestion Carte Agent "production et qualification"	MJ	3.0	DISPONIBLE	
Desktop	Smart Card Middleware Desktop	Idopt - Imprimerie Nationale	6.22.2.14	EN PRÉPARATION	API format PKCS11 pour la lecture de la carte agent.
Desktop	MiddlewareIASECC	MJ	3.3.2	DISPONIBLE	Middleware pour la lecture de la carte agent.
Desktop	Agent Signa	MJ	v1.0.5	DISPONIBLE	Interface API poste de travail (middlewareAESC) et SIGNA en protocole PKCS11.
Desktop	WorldLineSignerXAdES Library	Atos Origin	1.0.9	DISPONIBLE	
Desktop	ClassicClient	Gemalto	6.30.500	DISPONIBLE	
Desktop	Lecteurs_Cartes	MJ	1.0	DISPONIBLE	
Desktop	Safenet Authentification Client	Thales	10.9	DISPONIBLE	Gestion des clés USB sécurisés Safenet pour les accès administrateurs.

#### Sécurité - Poste de travail

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Desktop	Trend Micro Apex One Security Agent	Editeur - Trend Micro	14.0.12534	DISPONIBLE	Antivirus Poste de travail
Desktop	HarfangLab Hurukai agent	Editeur - HarfangLab	2.30.12	DISPONIBLE	Agent EDR
Desktop	ZED !	Editeur – PRIM'X	2023.5	DISPONIBLE	Conteneurs Chiffrés
Desktop	CRYHOD	Editeur – PRIM'X	2023.5	DISPONIBLE	Chiffrement du poste de travail et des médias amovibles (Disques, clé USB)



Desktop	ZONECENTRAL	Editeur – PRIM'X	2023.5	DISPONIBLE	Service de confidentialité applicable sur l'ensemble des fichiers d'une organisation. Il permet de gérer le droit d'en connaître et protège les données sensibles contre les accès externes et internes en cloisonnant les informations entre utilisateurs et services ainsi que vis-à-vis des opérateurs IT.
Desktop	BitLocker	Editeur – Microsoft		EN PRÉPARATION	Chiffrement du poste de travail.
Desktop	VPN Justice	MJ	2.1.0	DISPONIBLE	

## Sécurité - Gestion des certificats

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Progiciel	EJBCA Community	editeur Keyfactor	8.2	DISPONIBLE	
Progiciel	ejbca - enterprise	editeur Keyfactor	Version licence entreprise EJBCA Software Appliance 2.5.1	EN PRÉPARATION	PKI ou IGC (Public Key Infrastructure) - gestion des certificats pour l'autorité Ministère de la Justice. (certificats serveurs, clients ...)
Progiciel	rôle Microsoft AD CS 2022	éditeur Microsoft	Windows 2022	DISPONIBLE	pour les machines Microsoft ou les clients NDES.

## Sécurité - Authentification et Identité

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
	LDAP 389 DS	editeur - Redhat	1.2	A RETIRER	Service d'annuaire pour la gestion des accès applicatifs.
	LDAP 389 DS	editeur - Redhat	1.3	DISPONIBLE	Service d'annuaire pour la gestion des accès applicatifs.
	LDAP 389 DS	editeur - Redhat	1.4	A QUALIFIER	Service d'annuaire pour la gestion des accès applicatifs.
Progiciel	ilex meibo	editeur - meibo	5.1	A RETIRER	Le système d'alimentation Meibo Provisionning de l'annuaire LDAP Pages Blanches.
Progiciel	ilex meibo	editeur - meibo	7.1	DISPONIBLE internet EN PRÉPARATION intranet	Le système d'alimentation Meibo Provisionning de l'annuaire LDAP Pages Blanches.
	LemonLDAP	editeur - LemonLDAP	V1.4	A RETIRER	Solution d'authentification SSO du ministère.



	LemonLDAP	editeur - LemonLDAP	V2.x	<div>DISPONIBLE</div> internet <div>EN PRÉPARATION</div> intranet	Solution d'authentification SSO du ministère.
--	-----------	---------------------	------	-------------------------------------------------------------------	-----------------------------------------------

Fabrique du logiciel - socle de développement

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Application	springboot	editeur - spring	< 2.7.18	A RETIRER	Framework de développement java, utilisé pour les applications standards du MJ, notamment pour celles en architecture microservice, cloud native.
Application	springboot	editeur - spring	2.7.18	DISPONIBLE	Framework de développement java, utilisé pour les applications standards du MJ, notamment pour celles en architecture microservice, cloud native.
Application	springboot	editeur - spring	3.1.x 3.2.x 3.3.x	A RETIRER DISPONIBLE DISPONIBLE	Framework de développement java, utilisé pour les applications standards du MJ, notamment pour celles en architecture microservice, cloud native.
Application	symfony	editeur - symfony	5.4.25	DISPONIBLE	
Application	symfony	editeur - symfony	6.4	A QUALIFIER	

Fabrique du logiciel - CI/CD

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
CAAS - ULJ	Jenkins	CODEO	2.150.3	DISPONIBLE	Orchestrateur de déploiement. En fin de vie.  Sera remplacé par Gitlab-Runner (ULMJ) courant 2024
CAAS - ULJ	Gitlab	CODEO	11.11.8 Community Edition	DISPONIBLE	Gestionnaire de code. En fin de vie.  Devrait être réinstallé /upgradé avec tous les dépôts projets dans l'ULMJ courant 2024.
CAAS - ULJ	Sonatype Nexus Repository	CODEO, ULMJ	3.64 PRO	DISPONIBLE	Registre d'image applicative, gestionnaire d'artefact et registre de chart.
CAAS - ULJ	Sonatype Nexus Lifecycle	ULMJ	169	EN PRÉPARATION	Gestionnaire de sécurité des dépendances de code  disponibilité prévue : 2024



 <b>MINISTÈRE DE LA JUSTICE</b> <i>Justice Équité Proximité</i> <b>SG/SNUM/SPG</b>	<b>Cadre de Cohérence Technique</b>  <b>Version Applicable</b>	Page 13 / 17  <b>Date application :</b> <b>25/11/2024</b> <b>Version : 9.2</b>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------	--------------------------------------------------------------------------------------------

CAAS - ULJ	GitlabRunner	ULMJ	1.12	EN PRÉPARATION	Opérateur Openshift Effectue les intégrations continues  disponibilité prévue : 2024
CAAS - ULJ	OpenShift GitOps (Argo CD)	ULMJ	1.8	EN PRÉPARATION	Opérateur Openshift Effectue les déploiements continus  disponibilité prévue : 2024
CAAS - ULJ	Helm	CODEO, ULMJ	3	DISPONIBLE	binaire Helm disponible dans l'image mj/cdsh: 3.5-ubi
CAAS - ULJ	UBI	Redhat	UBI 7	DISPONIBLE	Version des images de bases en usages dans le cluster Openshift du Ministère.
CAAS - ULJ	UBI	Redhat	UBI 8	EN PRÉPARATION	Version des images de bases en usages dans le cluster Openshift du Ministère.

## Fabrique du logiciel - Gestion de projet Test

Lien catalogue - [Outils](#)

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Fabrique	Jira	Editeur - Atlassian	9.4.14	DISPONIBLE	Framework pour le suivi de l'activité et la gestion des projets en fonction de la méthode de gestion adoptée (Kanban/Scrum).
Fabrique	Confluence	Editeur - Atlassian	8.5.9	DISPONIBLE	Ce service consiste à créer dans Confluence un espace de travail collaboratif (Wiki) pour le projet afin d'assurer la cohérence, le partage et la transparence entre les équipes.
Fabrique	Squash TM	Editeur - Hénix	5.1	DISPONIBLE	Cet outil permet la créati on d'un référentiel de test (exigences / cas de test) , l'exécution des campagnes de test et la mise à disposition des indicateurs d' avancement via les reports et les tableaux de bord.
Fabrique	Mantis	Editeur - Mantis	1.2.20	A RETIRER	Outil de ticketing en cours de décommissionnement.

## Fabrique du logiciel - Performance

Lien catalogue - [Test de Performance](#)

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Fabrique	JMeter	Editeur - Apache	5.4.3 sur les injecteurs de Nantes - DC3  et 5.6.3 sur les injecteurs de Rennes - DC1	DISPONIBLE	Injecteur



Fabrique	Elastic Search	Editeur - Elastic	8.9	EN PRÉPARATION	nécessite de passer en java 17
Fabrique	Elastic Search	Editeur - Elastic	7.17.15	DISPONIBLE	Stockage/indexation des données envoyées par l'APM Server. réponse aux requêtes de recherche
Fabrique	APM Server	Editeur - Elastic	7.17.15	DISPONIBLE	collecte des métriques remontées par les agents Elastic APM puis constitution de documents Elasticsearch envoyés aux serveurs du cluster Elasticsearch.
Fabrique	Kibana	Editeur - Elastic	7.17.15	DISPONIBLE	Visualisation et analyse des métriques.
Fabrique	Grafana	Editeur - Grafana	10	EN PRÉPARATION	Outil permettant de visualiser les métriques remontées par les injecteurs via Jmeter
Fabrique	InfluxDB :	Editeur - Influxdata	2.7.4	EN PRÉPARATION	Outil permettant de stocker les informations envoyées par les injecteurs pour Grafana

## Fabrique du logiciel - Audit de Code

Lien catalogue - [Sourcing et audits de code](#)

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Fabrique	Checkmarx SAST	Editeur - CHECKMARX	9.6.7	DISPONIBLE	Cet outil permet de réaliser des scans sur des fichiers de code source pour contrôler la sécurité du code source sur la base du référentiel de développement sécurisé OWASP top 10 2021
Fabrique	Cast AIP	Editeur - CAST	8.3.55	DISPONIBLE	Cet outil permet de faire des scans sur des fichiers de code source pour contrôler la qualité du code source sur la base du référentiel MITRE CWE embarquée par l'outil.
Fabrique	Owasp dependency Track	Communauté OWASP Dependency track	4.12	EN PRÉPARATION	Cet outil permet de faire des scans sur des fichiers de code source pour y détecter des vulnérabilités connues (CVE) à partir de diverses sources de vulnérabilités connues notamment la base NVD (National Vulnerability Database) du NIST

## Fabrique du logiciel - Automatisation des Tests -IMT

Lien catalogue - [Automatisation des tests](#)



Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Fabrique	KATALON Studio	Editeur - KATALON	9.6	DISPONIBLE	Cet outil permet le développement et l'exécution des tests automatisés sur le poste de travail (IDE)
Fabrique	KATALON RUNTIME ENGINE	Editeur - KATALON	9.6	EN PRÉPARATION	Cet outil permet le développement et l'exécution des tests automatisés sur le poste de travail (IDE)

**Service d'infrastructure - Agents - ETI**

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Infrastructure	Visual TOM	Editeur - Abyss	7	DISPONIBLE	Agent d'automatisation des tâches, ordonnancement.
Infrastructure	NRPE	Editeur - Centreon		DISPONIBLE	Agent de supervision Centreon
Infrastructure	NS Client			DISPONIBLE	Agent de supervision Centreon Windows
Infrastructure	SNMP	distrib - redhat	v3	DISPONIBLE	Supervision
Infrastructure	Elastic Agent	Editeur - Elastic Cloud Enterprise	8.x	DISPONIBLE	Agent observabilité Elastic - (beats elastic)
Infrastructure	Agent Veeam	Editeur - Veeam	12.1	DISPONIBLE	<<<à voir>>
Infrastructure	APM Agent	Editeur - Elastic Cloud Enterprise		DISPONIBLE	jar pour l'APM.
Infrastructure	ESET Management Agent	Editeur - ESET	10.0	DISPONIBLE	Agent antivirus serveur (Windows et Linux)
Infrastructure	syslog	distrib - redhat		DISPONIBLE	Collecte des logs

**Service d'infrastructure - Exploitation de l'infrastructure- ETI**

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
	Easyvista	Editeur - Easyvista	2022	DISPONIBLE	Solution ITSM bâtie sur le progiciel EasyVista, Plateforme de Gestion de services (IT : incidents, problèmes, changements, configurations, ...).
Infrastructure	Centreon	Editeur - Centreon	24.04	DISPONIBLE	Supervision des applications et des systèmes.
Infrastructure	Grafana	Editeur - Grafana	9.2.19	DISPONIBLE	Reporting des métriques des applications et du socle.
Infrastructure	ECE	Editeur - Elastic Cloud Enterprise	8	DISPONIBLE	Service d'observabilité
Infrastructure	VEEAM	Editeur - Veeam	12.1	DISPONIBLE	Service de sauvegarde.
Infrastructure	VTOM	Editeur - Abyss	7	DISPONIBLE	Ordonnanceur.

