Cadre de Cohérence Technique

Circuit de validation

Date application	Version	Objet	Rédaction	Vérification	Approbation
24/07/2019	8.1.14	CCT 2019 (Voir historique des modifications pour le détail)	Le 24/07/2019 B. BOUCHAREB M WISSLER R. MORGAND C. LAMBERT	Le 24/07/2019 Boubaker BOUCHAREB	Le 24/07/2019 JB LAPEYRIE, Yves BRONOEL MC LESPINASSE, M. VELLUCI P. NOBLECOURT

Diffusion Élargie ☒ Restreinte ☐ Contrôlée ☐ exemplaire n°

Pour action	
Pour information	

HISTORIQUE DES MODIFICATIONS

Date application	Version	Objet	Rédaction	Vérification	Approbation
08/10/08	8.0VP0	Création du document, reprise CCT 7.1.3 de novembre 2006 élaboré par le COMIRCE	Olivier PASQUIN, CAPGEMINI	David MARCHAL, Reynald POIDEVIN	
04/11/08	8.0VP1	Version intégrant les travaux du schéma directeur 2009-2013	Olivier PASQUIN, CAPGEMINI		
28/11/08	8.0VP2	Version prenant en compte les remarques de la SDIT/ETD/BUA	Olivier PASQUIN, CAPGEMINI		
17/07/2009	8.1VP3	Compléments et corrections SDIT/ETD/BUA	David MARCHAL		
xx/xx/xxxx	8.1VP4	Corrections BUA finalisée	Le 17/07/2009 David MARCHAL		
04/02/11	8.1VP7	Autres corrections et quelques mises à jour	Le 4/02/2011 E. Heijligers		
24/10/11	8,1VP9	Remarques E2I/EXP, remarques du TOP	Le 24/10/2011 E. Heijligers	A Protière, JF Lebec	
14/12/11	8.1VP10	Mise en forme	Le 14/12/11 JF Lebec	C. Magne Jardinnet	
16/03/11	8.1.1	Changement des versions minimal de firefox et IE. Modification du framework ORM Prise en compte de remarque de D. Tobo sur outlook 2010.	Le 16/03/11 E. Heijligers B. Bouchareb		
25/05/12	8.1.2	Mise à jour des moteurs de recherche sur le poste de travail : ajout de windows desktop search	Le 25/05/2012 E. Heijligers		
12/09/12	8.1.3	Mise à jour de la version Firefox suite aux travaux sur le PdT	Le 12/09/12 E. Heijligers		
28/08/2013	8.1.5	Modification des outils de virtualisation	Le 28/08/2013 E. Heijligers		
14/01/2014	8.1.6	Remplacement de SPIP par Drupal	Le 14/01/2014 E. Heijligers		
04/04/2014	8.1.7	Remplacement d'openoffice par libreoffice Remplacement de struts par JSF Suppression de la version XP pour Windows	Le 04/04/14 E. Heijligers B. Bouchareb		
16/07/2014	8 .1.8	Ajout des couches « sécurité », « injection de dépendances», « transaction », « logs » et mises à jour de composants	Le 16/07/14 E. Heijligers B. Bouchareb		

24/08/15	8 .1.9	Mise à jour des versions de produits	Le 24/08/15	Le 31/08/2015 Boubaker BOUCHAREB	Le 07/09/2015 MC LESPINASSE, M. YOLIN, JB LAPEYRIE, P. NOBLECOURT
28/12/15	8.1.10	Relecture cellule qualité		C. Magne-Jardiné	
09/10/17	8.1.11	- Mise à jour des versions - Suppression : Nagios, Glassfish - Ajout : Flyway, Spring, MapStruct, Edge, Git, NGINX ,HAProxy, Recette usine, Audit de code	Le 10/10/2017 B. BOUCHAREB M.WISSLER	Le 10/10/2017 Boubaker BOUCHAREB	Le 10/10/2017 JB LAPEYRIE MC LESPINASSE, M. VELLUCI, P. NOBLECOURT
04/04/18	8.1.12	Ajout règles : non utilisation trigger non utilisation procédure stockées non utilisation dblink cnil/rgpd qualité de code-source archivages Mise à jour versions Ajout produit: bdocs, mediawiki, dokuwiki, HCP, GSI, Jira, SCCM, spring vault, liquibase Suppression produits : SAMS, Microsoft hyperV, etrust, powerdesigner Ajout chapitres : Coffrefort électronique, service horodatage , système de stockage objet , POS du SI remplacement chapitre : Archivage, la cartographie cible du SI suppression références : ARSIT, SFR, SDIT, Alerte plan de migration technique Applet/flash	Le 04/04/2018 B. BOUCHAREB M.WISSLER R.MORGAND C. LAMBERT	Le 04/04/2018 Boubaker BOUCHAREB	Le 04/04/2018 JB LAPEYRIE MC LESPINASSE, M. VELLUCI, P. NOBLECOURT