**Service d'infrastructure - Automatisation de l'infrastructure**

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
-----------	-----------	-------------------------	---------	--------	--------------



CI/CD	Gitlab	Editeur - Gitlab	15.11.9	DISPONIBLE	Gestionnaire de code - collaboration (wiki, partage)
CI/CD	Nexus - OSS	Editeur - Sonatype (Community Edition)	3.62.0	DISPONIBLE	Repository infra docker /raw/ruby/pypi
CI/CD	Satellite	Editeur - Redhat	6.14.4	DISPONIBLE	Gestion de la distribution du contenu RedHat en dc
CI/CD	AWX - Tower upstream	Editeur - Redhat	9.3.0	DISPONIBLE	Plateforme d'automatisation Ansible
	WSUS - Windows Server Update Services	Editeur - Microsoft	2022	DISPONIBLE	Déploiement des mises à jours des produits des serveurs Microsoft (jusqu'à Windows 2022).

#### Service d'infrastructure - Stockage

Référence	Composant	Catalogue - Fournisseur	Version	Statut	Commentaires
Infrastructure	NAS - Netapp	Fournisseur - NetApp - AFF 300	Ontap 9.12.1P8	DISPONIBLE	Stockage NFS, partage entre VM (A date uniquement pour la production).
Infrastructure	Stockage Objet - Observabilité	Fournisseur - NetApp Storage Grid (S3) - SG6060	11.7.0	DISPONIBLE	Stockage S3
Infrastructure	Stockage Objet - Métiers	Fournisseur - Hitachi HCP (Hitachi API)	G10 : 9.7.1.13 S11 : V4.0.0.23	DISPONIBLE	Stockage document de type S3 (API HCP), intégrité renforcé et versioning. Utilisation pour les ged applicatives.
Infrastructure	SAN	Fournisseur - Hitachi VSP 5600 (Nantes) VSP 5200 (Osny) upgrade en 5600 prévu en 2025	VSP : 90-09-25-00/00 Brocade : FOS 9.2.1a	DISPONIBLE	Stockage SAN.
Infrastructure	VSAN	HCI Hitachi et HCI Dell VXRAILS et vmware VSAN	vSAN8	DISPONIBLE	
Infrastructure	Stockage Objet - Sauvegarde	Fournisseur - Quantum active scale cold storage (S3) - P 200		DISPONIBLE	Interface pour stockage des sauvegardes DIT.
Infrastructure	Stockage déconnecté (bandes)	Fournisseur - Quantum Scalar I6 / Scalar I6000	Scalar I6 : > 305G Scalar I6000 : > 310G	DISPONIBLE	Stockage des sauvegarde.
Infrastructure	HCI	Fournisseur - Dell - Vxrails	min 8.0.310-28809519	DISPONIBLE	Infrastructure de virtualisation non critique
Infrastructure	HCI	Fournisseur - Hitachi - UCP	> 3.77	A RETIRER	Partiellement HORS SUPPORT EDITEUR
Infrastructure	HCI	Fournisseur - HPE - Simplivity	Version Simplivity : 4.1.1.639. Vcenter : 7.0U3o Esxi: 7.0U3c	A RETIRER	Dédié projet Harmonie

#### Load Balancing

Référence	Composant	Catalogue - Fournisseur	VersionStatut		Commentaires
-----------	-----------	-------------------------	---------------	--	--------------



Infrastructure	F5 Big IP - LTM	Fournisseur - F5	V17.1.1	DISPONIBLE	Gestion du load balancing et disponibilité des applications.  Exposition des VIPs sur les réseaux RPVJ, internet et intra DC.
Infrastructure	Haproxy		3.2	DISPONIBLE	Utilisé pour ECE

**Service d'infrastructure - Sécurité du socle**

Référence	Composant	Catalogue - Fournisseur	VersionStatut		Commentaires
Infrastructure	Big IP - AWAFF	F5	V17.1.1	DISPONIBLE	Web Application Firewall pour la protection des applications WEB, protège des attaques au niveau du protocole http et applicatif Web.
Infrastructure	Antivirus Server	ESET	10	DISPONIBLE	Antivirus déployé sur le parc serveur du Ministère.
Infrastructure	HSM	Fournisseur - Bull	X149	DISPONIBLE	Équipement hardware pour la gestion des clés, certificats.
Infrastructure	HSM - Firmware	Editeur - Bull	V147 - V1.3 - V0.5	A RETIRER	
Infrastructure	HSM - Firmware	Editeur - Bull		EN PRÉPARATION	
	Vault Secret	Hashicorp, ULMJ	v0X	A QUALIFIER	Opérateur Openshift  Effectue la synchronisation des secrets applicatifs de Vault Server au cluster Openshift 4  disponibilité prévue : 2024

**Service SSI - Cyberdéfense**

Référence	Composant	Catalogue - Fournisseur	VersionStatut		Commentaires
Composants internes non publiables (hors flux des acteurs CRC, flux sortants uniquement)					



## 02 - REFERENTIEL DES REGLES D'IMPLEMENTATION

Thématique	Règle		Applicabilité  O = obligatoire R = recommandé
<b>Gouvernance, Organisation, Méthodologie</b>	GEN-001	La mise en œuvre de tout nouveau produit / application doivent se conformer au CCT en vigueur.	O
	GEN-002	La mise en œuvre de nouveaux produits / applications non conformes au CCT en vigueur doit faire l'objet d'une demande de dérogation motivée.	O
	GEN-003	Tout choix de produit propriétaire doit faire l'objet d'analyse de la valeur préalable démontrant son avantage par rapport à des solutions open source voire du développement spécifique, dans le cadre du projet étudié.	O
	GEN-004	Une mise à niveau du socle technique doit être prévue pour toute application, tous les 18 mois au plus tard et le plan de migration technique doit être présenter au bureau SMART.	O
	GEN-005	Le développement spécifique des applications métiers doit utiliser les langages dans l'ordre des priorités indiqués dans le <a href="#">Référentiel Produits</a> .	O
		La conception d'une application est frugale vis à vis des ressources d'infrastructures consommées (Green IT).	
	GEN-006	Tout(e) nouveau(elle) produit /application doit être déclaré(e) dans le référentiel d'urbanisation du ministère de la Justice (URBI) avec attribution d'un code ministériel unique.	O
	GEN-007	La conception d'une application à partir d'un générateur de code dont les droits d'usage n'auraient pas été acquis par le ministère, lui permettant de maintenir ensuite le logiciel, n'est pas autorisée.	O
	GEN-008	Tout projet doit passer par les processus 'qualité' et 'audit' du Ministère de la Justice.	O
	GEN-011	Les exigences réglementaires CNIL /RGPD ainsi que la Directive spécifique police-justice s'appliquent au plus tôt dans la vie d'un projet.	O
	GEN-012	Toute mise en œuvre de produit /application doit faire l'objet d'une analyse de risque préalable. La phase de réalisation ne doit en aucun cas démarrer avant l'analyse de risque.	O
<b>Architecture micro services</b>  Compléments de lecture : cf. <a href="#">Microservices</a>	IMP-101	Chaque micro service est autonome dans le déploiement.	O
	IMP-102	Chaque micro service couvre un périmètre fonctionnel limité et cohérent.	O



Architecture résiliente « <i>design for failure</i> »	IMP-103	Les micro services respectent un couplage faible entre eux (cf. IMP-101, IMP-104), <b>notamment en termes de données</b> mais aussi en termes de traitement. Les micro services communiquent entre eux mais restent indépendants les uns envers les autres.	O
	IMP-104	Chaque micro service est capable de rendre un service fonctionnel minimum en cas de défaillances des autres micro services.	O
	IMP-105	Les micro services sont technologiquement indépendants les uns envers les autres.	O
	IMP-106	Tout micro service est <i>stateless</i> (sans état).	O
	IMP-107	Chaque micro service offre une intégration facilitée ; il est directement déployable au travers du conteneur qui le contient.	R
	IMP-108	Chaque micro service est réutilisable.	O
	IMP-201	Toute architecture respecte un couplage faible avec les systèmes tiers.	O
	IMP-202	Toute architecture <b>rend un service fonctionnel minimum, en cas de défaillances</b> des systèmes connexes.	O
	IMP-203	La problématique de disponibilité (suivant les exigences <b>DICT</b> ) est traitée <b>dès les phases d'architecture et de conception de l'application</b> : <ul style="list-style-type: none"> <li>• identification des points de faiblesse (« SPOF : Single Point Of Failure ») ;</li> <li>• identification des points de contention (« SPOC : Single Point of Contention »).</li> </ul>	O
	IMP-204	La conception d'une nouvelle architecture comme la rénovation d'une architecture existante/legacy tient compte de la résilience attendue et du niveau de disponibilité fixé par le propriétaire des risques identifiés en amont. Le niveau de résilience s'applique : <ul style="list-style-type: none"> <li>• localement, sur le ou les sites d'hébergement (haute-disponibilité sur site) ;</li> <li>• entre les sites, par le biais des mécanismes de réplication (haute-disponibilité intersite).</li> </ul>	O
	IMP-205	La conception d'applications critiques (D >= 3) repose sur les principes favorisant les échanges et répliqués multisites.	O
	IMP-206	La nécessité d'un PCI/PRI est prise en compte dès la phase de conception des applications critiques.	O
	IMP-207	Les applications métiers sont conçues en totale compatibilité avec l'extensibilité/scalabilité horizontale de l'environnement technique qui les hébergent (augmentation du nombre de nœuds/machines).	O



	IMP-208	Les applications métiers sont conçues en totale compatibilité avec l'extensibilité/scalabilité verticale de l'environnement technique qui les hébergent (augmentation de la capacité pour un nœud existant /machine existante).	O
	IMP-209	Les campagnes de tests de performance doivent être réalisées pour toute produit/application à portée nationale avant sa mise en production.	O
<b>Architectures et infrastructures « cloud ready »</b>	IMP-301	Les micro services sont conteneurisés (cf. IMP-107).	R
	IMP-302	Les conteneurs portant les micro services bénéficient d'un moteur d'orchestration qui facilite leur organisation et leur exploitation compte-tenu des ressources disponibles.	R
	IMP-303	L'architecture est conçue dans un modèle d'architecture distribuée, en termes d'environnement d'exécution (cluster) comme en termes de données (data stores).	R
	IMP-304	L'architecture est conçue en conformité avec les propriétés attendues dans un modèle MSA (micro services architecture).	O
	IMP-305	Les architectures <i>cloud ready</i> s'appuient sur un ou plusieurs bus de messages, selon les domaines applicatifs/domaines métier à décliner et à cloisonner entre eux (conformément à la définition de la valeur du critère de sécurité 'confidentialité' lors de l'étude DICT).	R
	IMP-306	Intégration continue et déploiement continu sont nativement pris en compte dans les processus d'automatisation.	O
	IMP-307	Implémentation de traçabilité de bout en bout pour l'imputabilité et l'observabilité.	R
	IMP-308	Implémentation des mécanismes permettant la supervision.	O
<b>Architecture des applications « security by design »</b>	IMP-401	Implémentation de la protection des accès aux services par jeton d'authentification cf. <a href="#">Principe d'authentification</a>	O
	IMP-402	Implémentation de la protection des services suivant les habilitations.	O
	IMP-403	Implémentation de la protection des données au regard du droit d'en connaître le cas échéant.	O
	IMP-404	Implémentation de la protection des données sensibles par un mécanisme de chiffrement le cas échéant	O
	IMP-405	Implémentation des traces d'audit de sécurité	O
	IMP-406	Respect des règles de cloisonnement réseau, notamment internet/intranet	O
	IMP-407	Implémentation de la protection contre les attaques malveillantes connues (CSRF, XSS, ...) par les mécanismes de filtres HTTP	O



## Cadre de Cohérence Technique

### Version Applicable

	IMP-408	Mise en oeuvre les mesures nécessaires afin de garantir la sécurité du code logiciel et de leur conception au regard du TOP-10 de l'OWASP, <i>a minima</i> .	O
	IMP-409	Tout port non nécessaire au fonctionnement normal d'une application est fermé.	O
	IMP-410	La conception d'applications répond à une architecture susceptible d'être décentralisée, via des flux intersites, dont le fonctionnement privilégie le passage par la PFE.	O
	IMP-411	Toute application/service applicatif exposé est publié via un composant de filtrage de contenu (de type Web Application Filtering) et un reverse-proxy.	O
	IMP-412	Les téléversements de fichiers doit faire l'objet d'une analyse antivirus en amont du flux, avec prise en charge de la gestion des erreurs par l'application à l'origine du téléversement.	O
	IMP-413	Dans les centres d'exploitation, les données ne sont pas stockées sur les serveurs mais sur des systèmes partagés (exemple SAN/NAS).	O
	IMP-414	Une application ne peut accéder directement à la base de données d'une autre application.	O
	IMP-415	Pour le 'tiers' serveur base de données, les solutions de haute disponibilité unifiées, standard, et industrielles à disposition dans les centres de service sont privilégiées. A défaut, les solutions fournies par les moteurs SGBD seront utilisées.	O
<b>Principe de mutualisation</b>	SEC-101	La mutualisation d'infrastructures (au niveau physique) et de services (au niveau logique) est possible pour des raisons de construction (selon existant), de moyens, de coûts et ce, dans le respect des conclusions de toute étude de risques préalable.	R
<b>Principe d'authentification</b>	SEC-201	Tout utilisateur est authentifié au sein du SI.	O
	SEC-202	Tout service/application est authentifié au sein du SI.	O
	SEC-203	L'authentification des utilisateurs pour les accès aux applications /produits doivent s'appuyer sur les services socles de confiance SSO et /ou Kerberos du Ministère.	O
	SEC-204	Les besoins propres des applications - en identification, authentification, autorisation - ne donnent pas lieu à la duplication du référentiel d'identité / annuaire ministériel (LDAP/AD). S'agissant de progiciel, si le besoin d'import du référentiel d'identité / annuaire ministériel s'avère nécessaire, ce point doit faire l'objet de justification.	O



## Cadre de Cohérence Technique

### Version Applicable

	SEC-205	Si une application du ministère est accessible à des utilisateurs d'une autre administration, à partir de leur infrastructure (via RIE par exemple), le principe de délégation (autour de l'authentification et du respect des droits d'accès) s'effectue exclusivement sous conditions de garanties de sécurité définies au préalable.	O
Principe d'autorisation	SEC-301	L'usage des services applicatifs est protégé conformément aux habilitations.	O
	SEC-302	Les habilitations de premier niveau (profils) sont gérées par l'annuaire LDAP/AD ministériel.	O
	SEC-303	Les habilitations fines (permissions) sont gérées par les applications.	O
	SEC-304	Les habilitations (par exemple, les droits fins d'une application) associées aux utilisateurs sont contenues dans une base protégée.	O
	SEC-305	Si une application du ministère est accessible à des utilisateurs d'une autre administration à partir de leur infrastructure (via RIE par exemple), l'authentification et la gestion des droits de ces utilisateurs ne peuvent être déléguées qu'à condition d'apporter des garanties de sécurité.	O
	SEC-306	Les autorisations réservées aux comptes à privilège pour les actes d'administration sont gérées via un référentiel d'identité et d'accès dédié, distinct du référentiel utilisateur.	O
Principe d'accès	SEC-401	Tout accès au SI est conçu conformément aux exigences réglementaires en vigueur, selon le niveau d'homologation ou d'usage visé et en adéquation avec le niveau d'habilitation des futurs utilisateurs du SI considéré.	O
	SEC-402	Les besoins d'accès à une application via le VPN du Ministère sont pris en compte dès le début du projet	O
	SEC-404	Les besoins d'accès à Internet des applications, à partir des datacenters, doit faire l'objet d'une autorisation explicite déclinée sous la forme d'une inscription des URLs cibles dans une liste blanche.	O
Principe de cloisonnement	SEC-501	Les règles de cloisonnement réseau (en vertical pour décomposer la chaîne de communication dans un DC et en horizontal pour distinguer les composants par usage ou par application) sont respectées, conformément aux bonnes pratiques.	O
	SEC-502	Les services Internet et les services Intranet sont cloisonnés et disjoints. Le non-respect de ce principe d'architecture donne lieu à un no-go de change ou à un retrait du service le cas échéant. Tout échange nécessaire entre une zone dite Internet et une zone dite Intranet est soumis à étude : la conformité réglementaire au regard des classes de réseau (cf. II901) s'applique.	O
	SEC-503	Chaque grande zone réseau est délimitée par un équipement de filtrage (pare-feu).	O



	SEC-504	Toute fonction d'administration technique (moyens et réseaux associés) est distincte des fonctions d'utilisation.	O
	SEC-505	Tout composant appartient exclusivement à la zone au sein de laquelle il est positionné.	O
<b>Principe de journalisation - traçabilité - audit</b>	EXP-101	<p>La journalisation est prévue dès la conception de l'application :</p> <ul style="list-style-type: none"> <li>▪ au titre de l'exploitation par les outils de supervision métiers,</li> <li>▪ au titre de la supervision applicative,</li> <li>▪ au titre de la supervision de sécurité,</li> </ul> <p>en indiquant notamment les personnes autorisées à y accéder, le mode d'administration et la durée de conservation/séquestre des traces.</p>	O
	EXP-102	Les journaux respectent les formats et les normes d'exploitation définis ou retenus par le ministère.	O
	EXP-103	La traçabilité des actions de gestion des utilisateurs et de leurs droits est assurée.	O
	EXP-104	La journalisation, au travers du niveau de détail des événements collectés, autorise contrôles et audits à tout moment.	O
	EXP-105	La journalisation repose sur un mécanisme de diffusion du temps de référence qui est homogène au sein du SI.	O
<b>Principe de sauvegarde</b>	EXP-201	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en œuvre par le ministère.	O
	EXP-202	Toutes infrastructures de sauvegarde et moyens associés respectent la cohérence du principe de cloisonnement mis en œuvre au sein du SI.	O
	EXP-203	Tout besoin de sauvegarde fait l'objet d'un plan de sauvegarde formalisé.	R
	EXP-204	Tout besoin de sauvegarde fait l'objet d'une étude en adéquation avec le cadre PCI/PRI retenu.	R
<b>Principe d'administration technique</b>	SEC-601	L'administration technique d'une ressource (EAR, SEC, SYS, APP, DB) s'effectue au travers d'une interface réseau dédiée.	O
	SEC-601	Dans le cas de contraintes physiques avérées et par dérogation, le mécanisme de trunk de VLAN autorise la mutualisation sur une même interface et un même réseau physique le transport d'un VLAN métier et d'un VLAN admin.	R
<b>Sécurité réseau</b>	SEC-701	Hors DC, pour les sites web exposés sur Internet, le RIE et RPVJ, les accès sont en TLS 1.3.	O
	SEC-702	Des mécanismes de filtre HTTP protègent contre les attaques malveillantes connues (CSRF, XSS, ...).	O
	SEC-703	Pour tout équipement de filtrage, tout flux non explicitement autorisé est interdit (principe des règles explicites).	O



## Cadre de Cohérence Technique

### Version Applicable

	SEC-704	Les fonctionnalités de routage sont portées par le cœur de réseau.	O
	SEC-705	Pour les communications inter-sites (via nuage RIE par exemple), le chiffrement des flux sur une cryptographie à l'état de l'art est étudié et mis en oeuvre. Les tunnels de communication sont créés à partir de clés de chiffrement répondant aux exigences de sécurité et à la maîtrise des équipes qui en ont la charge.	O
	SEC-706	Les flux dédiés à la réplication de données intersite bénéficient de pare-feux de réplication dédiés.	R
Sécurité des systèmes	SEC-801	Tout poste de travail est équipé d'un antivirus et autre solution EDR qualifiés par le ministère (à jour de base antivirus si existante).	O
	SEC-802	Tout serveur (hors DC / AD) est équipé d'un antivirus et autre solution EDR qualifiés par le ministère (à jour de base antivirus si existante).	O
	SEC-803	Tout système d'exploitation, client comme serveur, est délivré selon des objectifs de sécurité prédéfinis, en termes de sécurisation/maîtrise des configurations comme en termes de MCS.	O
Sécurité des données	DTA-101	Les droits d'accès / autorisations sur les données garantissent le respect du besoin d'en connaître.	O
	DTA-102	Les droits d'accès / autorisations sur les données garantissent le respect du principe de moindre privilège.	O
	DTA-103	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en oeuvre par le ministère.	O
	DTA-104	<b>L'usage de triggers au sein d'un SGBDR, sauf contrainte majeure traitée par dérogation soumise à autorisation écrite du Ministère, n'est pas autorisé. Le cas échéant, le projet devra - au préalable - soumettre à validation cette utilisation en fournissant sa justification.</b>	O
	DTA-105	<b>L'usage de procédures stockées au sein d'un SGBDR, sauf contrainte majeure traitée par dérogation soumise à autorisation écrite du Ministère, n'est pas autorisé. Le cas échéant, le projet devra - au préalable - soumettre à validation cette utilisation en fournissant sa justification.</b>	O
	DTA-106	<b>L'usage d'un système de type Dblink (database link) au sein d'un SGBDR n'est pas autorisé.</b>	O
	DTA-201	La documentation propre à chaque base de données centrale est constituée au minimum d'un dictionnaire de données, d'un ensemble de règles de gestion, et d'un modèle conceptuel de données (ou d'un diagramme de classe). Cette documentation, actualisée en fonction d'éventuelles mises à jour, est consultable.	O



	DTA-202	Les volets conservation / archivage / séquestre des documents est à prendre en charge dès la conception : <ul style="list-style-type: none"> <li>• pour quelle durée ?</li> <li>• à quel moment doit-il être détruit ou basculé sur un serveur d'archivage dans un format pérenne ?</li> <li>• pour quelles autorisations et quels profils/rôles d'utilisateurs spécifiques (ex. pour le séquestre : <i>Security Officer</i>) ?</li> </ul>	O
	DTA-203	Le système de référentiel justice ministériel (SRJ) est utilisé pour toute produit/application ayant besoin de données référentielles métier.	O
	DTA-204	L'utilisation du système de référentiel justice ministériel passe par les API. Tout import du SRJ dans un SI pour des usages locaux est à justifier.	O
	DTA-205	Un processus de mise à jour régulière du référentiel pour les applications utilisant une copie du référentiel est réalisé.	O
	DTA-206	Les modifications locales sur des données provenant d'un référentiel ne sont pas autorisées.	O
	DTA-207	Lorsqu'une application comporte à la fois des données actives et des données historiques, elles sont stockées dans des bases ou des fichiers différents.	O
	DTA-208	Les applications prennent en compte les processus et les traitements d'exportation et de mise à disposition de leur données aux fins d'analyse, de statistiques et ce, dès la conception de l'application (hors réplication des bases).	O
	DTA-209	Les formats PDF, TXT, XML, et HTML sont utilisés pour l'affichage des documents.	O
	DTA-210	Le format PDF (Portable Document Format) est utilisé pour la présentation des impressions à la demande.	O
	DTA-211	Acrobat Reader est utilisé pour manipuler le format PDF, offrant des possibilités de visualisation, d'impression ou d'échange.	O
	DTA-212	Les services d'édition mutualisés (cf. 03 - Référentiels des services socles) sont à utiliser pour toute application nécessitant de fusionner des trames avec des données métier : les cas d'usage qui requièrent ces services concernent notamment dans le cadre des éditions dites "interactives".	R
Règles d'intégration	IMP-601	Les processus d'intégration et de déploiement sont compatibles avec le socle CI/CD du Ministère de la Justice ou Interministériel.	O
	IMP-602	Le déploiement des applications est automatisé.	R
Expérience utilisateur et accessibilité	IMP-701	Découplage IHM / services de traitement	R
	IMP-702	Prise en compte du Référentiel général d'amélioration de l'accessibilité (RGAA), version 4.1	O



## Cadre de Cohérence Technique

### Version Applicable

	IMP-703	Prise en compte du Design System de l'Etat (DSFR) version 1.10 et plus, a minima pour les services exposés sur Internet	R
	IMP-704	Toute application vise le minimum d'adhérence au poste de travail. Elle est indépendante du système d'exploitation (OS) de ce poste de travail. En conséquence : il s'agit d'une application WEB - c'est à dire une application qui s'appuie sur les protocoles et langages standardisés du web (HTTP/HTTPS, HTML, CSS, JavaScript).	O
	IMP-705	Les nouvelles applications fonctionnent sur les navigateurs et périphériques utilisés par les clients usagers sur l'intranet; les périphériques comprennent également les terminaux mobiles. Sur Internet, toute application web est conçue afin d'offrir des IHM et une ergonomie adaptées aux navigateurs, terminaux mobiles du moment. De manière générale, les applications web doivent implémenter le fonctionnement dit "web responsive design"	R
	IMP-706	Toute règle de contrôle est implémentée dans la couche IHM en respectant les contraintes d'accessibilité.	R
	IMP-707	Les contrôles réalisés (en JavaScript) sur le client sont vérifiés sur le serveur lors des appels de services.	O
	IMP-708	Les contrôles réalisés (en JavaScript) sur le client sont vérifiés sur le serveur lors des appels de services.	O
API REST	API-101	La sémantique de nommage du standard API est respectée.	R
	API-102	Implémentation de la documentation aux normes OpenAPI.	O
	API-103	Pour toute donnée, les conditions d'une possible réutilisation sont envisagées. Dans le cas pratique, la conception d'une API est envisagée pour toute nouvelle application.	R
	API-104	Les API sont clairement définies et documentées afin de faciliter leur consommation future.	O
	API-105	Un catalogue d'API est maintenu à jour au sein du Ministère.	R
	API-106	Les composants fonctionnels manifestement communs à plusieurs applications sont développés sous forme de services réutilisables.	O
	API-107	Les données existantes sont réutilisées.	O
	API-108	API et bibliothèques sont utilisées pour interagir avec les autres systèmes (système de gestion de base de données, système d'exploitation, etc.).	O
	API-109	Les API sont analysées en termes de sécurité de code logiciel avant leur publication.	O
	API-110	Les API sont suivies au titre du contrôle d'erreurs de configuration.	O
Echanges	EXC-101	Les flux fichiers de types externes /partenaires doivent passer par la plateforme d'échange ministériel.	O
	EXC-102	Les flux fichiers de types internes doivent passer par la plateforme d'échange ministériel.	O