09/07/2018	8.1.13	Mise à jour des urls des documents de référence et applicable suite au changement de version d'Alfresco Remplacement du terme « recette usine » par « Vérification pour acceptabilité (VPA) » Ajouts de différents produits : - Squash TM, f.lux, tablette braille esytime, freemind, freeplane, Xmind Pro 8, keepass, Dragon Naturally Speaking, Ghostscript, zed, cryhod, zonecentral, pdfcreator, Microsoft Print to PDF, PDFsam basic, Modelio, Sparx Enterprise Architect. Précision version - TrendMicro officescan	Le 09/07/2018 B. BOUCHAREB M WISSLER R. MORGAND C. LAMBERT	Le 09/07/2018 Boubaker BOUCHAREB	Le 09/07/2018 JB LAPEYRIE MC LESPINASSE, M. VELLUCI, P. NOBLECOURT
24/07/19	8.1.14	Montée de version: tomcat 9, tomcat vault, PHP, Nginx, RHEL, flyway, liquibase, spring boot, spring framework, mybatis, hibernate, angular, Quartz, less, ElasticSearch, Squash, Mega Hopex, Geoserver, mapinfo, TrendMicro OfficeScan, Solr, HCP Suppression du contenu du chapitre 7 « Description des environnements », remplacé par le référencement du document cadre de référence des tests (R09). Modification chapitre supervision technique (seul Centreon est utilisé dorénavant) Suppression de l'utilisation d'oracle JDK au profit de l'openJDK Référencement sill 2019 Ajout : librairie css saas Métrologie (netdata, wmi-exporter, prometheus) Hyper-V (avec précision de migration des versions 2012R2)	Le 24/07/2019 B. BOUCHAREB M WISSLER R. MORGAND C. LAMBERT	Le 24/07/2019 Boubaker BOUCHAREB	Le 24/07/2019 JB LAPEYRIE MC LESPINASSE, M. VELLUCI, P. NOBLECOURT

SOMMAIRE

1. Objectifs....10
1.1. Besoins et périmètre....10
1.2. Acteurs ciblés....11
1.3. Niveaux de préconisation....13
1.4. Domaine d'application....13
1.5. Structuration du CCT....15
2. Références....17
2.1. Documents de référence....17
2.2. Documents applicables....18
3. Principes généraux d'architecture....19
3.1. Propriétés recherchées....19
3.1.1. Performance du SI....19
3.1.2. Découplage / couplage lâche....19
3.1.3. Partage de la ressource poste de travail....19
3.1.4. Principe de non-adhérence....20
3.1.5. Homogénéité des IHM....20
3.1.6. Caractère industriel des applications....20
3.1.7. Principe de continuité....21
3.1.8. Interopérabilité....21
3.2. Règles générales....21
3.2.1. Tenir compte des contraintes liées à l'infrastructure technique existante....21
3.2.2. Choisir des solutions techniques connues et éprouvées....21
3.2.3. Intégration dans l'infrastructure technique....22
3.2.4. Indépendance vis à vis des autres applications....22
3.2.5. Indépendance vis à vis des données....22
3.2.6. Utilisation des ressources de communication....22
3.2.7. Facilité d'exploitation, de déploiement et d'administration....23
3.2.8. Protection des données personnelles....23
3.3. Vers une architecture orientée services....23
3.4. Vers un SI urbanisé....24
3.5. La modélisation du SI....24
3.5.1. Plan d'Occupation des Sols du SI du ministère de la Justice....25
3.5.2. Trajectoire pour parvenir à un SI plus urbanisé....28
3.6. Respect des normes et standards....30
3.7. Référentiels généraux : RGI, RGS, RGAA et Charte ergonomique des sites publics....30
3.7.1. Référentiels généraux....30
3.7.2. Ergonomie et accessibilité....31
3.8. Stratégie « double source »....32
3.9. Architecture applicative....32
3.9.1. Structuration des « applications » en couches....32
3.9.2. Technologies des applications....33
3.10. Sécurité....34
3.10.1. Cycle de vie des applications....35
3.10.2. Gestion de l'identité numérique....35