## Cadre de Cohérence Technique

### Version Applicable

Page 10 / 10

Date application :  
25/11/2024  
Version : 9.2

	EXC-102	Les flux fichiers inter-domaines métiers passent par la plateforme d'échange ministériel.	R
	EXC-103	Les flux fichiers prennent en compte les besoins de monitoring, de reprise des données pour leur bonne exploitation.	O
	EXC-104	Tout échange inter-applicatif synchrone est mis en oeuvre sous forme d'API Rest.	O
	EXC-105	Les échanges par Web Service ou API permettent de s'assurer de l'identité du partenaire.	O
	EXC-106	Des solutions garantissant l'intégrité de l'information dans le cadre d'échanges inter-applicatifs sont mises en oeuvre.	R
	EXC-107	Le format de container Zed est le format à utiliser pour l'échange de données sensibles entre utilisateurs.	O
	EXC-108	Tout transfert de fichier depuis et vers une application métier fait l'objet d'une analyse préalable.	O
	EXC-108	Tout transfert de fichier depuis et vers une application métier fait l'objet d'une analyse préalable.	O
Exploitation/Automatisation /Infrastructure	EXP-301	La publication d'applications aux utilisateurs repose sur un nom de service qualifié (FQDN) et non une adresse IP.	O
	EXP-302	Les applications nationales Intranet utilisent un nom de domaine de type *.intranet.justice.gouv.fr. (à venir sso.intranet.justice.gouv.fr)	O
	EXP-303	Tout serveur synchronise son horloge sur le serveur NTP du Ministère ou sur l'un de ses relais officiels.	O
	EXP-304	Le mode conteneurisé Openshift, pour les applications métier, est privilégié - système d'exploitation Linux lorsque ce n'est pas possible.	R
	EXP-305	Chaque service applicatif exécuté sur un serveur repose sur un compte technique/compte de service qui lui est propre.	O
	EXP-306	L'utilisation de comptes à privilèges de type administrateur (root) ou utilisateur (personne physique) n'est pas autorisé.	O
	EXP-307	La planification de tâches/batches utilise un logiciel d'ordonnancement parmi ceux en vigueur au centre de production.	O
	EXP-308	Les applications s'appuient sur le socle technique des postes de travail en vigueur au Ministère.	O
	EXP-309	Les applications s'appuient sur les services socles du Ministère de la Justice et/ou les services socles Interministériel.	O



## 03 - REFERENTIEL DES SERVICES SOCLES

### Sommaire

1. [Annuaire - LDAP](#)
2. [Annuaire et authentification](#)
3. [Coffre-fort électronique](#)
4. [Signature électronique](#)
5. [GED et stockage de documents](#)
  1. [GED](#)
  2. [COLLABORATIF](#)
  3. [Stockage de document](#)
6. [Observabilité](#)
7. [SMTP](#)
8. [Plateforme d'échange](#)
9. [Messageries](#)
10. [Editique](#)
11. [Proxy](#)
12. [Archivage](#)
13. [PKI](#)
14. [Service Interministériel](#)
15. [Plateformes d'échange](#)
16. [Bastions d'administration](#)
17. [Antivirus](#)

### Annuaire - LDAP

#### Les principaux annuaires ministériels

Zone	Produit	Services	Descriptions
Intranet RIE	<a href="#">LDAP</a>	Annuaire des utilisateurs intranet MJ. Utilisateur partenaires RIE. Prend en charge la gestion des profils applicatifs	Cet annuaire est synchronisé tous les jours avec l' <a href="#">ActiveDirectory</a> .
Internet	<a href="#">LDAP</a>	Annuaire des utilisateurs extranet MJ. Ne prend pas en charge la gestion des profils applicatifs	
Intranet RIE	Active Directory	Annuaire des utilisateurs / poste de travail	

#### Outils de gestion d'annuaire

Zone	Produits	Services	Descriptions
Intranet	Meibo	Provisioning/Administration des utilisateurs	
Internet	WS provisioning	Provisioning	

[Revenir au sommaire](#)

### Annuaire et authentification

Le service [LDAP/SSO](#) est le socle d'authentification et d'identité standard des applications du ministère.

Zone	Produit	Services	Descriptions
------	---------	----------	--------------



Intranet	<a href="#">LemonLDAP</a>	Authentification des accès aux applications métiers en Intranet	Support de 2 modes d'authentification :  SAML V2 et Reverse Proxy (le mode SAML V2 est à privilégier)  Authentification forte
RIE	<a href="#">LemonLDAP</a>	Délégation d'authentification SAML vers les partenaires raccordés au RIE	Support de 2 modes d'authentification :  SAML V2 et Reverse Proxy (le mode SAML V2 est à privilégier)  Authentification forte
Internet	<a href="#">LemonLDAP</a>	Authentification des accès aux applications métiers en Internet	Support des modes d'authentification :  SAML V2, OIDC et Reverse Proxy (le mode SAML V2 est à privilégier)  Authentification forte  Authentification multifactorielle
Intranet	Active Directory	Service d'annuaire Active Directory/authentification Kerberos	Authentification des utilisateurs/postes de travail

[Revenir au sommaire](#)

## Coffre-fort électronique

SCORPION propose :

- Coffre fort électronique,
- Horodatage

Le service SCORPION est le Coffre-Fort Numérique (CFN) du Ministère, conforme à la norme NF Z42-020 offrant les niveaux de sécurité nécessaires à la conservation d'objets numériques dans des conditions de nature à en garantir leur valeur probante.

Zone	Produit	Services	Descriptions
Intranet	<a href="#">CS Trusty</a>	interface web	Application permettant aux utilisateurs autorisés d'accéder au coffre pour en extraire les objets numériques dont ils sont propriétaires.
		api archiver	Permettent de déposer les objets numériques dans le coffre
		api horodatage	
NA	File Archiver (CS Trusty)	Agent applicatif pour la collecte.	Module additionnel de SCORPION prenant en charge la collecte des objets numériques et les déposer dans le coffre via les API.  A déployer sur serveur et configurer selon le besoin. Voir aussi <a href="#">mtt-filearchiver</a> des <a href="#">composants transverses</a>

[Revenir au sommaire](#)

## Signature électronique

SIGNA est le service de signature, de vérification de la signature électronique et de cachet électronique.

Zone	Produits	Services	Descriptions
Intranet & RIE	SIGNA développement interne	Interface web signature pour les utilisateurs	Gestion des documents à signer
	DSS UE	API signature et cachet	Signature électronique / Qualifiée  Cachet
	<<middleware>>		

[Revenir au sommaire](#)

## GED et stockage de documents



## GED

Le service "GED Générique" du Ministère propose la possibilité d'instancier un espace GED au besoin. Ce service s'appuie sur le produit Alfresco.

Zone	Produits	Services	Descriptions
Intranet	Alfresco	Service de Gestion Electronique de Documents	Application permettant de stocker, sauvegarder la documentation de référence

## COLLABORATIF

Le service "GED Générique" du Ministère propose la possibilité d'instancier un espace GED au besoin. Ce service s'appuie sur le produit Sharepoint.

Zone	Produits	Services	Descriptions
Intranet	SharePoint	Service de collaboration documentaire	Application permettant le partage, l'édition et la coédition, documentaire pour les agents du ministère de la Justice

## Stockage de document

Le service HCP du Ministère est la solution de stockage objet du Ministère, permettant de gérer de très grandes volumétries tout en garantissant un niveau d'intégrité très élevé.

Application permettant aux utilisateurs autorisés d'accéder au coffre pour en extraire les objets numériques dont ils sont propriétaires

Zone	Produits	Services	Descriptions
Intranet & RIE	HCP	Application web de gestion des documents	Application permettant aux utilisateurs autorisés d'accéder au service effectuer manuellement les opérations sur les documents dont ils sont propriétaires : consultation, dépôt, suppression, ...
	Hitachi Content Platform	API Rest de gestion des documents	

Voir aussi [mtt-proxy-storage](#) des [composants transverses](#)

[Revenir au sommaire](#)

## Observabilité

### ITO

Zone	Produits	Services	Descriptions
Toute zone DC	ECE Agent	Agent de collecte (beats elastic).	Collecte des logs, des métriques pour les OS serveurs supportés (windows ou Linux).
	APM Agent	APM	jar d'introspection pour récupération des métriques et traces applicatives, pour les langages supportés.
	RUM	Real User Monitoring	Collecte les données d'expérience utilisateur, optimisées par l'agent APM Real User Monitoring (RUM), permettent de quantifier et d'analyser les performances perçues d'une application Web.
	ECE Server	Indexation, IHM Dashboard et rapports	Indexation et de correlation des métrics et logs. outils de dashboard, publication de rapport et analyse.

[Revenir au sommaire](#)

## SMTP

Zone	Produits	Services	Descriptions
------	----------	----------	--------------



Toute zone DC	SMTP	Envoi de mail	Service d'envoi de mail des applications en DC, envoi de mail en interne ou vers l'extérieur.
---------------	------	---------------	-----------------------------------------------------------------------------------------------

[Revenir au sommaire](#)

## Plateforme d'échange

Le service PFE du Ministère propose des services d'échanges de fichiers sécurisés inter-applicatif

Zone	Produits	Services	Descriptions
Interne DC	Axway	Transfert de fichier HTTP, sftp, FTPS	Plateforme d'échange pour le transfert de fichier internet et externe.
		Transfert de fichier HTTP, sftp, FTPS	
Externe RIE		Transfert de fichier HTTP, sftp, FTPS	
Internet		Transfert de fichier HTTP, sftp, FTPS	

[Revenir au sommaire](#)

## Messageries

Zone	Produits	Services	Descriptions
Toutes zones	Exchange	Service d'envoi et de réception de courrier électronique	Service basé sur la technologie Microsoft Exchange

[Revenir au sommaire](#)

## Editique

Zone	Produits	Services	Descriptions
Intranet	OpenText Exstream CN	Interface web de conception déléguée de trame pour les utilisateurs	Application Web (Content Author) permettant aux utilisateurs métier de créer et/ou modifier des trames de document à base d'une trame maîtresse conçue dans l'environnement de développement Expert (client lourd de Design).
	+ API Gateway (façade aux API Produit)	API Rest de composition unitaire de document transactionnel /Interactif	Permet la composition d'un document à base d'une trame déployée et d'un flux d'entrée XML sous plusieurs formats (docx, PDF/A3). Cette composition peut concerner aussi un document interactif au statut "Brouillon" (on parle ici de service Fulfillment)
		API Rest de composition par lot de documents	Permet la composition d'un lot de document à base d'une trame déployée et d'un flux d'entrée XML sous plusieurs formats (docx, PDF/A3, AFP, PCL, ...)
		API Rest de composition de document en édition interactive	Permet la composition d'un document interactif au statut "Brouillon" à base d'une trame déployée et d'un flux d'entrée XML en vue de son enrichissement dans l'interface Web d'Empower (ajout /modification de textes, page d'interview, intégration de paragraphes depuis une bibliothèque de paragraphes prédéfinie, ...)

[Revenir au sommaire](#)

## Proxy

Le service proxy permet aux applications hébergées en DC de sortir vers internet en http(s).

Zone	Produits	Services	Descriptions
Interne vers Internet	Squid	Appel http(s) vers internet	<a href="https://wiki.codeo.intranet.justice.gouv.fr/x/ZdUVC">https://wiki.codeo.intranet.justice.gouv.fr/x/ZdUVC</a>

[Revenir au sommaire](#)

## Archivage



[A2S - AXONE - Espace ISS - CODEO - WIKI \(justice.gouv.fr\)](#)

- Système d'archivage intermédiaire et long terme, hybride et électronique en lien avec le programme PSAE
- Disposer d'un système d'archivage électronique hybride (papier et numérique) permettant de gérer les archives produits par l'administration centrale.
- Proposer une offre de services aux juridictions souhaitant gérer les archives physiques.

Zone	Produits	Services	Descriptions
Intranet & RIE	Axone (XAM /VITAM)	Interface web de gestion d'archives physiques et électroniques	Application Web de gestion de sites et de salles d'archives physique (logistique), de gestion de plan de classement, processus d'accès (recherche et consultation), de versement manuel (bordereaux physique et dossier numérique = <a href="#">SIP</a> ), d'élimination, de préservation, de supervision (registre des fonds, audit de valeur probante, ...), ...  Solution multi-tenant (coffres) avec offre de stockage objet (Swift sur <a href="#">VaS</a> )
Intranet	XDH	Interface web de gestion et de supervision de canaux de versements automatiques	IHM de définition de canaux de versement de dossiers numériques produits par les applicatifs métier du MJ et de l'Administration Centrale (PPN, Parcours, Portalis, HARMONIE, DADP, ...)
		API Rest de versement automatique	API de collecte d'archives numériques en mode unitaire ou par lot. Le dossier versé est dans un format pivot simplifié qui sera transformé en SIP (format standard <a href="#">SEDA</a> )
		Service d'accusé de réception de versement (ATR)	Accusée de réception fonctionnel (ATR=Acknowledgement Transfert Response) rendu pour chaque applicatif client à l'issue d'un versement du paquet (lot SIP) dans Axone

[Revenir au sommaire](#)

## PKI

### PEKIN

Propose (ou IGC : Infrastructures de gestion des clés) une infrastructure destinée à gérer le cycle de vie des certificats du Ministère de la Justice.

<<à compléter modifier par Eric Campbell>>

Zone	Produits	Service	Descriptions
Interne	ejbca	IHM web pour la la gestion des certificats serveur ou client	La génération de certificat et des AC.
		Certificats serveur / client SSL (TLS)	Le renouvellement de certificat et des AC.
		De chiffrement (IPSec, BitLocker, MS Doc Encryption)	La révocation de certificat et des AC.
		Signature de code, signature responsable de certificats.	La publication des autorités de certifications (AC).
		Horodatage, Cachet	La publication des listes de révocation.
		Clip	
		Accès Administrateur	

### Icare

Propose une infrastructure destinée à gérer le cycle de vie des certificats du Ministère de la justice dans l'environnement Microsoft.

Zone	Produit	Services	Descriptions
Interne	rôle ADCS de Windows	Certificats poste de travail Windows	

[Revenir au sommaire](#)

## Service Interministériel



Service délivré par la DINUM ou proposer en interministériel par des entités de l'état.

Zone	Produits	Services	Descriptions
Internet& RIE	PISTE	API Management	Service d'API Management proposé par l'AIFE, permet d'exposer des services dans le RIE ou sur Internet.  Catalogue, plateforme de staging, et possibilité d'interconnexion diverses.
RIE	PI / PI Gen 2	Offre Cloud IAAS - Cloud au centre	Cloud de l'état, offre IAAS SecNumCloud, service IAAS, niveau de service élevé.
		Offre Cloud Native - Cloud au centre	Cloud de l'état, offre OpenShift - en cours de déploiement.
RIE	Nubo	Offre Cloud IAAS - Cloud au centre	Cloud de l'état, offre IAAS SecNumCloud, service IAAS, portail riche.
Internet	Resana	Digital Workplace	Plateforme collaboratif.
	Resana secure	Service d'échange de fichier	Outil d'échange de fichier sécurisé.

## Plateformes d'échange

Zone	Produits	Services	Descriptions
Internet /Intranet/RIE	PLEX	<u>PL</u> ate-forme d'échange <u>EX</u> tern <u>E</u>	Echanges de fichiers volumineux avec messagerie sécurisés, accessible sur internet/RIE  Réservé aux partenaires habilités.
Interne	PLINE	<u>PL</u> ate-forme d'échange <u>IN</u> tern <u>E</u>	Echanges de fichiers volumineux avec messagerie sécurisés.  Disponible uniquement en intranet
Internet /Intranet/RIE	KISS	Plateforme d'échange de fichiers (cf. <a href="#">01 - REFERENTIEL PRODUITS</a> )	Echanges de fichiers en protocole SFTP.  Disponible pour des échanges inter-applicatif intranet  Disponible pour des échanges inter-applicatif internet/RIE avec des partenaires habilités

## Bastions d'administration

Services d'administration de serveurs en DC et DIT.

Zone	Produits	Services	Descriptions
Interne	Citrix	Accès Administrateur	<a href="https://nantes.aadmin.intranet.justice.gouv.fr/logon/LogonPoint/index.html">https://nantes.aadmin.intranet.justice.gouv.fr/logon/LogonPoint/index.html</a> <a href="https://osny.aadmin.intranet.justice.gouv.fr/logon/LogonPoint/index.html">https://osny.aadmin.intranet.justice.gouv.fr/logon/LogonPoint/index.html</a>  Accès aux environnements de production et préproduction en DC1 et DC3.  Géré par Didier Pinson.
Interne	Wallix	Accès Administrateur	<a href="https://bar.intranet.justice.gouv.fr/wabam/portailXXX">https://bar.intranet.justice.gouv.fr/wabam/portailXXX</a> <a href="https://dc1.bar.intranet.justice.gouv.fr/wabam/portailXXX">https://dc1.bar.intranet.justice.gouv.fr/wabam/portailXXX</a> <a href="https://dc3.bar.intranet.justice.gouv.fr/wabam/portailXXX">https://dc3.bar.intranet.justice.gouv.fr/wabam/portailXXX</a>  Accès aux environnements de production en DIT.  Accès aux environnements de développement et recette en DC1/DC3/DC5.  Géré par ISS/ETI/SES.
Interne	Windows RDSH	Accès Administrateur	Pour les administrateurs en DIT.  Ferme AARDS <a href="https://rds0.dc1.aards.intranet.justice.gouv.fr/RDWeb/Pages/fr-FR/login.aspx">https://rds0.dc1.aards.intranet.justice.gouv.fr/RDWeb/Pages/fr-FR/login.aspx</a> accédée une fois connecté à l'Accès Administrateur Citrix.  Géré par TOP/BUC.

[Revenir au sommaire](#)

## Antivirus



Services d'analyse antivirus.

Zone	Produits	Services	Descriptions
Interne /Internet	ESET	Antivirus serveur	
Internet/RPVJ	Trend Micro IWSVA	SAFII (Service Antivirus des Flux Internet et Intranet)	Géré par ISS/ETI/SES.  Service obsolète, licence expirée. Etude renouvellement en cours.
Internet	Trend Micro	Antivirus messagerie	Géré par TOP/BUC
Interne	Trend Micro	Antivirus poste de travail	Géré par TOP/BUC

[Revenir au sommaire](#)



## 04 - REFERENTIEL DES PATTERNS D'ARCHITECTURE

[01 - Patterns d'architecture technique](#)

[02- Patterns d'architecture logicielle](#)



## 01 - Patterns d'architecture technique

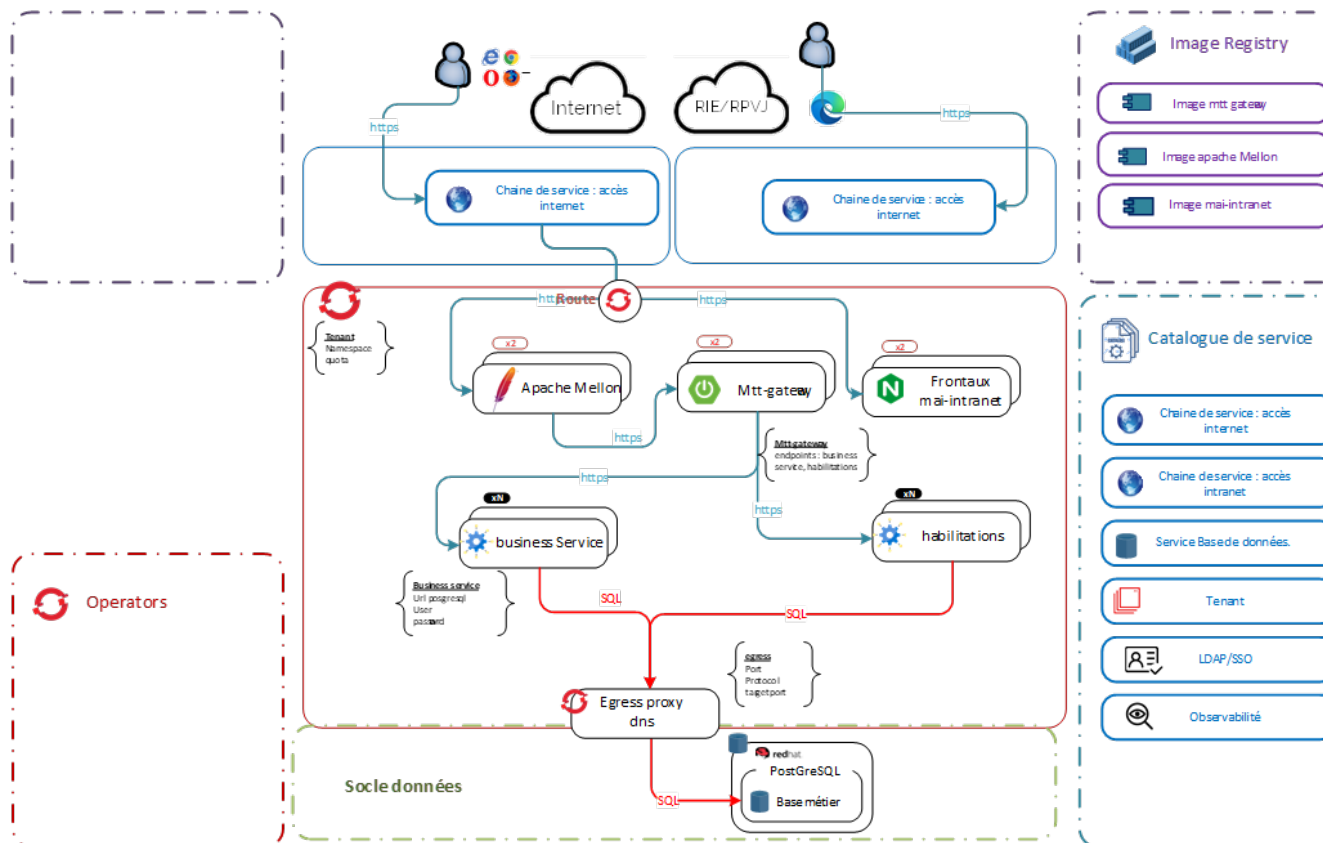
### Application micro-services standard

Cas d'usage : Développement spécifique des applications métiers du Ministère de la Justice

- Avec authentification SSO SAML V2
- Avec un stockage de données en BDD relationnelle
- Architecture Frontend / Backed séparée

Le pattern « Application micro service standard » s'appuie sur les building blocks suivants :

- Tenant
- Liaison & exposition
- Authentification
- Base de données – Relationnelle – PostgreSQL
- Log
- Supervision



### Publication de contenu

Cas d'usages : site de publication.

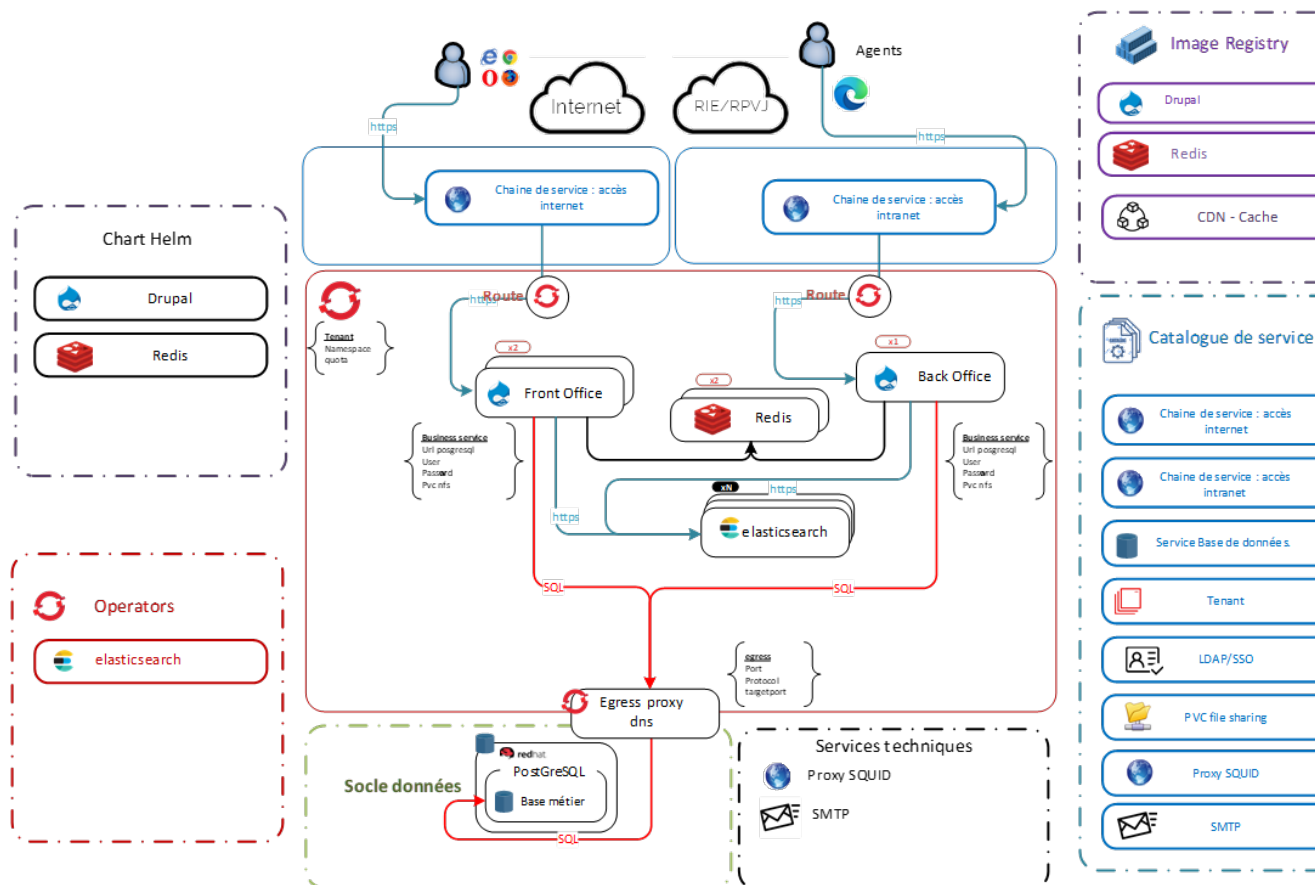
- Contribution de contenus.
- Publication de contenus.