3.10.3. Identification et authentification....35
3.10.4. Habilitations et profils....36
3.10.5. Architecture réseau multi zones....36
3.10.6. Sécurisation RPVJ....37
3.10.7. Confidentialité / Chiffrement....37
3.10.8. Mobilité (nomadisme et télétravail)....37
3.11. Matrice de classes d'applications....38
3.12. Sûreté de fonctionnement....38
3.12.1. Stratégie « double cœur »....39
3.12.2. Plan de Reprise Informatique (PRI) / Plan de Continuité Informatique (PCI)....39
3.12.3. Qualité de service....39
3.12.4. Gestion de l'extensibilité (« scalability »)....41
4. Applicatifs....42
4.1. Socles des applications....42
4.1.1. Poste de travail....42
4.1.2. Développement spécifique d'applications....49
4.1.3. Serveurs de présentation (Web ou CITRIX)....52
4.1.4. Serveurs d'applications....53
4.1.5. Serveurs de base de données....54
4.1.6. Progiciels....55
4.2. Services applicatifs....56
4.2.1. Services référentiels et nomenclatures....56
4.2.2. Annuaire ministériel....56
4.2.3. Messagerie et travail collaboratif....57
4.2.4. Agenda partagé....58
4.2.5. Gestion de contenus d'entreprise (ECM) / GED....59
4.2.6. Editique....60
4.2.7. Moteur de recherche....61
4.2.8. Acquisition....62
4.2.9. Services de gestion de l'identité numérique....62
4.2.10. Décisionnel....63
4.2.11. Systèmes d'Information Géographique....64
4.2.12. Portail....64
4.2.13. E-formation....65
4.2.14. Orchestration de services....65
5. Infrastructure....67
5.1. Socles techniques....67
5.1.1. Poste de travail....67
5.1.2. Serveurs....68
5.1.3. Serveurs locaux de ressources....69
5.1.4. Imprimantes....70
5.1.5. Autres équipements....71
5.1.6. Virtualisation des ressources....71
Pour les serveurs virtualisés sous Microsoft HyperV 2012R2 (fin de support 2023), il est nécessaire de planifier une migration technique pour migrer vers les versions 2016....72
5.1.7. Mutualisation / consolidation des ressources....72
5.2. Réseau....74

5.2.1. Réseau local (LAN)....74
5.2.2. Réseau distant RPVJ (WAN)....76
5.2.3. Pare-feu....81
5.2.4. Mobilité (nomadisme et télétravail)....81
5.3. Services techniques....82
5.3.1. DNS / Résolution de nom....82
5.3.2. NTP / serveur de temps....82
5.3.3. Annuaires de ressources....83
5.3.4. Plateformes d'échanges....83
5.3.5. Archivage....85
5.3.6. Système de Stockage objet....88
5.4. Services de sécurité....89
5.4.1. Infrastructure de gestion des clés....90
5.4.2. Fédération d'identité....90
5.4.3. Habilitation et gestion des profils....91
5.4.4. Chiffrement (canal, messages et stockage)....91
5.4.5. Garantie de l'intégrité de l'information....92
5.4.6. Signature et vérification de signature électronique....92
5.4.7. Service d'Horodatage....93
5.4.8. Coffre-fort numérique....93
5.4.9. Antivirus....93
6. Exploitation....94
6.1. Administration....94
6.1.1. Sauvegardes....94
6.1.2. Gestion des logs....95
6.1.3. Création d'images / gestion de partitions....95
6.1.4. Ordonnancement....95
6.1.5. Télédistribution....96
6.1.6. Prise de contrôle à distance....96
6.1.7. Gestion de parc....97
6.1.8. Gestion des incidents....97
6.1.9. Mise à jour des applications....98
6.2. Exploitabilité....98
6.3. Supervision....99
6.3.1. Supervision technique....99
6.3.2. Supervision applicative....99
6.4. Capacity planning....100
6.5. Hébergement (services déconcentrés)....100
6.6. Support/Télémaintenance....101
7. Description des environnements....103
8. Cadre de développement....104
8.1. Règles de mise en œuvre....104
8.2. Règles générales de conception de l'architecture de l'application....104
8.3. Architectures « client léger » et « client riche »....105
8.4. Outils de conception d'application....106
8.4.1. Génération de code....108
8.5. Performance des applications....108