Le pattern « Gestion de contenu » s'appuie sur les building blocks suivants :

- Tenant
- Liaison & exposition
- Authentification pour la partie contribution
- CMS - Drupal
- Base de données – Relationnelle – PostgreSQL
- Moteur de recherche – Elasticsearch
- Cache – CDN



- Cache – Redis
- Stockage - NFS

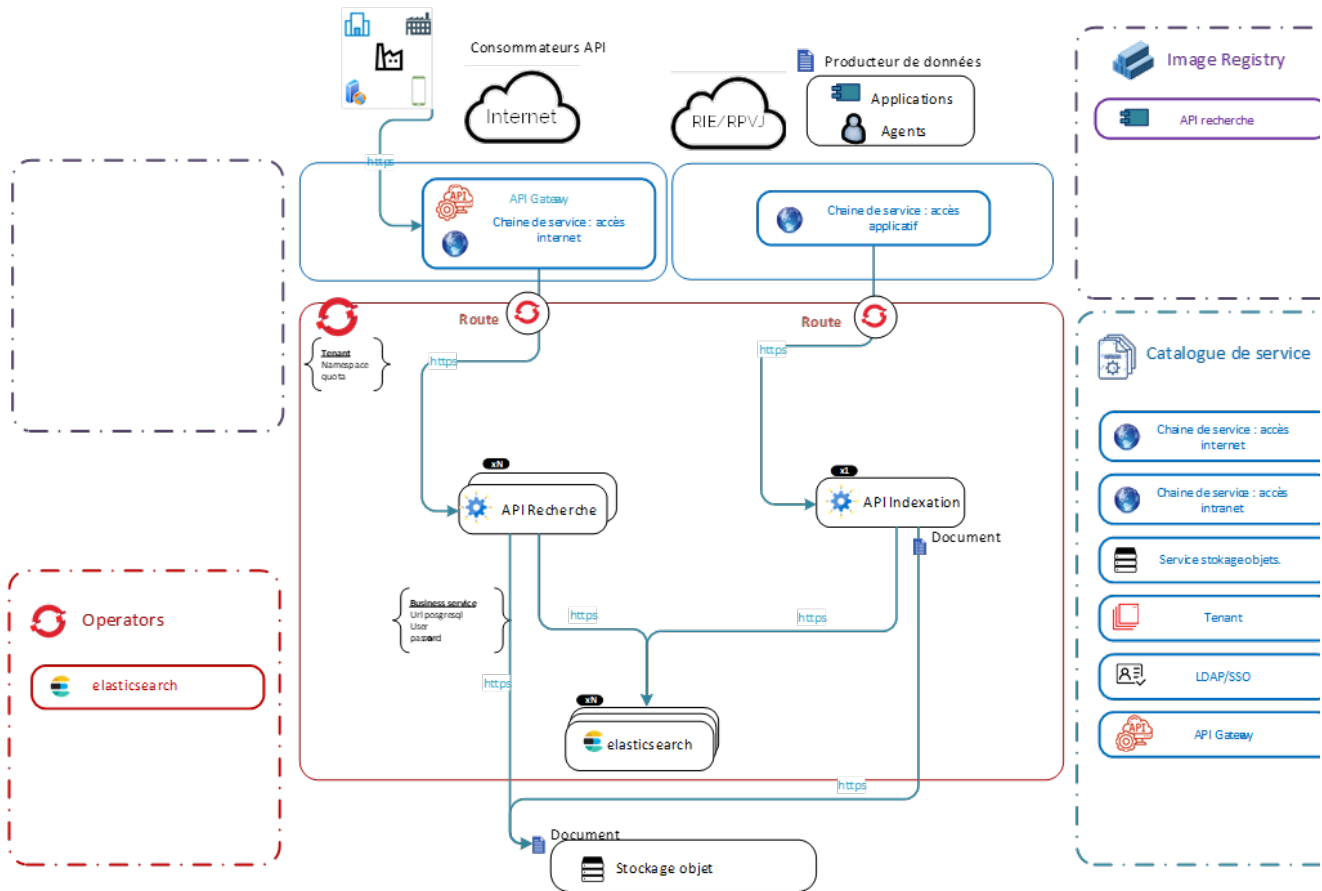


## Exposition de données indexation et recherche

Le pattern « Opendata » s'appuie sur les building blocks suivants :

- Tenant
- Liaison & exposition
- Moteur de recherche – ElasticSerach
- APIM
- Log
- Supervision
- Stockage Bloc et S3





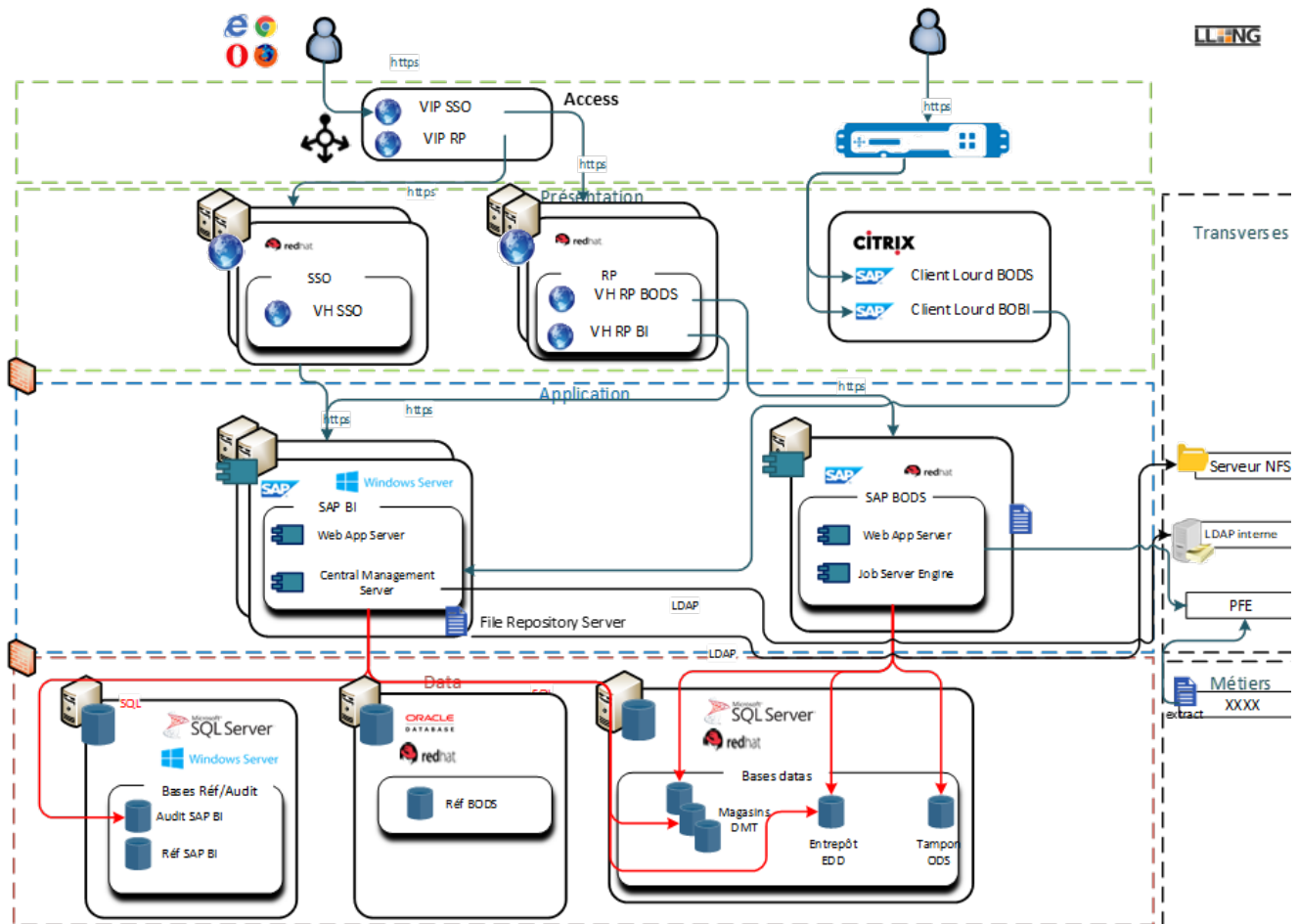
## Authentification

## Internet / Intranet

## Architecture décisionnelle

Architecture sur socle VM, les données sont traités en amont les copie de base sont interdites







## 02- Patterns d'architecture logicielle

### Sommaire

- [Architecture Microservices standard](#)
- [Export de données](#)
- [Authentification](#)
- [Chiffrement de données](#)
- [Recherche avec Elasticsearch](#)
- [Internet / Intranet](#)
- [Echanges de données](#)
- [Production des indicateurs statistiques](#)

### Architecture Microservices standard

L'architecture microservices d'une application standard en développement spécifique est composée des éléments suivants

Composant	Implémentation	Mise en oeuvre O = obligatoire F = facultatif
IHM	MAI-XX	F
Authentification	<ul style="list-style-type: none"><li>• Apache Mellon pour <a href="#">SAML V2</a></li><li>• ou autre MTT implémentant le protocole (<a href="#">OAuth2</a>, <a href="#">OpenID Connect</a>, ...)</li></ul>	O
Routage	<a href="#">MTT-GATEWAY</a>	O
Gestion des droits applicatifs	MAS-HABILITATION	F
Microservices	MAS-XX	O
Stockage de Données structurées	Base de données	F
Stockage de documents	<a href="#">MTT-PROXY-STORAGE</a>	F
Stockage dans SCORPION	<a href="#">MTT-FILEARCHIVER</a>	F

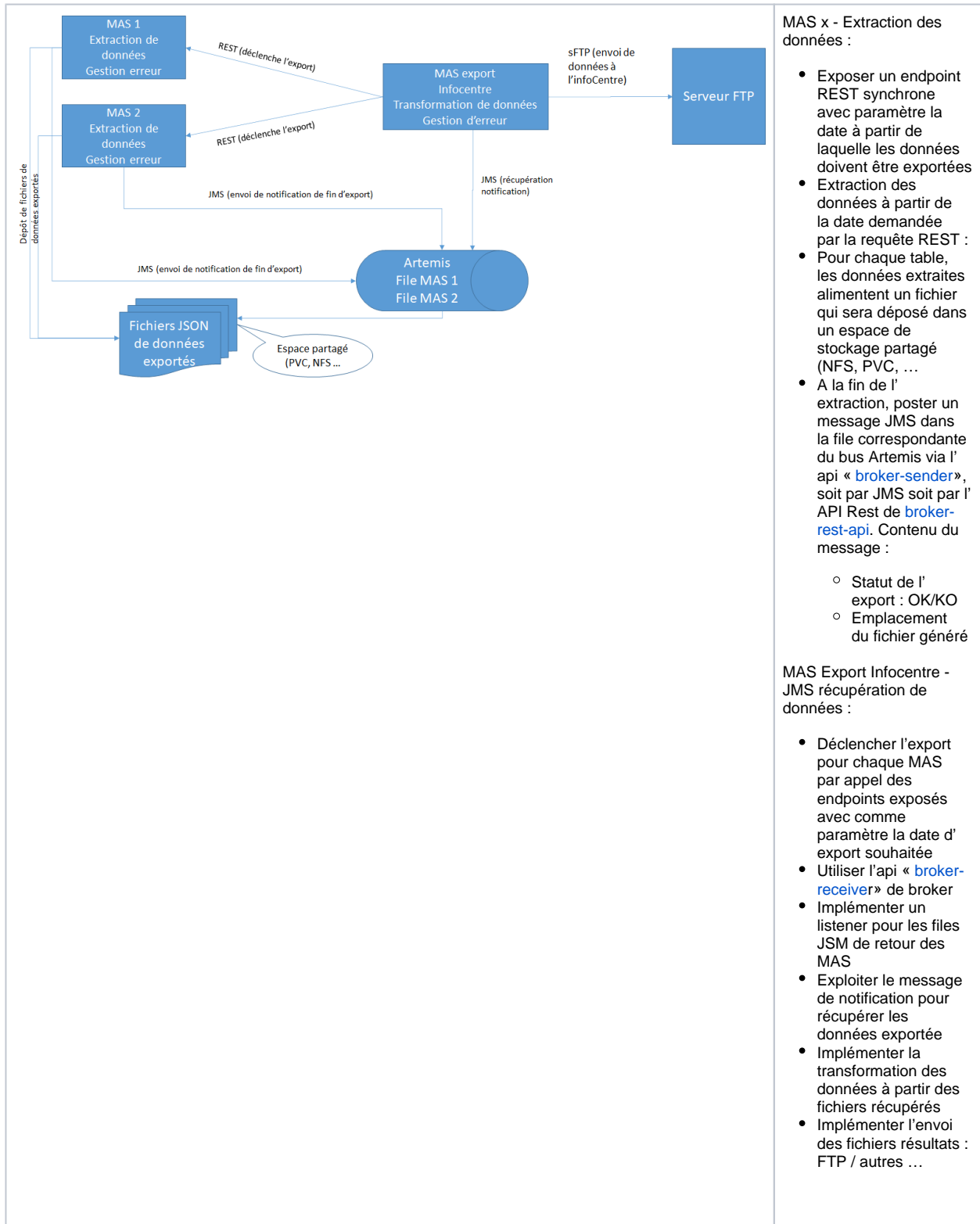
[Retour au sommaire](#)

### Export de données

Ce pattern est applicable pour les exports de données. Exemple de cas d'usage : exports pour les InfoCentre.

Schéma de principe	Détail
--------------------	--------





[Retour au sommaire](#)

## Authentification

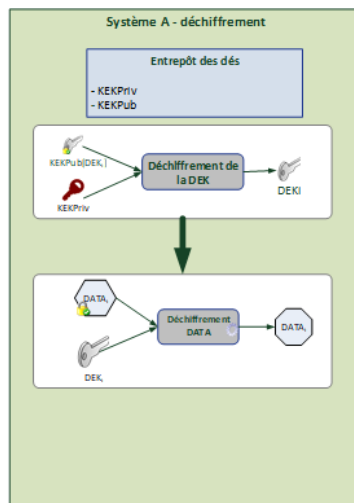
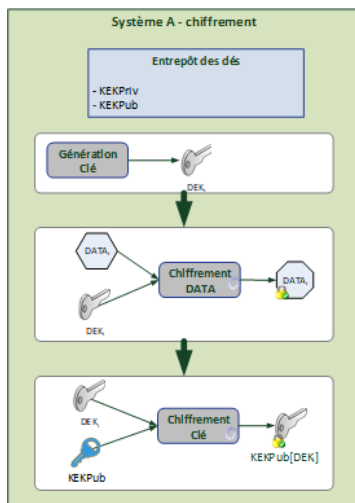


SAML V2	Lemon-LDAP V1 Lemon-LDAP V2	Pattern privilégié pour les authentifications des utilisateurs, via navigateur.  Le socle joue le rôle de l'IDP vis à vis des applications MJ qui jouent le rôle de SP.
OAuth 2	Lemon-LDAP V2	Pattern privilégié pour les authentifications inter-applicatif
Reverse Proxy - Headers	Lemon-LDAP V1 Lemon-LDAP V2	
Délégation d'authentification - SAML V2	Lemon-LDAP V1 Lemon-LDAP V2	Pattern pour l'authentification des utilisateurs partenaires externes : le socle joue le rôle de SP vis à vis du SSO partenaire et IDP vis à vis des applications MJ

[Retour au sommaire](#)

## Chiffrement de données

Chiffrement/déchiffrement au sein d'un même système (pas de partenaire).



La solution de chiffrement retenue est basée sur une architecture à deux niveaux de clés :

- Utilisation d'une KEK (Key Encryption Key) : clé de chiffrement de clés (chiffre la clé de chiffrement uniquement)
- Utilisation d'une DEK (Data Encryption Key) : clé utilisée pour le chiffrement des données (et des fichiers)

Cette architecture à deux niveaux de clés facilite la rotation des clés (la rotation est souvent réalisée uniquement sur la KEK). La rotation de la DEK est à envisager dans le cas où la durée de vie de la donnée est supérieure à la durée de vie de la clé (ou en cas de compromission).

La responsabilité du chiffrement /déchiffrement est déléguée aux composants manipulant la donnée. L'idéal serait de déléguer cette responsabilité de chiffrement à un KMS centralisé. Ne possédant pas encore cette brique (étude en cours) il est nécessaire de trouver une alternative dégradée simple à mettre en œuvre mais permettant de répondre à minima aux contraintes de sécurité. Afin de respecter le RGSv2, il est nécessaire de suivre les tailles de clé et les algorithmes de chiffrement suivants : KEK : paire de clé RSA (clé publique / clé privée) – 2048bits – chiffrement asymétrique

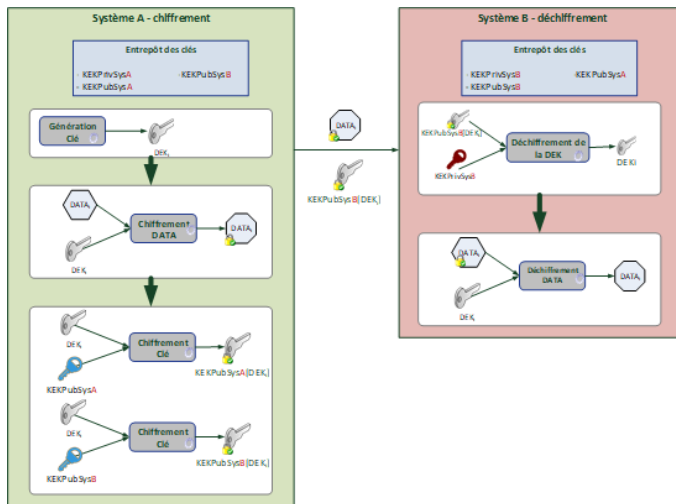
- Chiffrement avec la clé publique
- Déchiffrement avec la clé privée
- Algorithme : RSAES-OAEP

DEK : clé AES 256 bits – chiffrement symétrique

- Chiffrement/déchiffrement avec la même clé.
- Algorithme : AES/GCM



Chiffrement/déchiffrement réalisé par plusieurs systèmes (multi partenaires).



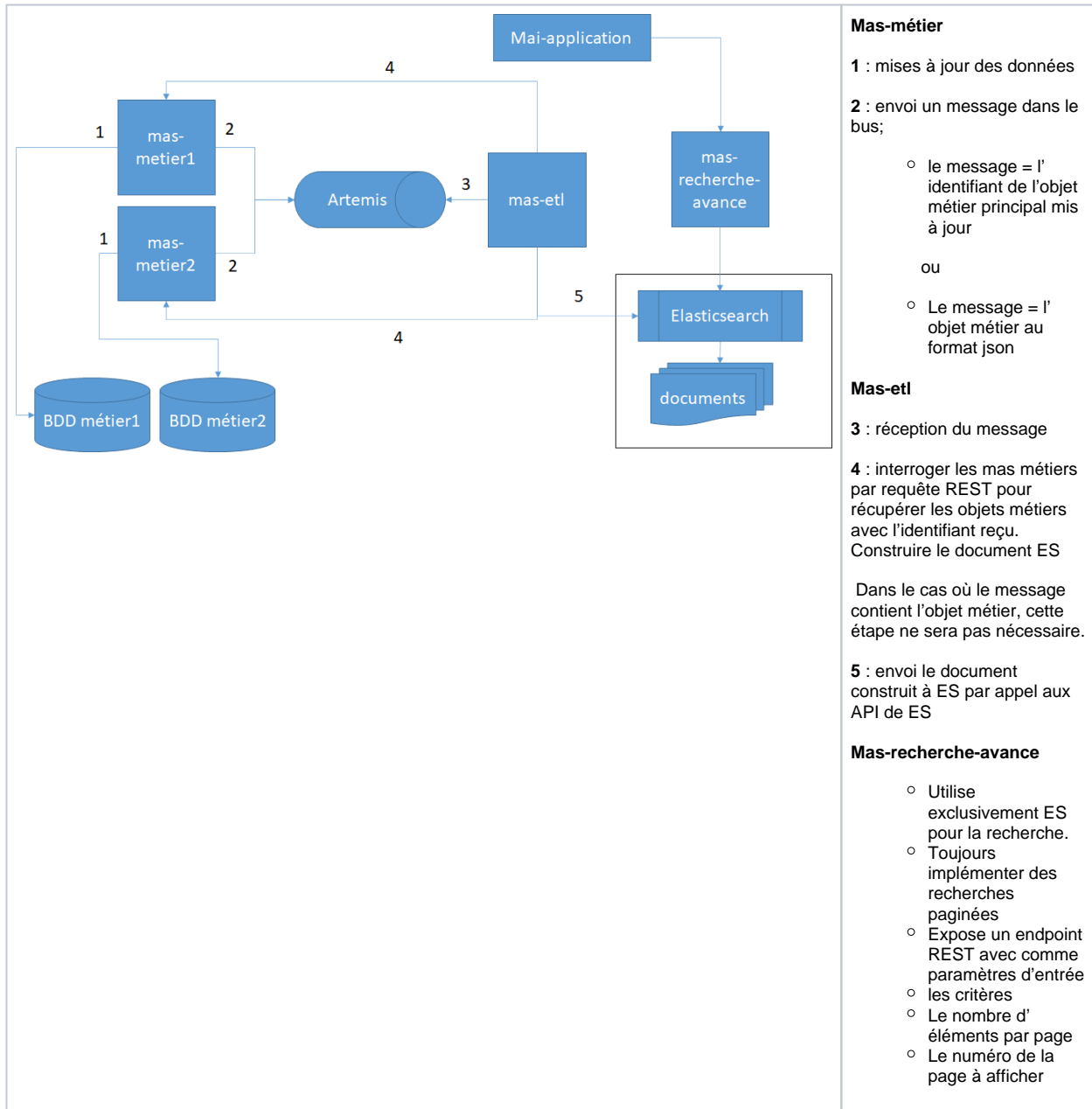
[Retour au sommaire](#)

## Recherche avec Elasticsearch

Schéma de principe

Détail





[Retour au sommaire](#)

Internet / Intranet

[Retour au sommaire](#)

Echanges de données

Pattern	Implémentation	Cas d'usages
---------	----------------	--------------



Asynchrone - <b>Pattern privilegié</b>	<p>Ces échanges passent par l'utilisation d'un bus de message Artémis (cf. <a href="#">01 - Référentiel Produits - ISS / TOP / SMART</a>)</p> <p>Protocole privilégié : JMS</p> <p>Modalités : queue ou publish/subscribe</p> <p>Architecture de déploiement (cf. <a href="#">01 - Patterns d'architecture technique</a>)</p>	<ul style="list-style-type: none"> <li>• Echange inter-domaines métier</li> <li>• Echange inter-produits</li> <li>• Echange intra applicatif</li> </ul>
Synchrone	<p>Ces échanges passent par les appels API REST</p> <p>Architecture de déploiement (cf. <a href="#">01 - Patterns d'architecture technique</a>)</p>	<ul style="list-style-type: none"> <li>• Echange inter-produits</li> <li>• Echange intra applicatif</li> <li>• Echange inter-domaines métier via l'API Manager (cf. Produit- API Manager <a href="#">01 - REFERENTIEL PRODUITS</a>)</li> <li>• Echange avec des partenaires externes</li> </ul>
Hybride	<p>Combinaison du pattern asynchrone et synchrone :</p> <ol style="list-style-type: none"> <li>1. asynchrone : notification de l'arrivée d'un événement. Le message contient le juste nécessaire des données.</li> <li>2. synchrone : appel API pour obtenir des données plus complète</li> </ol>	<ul style="list-style-type: none"> <li>• Echange inter-domaines métier</li> <li>• Echange inter-produits</li> </ul>
Pseudo synchrone	<p>Ces échanges passent par l'utilisation d'un bus de message Artémis (cf. <a href="#">01 - Référentiel Produits - ISS / TOP / SMART</a>) avec l'implémentation du mode "request-reply"</p> <p>Architecture de déploiement (cf. <a href="#">01 - Patterns d'architecture technique</a>)</p>	
Transfert de fichier	<p>Utilisation de la solution SecureTransport (cf. Produit- Transfert de fichier dans <a href="#">01 - REFERENTIEL PRODUITS</a>)</p>	<ul style="list-style-type: none"> <li>• Echanges de fichiers avec les partenaires externes</li> <li>• Echanges de fichiers inter-domaine métier</li> </ul>

[Retour au sommaire](#)

## Production des indicateurs statistiques

Type d'indicateurs	Implémentation	Cas d'usage	Type de restitution	Caractéristiques des données
Pilotage opérationnel	Au niveau projet /produit	<ul style="list-style-type: none"> <li>• Suivi opérationnel</li> <li>• Recherche d'informations détaillées y compris personnelles et /ou sensibles</li> <li>• Recherche avancée sur une population étudiée</li> <li>• Pas de croisement de données</li> </ul>	<ul style="list-style-type: none"> <li>• Listes détaillées de données, tableaux de bord filtrées selon différents critères</li> <li>• Eléments de comptage de niveau local ventilés sur différents critères</li> <li>• Données détaillées sur des éléments ciblés</li> </ul>	<p>Fraîcheur : temps réel</p> <p>Périmètre : base de données opérationnelle avec filtrage des données selon les habilitations le cas échéant</p>
Décisionnel - Info Centre	<ul style="list-style-type: none"> <li>• Pilotage de l'activité</li> <li>• Aide au choix des orientations stratégiques</li> <li>• Croisement de données possibles</li> </ul>	<ul style="list-style-type: none"> <li>• Pilotage de l'activité</li> <li>• Aide au choix des orientations stratégiques</li> <li>• Croisement de données possibles</li> </ul>	<ul style="list-style-type: none"> <li>• Reporting</li> <li>• Tableaux de bord</li> <li>• Indicateurs basés sur des données pseudonymisées et agrégées</li> </ul>	<p>Fraîcheur :</p> <ul style="list-style-type: none"> <li>• J-1</li> <li>• Hebdomadaire</li> <li>• Mensuel</li> </ul> <p>Périmètre : données exportées depuis bases opérationnelle, anonymisées /pseudonymisées, historisées</p>



<p>Pilotage de la politique publique</p> <p>Etudes statistiques / Statistiques publiques</p>	<ul style="list-style-type: none"> <li>• Statistique publique</li> <li>• Etude de phénomènes sur une population ou échantillon</li> <li>• Fouille et croisement de données</li> <li>• Croisement de données possibles</li> </ul>	<ul style="list-style-type: none"> <li>• Statistique publique</li> <li>• Etude de phénomènes sur une population ou échantillon</li> <li>• Fouille et croisement de données</li> </ul>	<ul style="list-style-type: none"> <li>• Tableaux / graphiques</li> <li>• Indicateurs basés sur des données agrégées</li> </ul>	<p>Fraîcheur :</p> <ul style="list-style-type: none"> <li>• Mensuel</li> <li>• Trimestriel</li> <li>• Annuel</li> </ul> <p>Périmètre : données exportées, éventuellement non anonymisées, historisées</p>
----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[Retour au sommaire](#)



## 99 - Annexes

[Microservices](#)



## Composants transverses MJ

Le Ministère dispose d'une liste de composants techniques transverses permettant de faciliter la réalisation de certaines règles / exigences de mise en oeuvre.

### Sommaire

1. [Conditions générales d'utilisation](#)
  1. [Mise à disposition](#)
  2. [Responsabilités](#)
2. [Liste des composants transverses](#)
  1. [mtt-gateway](#)
  2. [mtt-security](#)
  3. [mtt-filearchiver](#)
  4. [mtt-proxy-storage](#)
  5. [broker-api](#)
  6. [broker-rest-api](#)
  7. [mtt-doc-converter](#)
  8. [mtt-zed-api](#)
  9. [mtt-crypto](#)
  10. [mtt-logger](#)
  11. [mtt-export-data](#)

### Conditions générales d'utilisation

#### Mise à disposition

Les composants transverses sont mis à dispositions aux partenaires du Ministère sous 2 formes

Forme	Modalité	Pour qui ?	
		Développements en dehors du MJ	Développements dans les environnements MJ
Code source	Zip	X	
	Gitlab MJ		X
Binaire	Artifactory Nexus MJ		X

#### Responsabilités

**2.1** Les composants transverses du Ministère sont proposés aux partenaires à titre d'accélérateur de mise en œuvre.

**2.2** Les partenaires sont libres de les adopter ou non. Dans le second cas, le partenaire doit réaliser l'équivalent de ces composants en respectant les règles / exigences de mise en œuvre; les réalisations peuvent prendre comme point de départ le code source fourni par le Ministère.

**2.3** L'utilisation de la "forme code source" des composants transverses (intégration du code source du composant dans le code source des applications), est considéré comme un "fork", qu'il y ait ou non des modifications opérées. Par conséquent, le code source "forké" fait partie des livrables du partenaire au même titre que le reste.

**2.4** MCO : le Ministère n'assure pas la MCO des composants transverses

- Les corrections d'anomalies (bug ou CVE) constatées : deux cas de figure
  - Utilisation de la forme code source "forké" (cf 2.2) : le partenaire est responsable des correctifs. Le MJ est libre de reporter les correctifs dans son code source en temps utile.
  - Utilisation de la forme binaire : le partenaire ou le MJ proposent des corrections dans Gitlab sous la forme des MR (merge requests). Le MJ valide les proposition et publie les releases dans Nexus
- Montée de versions des socles logiciels : idem précédemment.
- Evolution fonctionnelle : idem précédemment

[Retour au sommaire](#)

### Liste des composants transverses

Composant	Description	URL (accessible uniquement dans le réseau MJ)	Type	Modalité d'utilisation
-----------	-------------	-----------------------------------------------	------	------------------------



<b>mtt-gateway</b>	<p>Cette brique est un reverse proxy qui permet de concentrer les appels aux services backend. Elle assure :</p> <ul style="list-style-type: none"> <li>le routage</li> <li>la récupération des autorisations (micro-droits)</li> <li>la propagation de l'identité sous forme de JWT au service backend</li> <li>la sécurité CSRF/CORS frameOptions</li> <li>la conversion de l'encoding des informations transmises en header</li> </ul>		Exécuta- ble	A instancier et configurer
<b>mtt-security</b>	<p>Librairie permettant de gérer la propagation de l'identité au sein des différents micro-services.</p> <p>Implémenter la forge et la vérification des jetons JWT.</p>		Librairie	Dépendance logicielle
<b>mtt-filearchiver</b>	<p>Composant permettant de collecter des fichiers générés par les applications et de les envoyer dans le coffre-fort SCORPION</p>		Exécuta- ble	A instancier et configurer
<b>mtt-proxy-storage</b>	<p>Composant implémentant les différentes solution de stockage supportés au MJ : HCP, S3</p> <p>Ce composant expose les API normalisées qui s'abstraient des technologies de stockage sous-jacentes, utilisables par les applications</p>		Exécuta- ble	A instancier et configurer
<b>broker-api</b>	<p>Librairie implémentant une surcouche permettant de faire abstraction du protocole JMS.</p> <p>Prend en charge le traitement des messages volumineux</p> <p>Implémentation des modes queue (mono consommateur) et topic (multi consommateur)</p> <p>Implémentation des échanges "pseudo synchrone" (request-reply)</p>		Librairie	Dépendance logicielle
<b>broker-rest-api</b>	<p>Composant exposant des endpoints REST prenant en charge la mise en file JMS des messages via le protocole HTTP.</p> <p>Utile pour les clients ne souhaitant pas mettre en oeuvre JMS.</p> <p>Ne prend pas en charge la consommation des messages.</p>		Exécuta- ble	A instancier et configurer
<b>mtt-doc-converter</b>	<p>Librairie implémentant la conversion des documents de différents types (ODT, DOCX, WordPerfect, ...) en PDF.</p> <p>Prend en charge les 3 niveaux de conformités PDF/A pour le PDF résultant.</p> <p>Prend en charge la conversion avec pièces jointes dans le PDF résultant</p>		Librairie	Dépendance logicielle
<b>mtt-zed-api</b>	<p>Librairie permettant de</p> <ul style="list-style-type: none"> <li>créer un conteneur ZED chiffré et y mettre les fichiers</li> <li>extraire les fichiers depuis un conteneur ZED chiffré</li> </ul> <p>Utile pour les applications devant implémenter les cas d'usage de transmission de fichiers (canal mail par exemple) avec exigence de sécurisation par conteneur chiffré.</p>		Librairie	Dépendance logicielle
<b>mtt-crypto</b>	<p>Librairie de chiffrement :</p> <ul style="list-style-type: none"> <li>génération de clés asymétriques AES-256 à la volée</li> <li>chiffrement / déchiffrement des données : <ul style="list-style-type: none"> <li>en mode stream pour les données volumineuses</li> <li>en mémoire pour les données à faibles volumétries</li> </ul> </li> </ul> <p>Utile dans l'implémentation des exigences de chiffrements des données d'applications sensibles</p>		Librairie	Dépendance logicielle
<b>mtt-logger</b>	<p>Librairie permettant de générer les logs conformement aux normes de traces</p>		Librairie	Dépendance logicielle
<b>mtt-export-data</b>	<p>Librairie implémentant le pattern export de données</p>		Librairie	Dépendance logicielle

[Retour au sommaire](#)

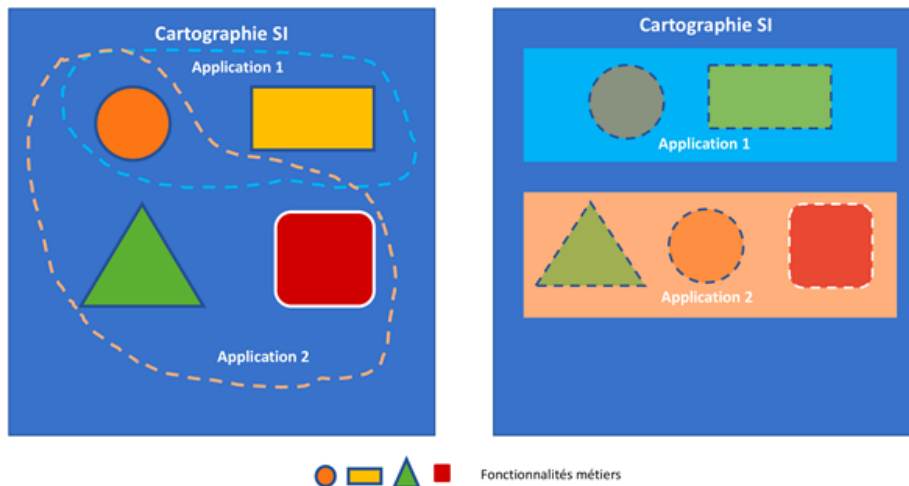


## Microservices

### Les principes directeurs

#### Généralités

Une architecture servant l'architecture fonctionnelle et non une application.



- La figure ci-dessus illustre la différence fondamentale de vision du SI dans les 2 démarches :
  - A gauche, les applications n'ont qu'une importance toute relative dans la cartographie du SI ; à contrario, les microservices (représentant des fonctionnalités métiers) y sont des éléments constitutifs.
  - A droite, les applications sont au cœur de la cartographie ; les fonctionnalités métiers couvertes y sont masquées. Il faudrait procéder à une analyse fonctionnelle des 2 applications pour identifier la redondance du service métier

### Conception

Un microservice représente **une fonctionnalité métier unitaire**, par exemple « Rédaction de procédure », « Délégation de signature », ....

La complexité d'un microservice dépend de l'acte métier couvert. La granularité du découpage ne doit être

- Trop fine, le microservice perd sa caractéristique de représentation d'une fonctionnalité métier.
- Trop grosse, le microservice perd son caractère unitaire de la fonctionnalité métier.

Une architecture qui permet le **pilottage par les données** (« **datacentric** »)

### Règle d'implémentation

Un microservice est

- Sans état (stateless)
- Limité à **une fonctionnalité métier**
- Techniquement indépendant des autres microservices (i.e. est déployable dès lors que tous ses composants internes sont opérationnels)
- A ses propres piles techniques : langage, librairies, serveur d'application, BDD, ...
- Est une « unité de déploiement » à part entière
- La dépendance entre microservices doit être limitée ; une attention particulière doit être apportée à la dépendance cyclique entre microservice
- Les dépendances entre microservices sont réalisées à travers des appels API
- La dépendance est limitée strictement au niveau fonctionnel i.e. l'arrêt des services dont le microservice dépend :
  - Ne doit pas empêcher son déploiement
  - Ne doit pas provoquer des dysfonctionnements non maîtrisés
  - Ne doit pas empêcher un fonctionnement minimal en mode dégradé (résilient)
- La gestion des dépendances inter-microservices passe par les contrats d'interface