8.6. Qualité du code....109
8.7. Matrice d'expression de besoins Sécurité....110
9. Annexes....111
9.1. Glossaire....111
9.2. Référentiels et liens utiles....115
9.2.1. Référentiels....115
9.2.2. Contacts....115

INDEX DES ILLUSTRATIONS

Illustration 1: Structuration des socles et des services mutualisés.....15
Illustration 2: Structuration du SI Justice suivant les quatre vues.....24
Illustration 3: Décomposition du POS du SI.....26
Illustration 4: POS du SI du ministère de la Justice.....27
Illustration 5: Architecture des applications.....29
Illustration 6: Exemple de structuration des applications en cinq couches.....33

1. OBJECTIFS

1.1. BESOINS ET PÉRIMÈTRE

Le Système d'Information (SI) Justice est l'ensemble des dispositions organisationnelles et techniques permettant la création, la modification, la vérification, la mise à disposition, l'utilisation, la circulation interne et l'échange externe d'informations pour le ministère de la Justice.

La partie informatisée du SI se concrétise par un ensemble d'applications et de services qui fonctionnent sur une infrastructure matérielle constituée généralement par une infrastructure de communication et un ensemble de plates-formes.

Dans un contexte d'évolution rapide de l'environnement (législatif, réglementaire, technique, ...) marqué par des changements importants (émergence de la collégialité et du travail collaboratif, coopération accrue à l'interministériel et à l'intergouvernemental, ...), l'objectif principal recherché par le ministère de la Justice est de disposer d'un SI adapté (aux besoins du moment) et agile (rapidement et à coûts réduits).

Dans ce contexte, le **Cadre de Cohérence Technique (CCT)** du SI a plusieurs objectifs :

- permettre aux applications de partager dans de bonnes conditions l'infrastructure matérielle et l'infrastructure de communication ;
- permettre aux applications d'interopérer entre elles et avec les partenaires extérieurs. Sur ce dernier point, le CCT s'appuie, complète et précise le « Référentiel Général d'Interopérabilité (RGI) des SI des administrations » de la DINSIC (cf. [A03]) ;
- assurer une bonne pérennité des composants de base par la mise en œuvre de démarches de choix instrumentées, et limiter la variabilité des plates-formes et des configurations par une évolution concertée des composants ;
- maîtriser les coûts d'acquisition des progiciels et des composants logiciels ainsi que ceux des services d'intégration et d'administration en évitant que chaque application n'impose ses propres composants de base (outils bureautiques, multimédia, de gestion des sauvegardes, de gestion des impressions, couches de communication, bases de données locales, gestion d'habilitation, ...) ;
- assurer la maîtrise technique des environnements en limitant la multiplication des technologies et des méthodes ;
- fiabiliser le système d'information en préconisant des briques techniques de sécurité à mettre en œuvre.

Le CCT est un des résultats majeurs du travail des architectes du SI du SSIC, qui veillent à en maintenir la cohérence, la maintenabilité et l'évolutivité. Ce travail est le fruit d'une activité continue visant à préserver pour le SI ses qualités de cohérence et d'évolutivité.

Le CCT constitue un ensemble de règles, de recommandations et de préconisations qui s'ajoutent à celles des référentiels généraux de la DINSIC (cf. [A03], [A06] et [A07]).

Ce CCT doit être Partagé, Visible et Évolutif :

- **Partagé** :
  Le cadre sera d'autant mieux adapté qu'il répondra aux besoins des utilisateurs du SI y compris les partenaires extérieurs et les usagers, d'une part, et qu'il sera à l'état de l'art, d'autre part.
- **Visible** :
  La visibilité du cadre apparaît comme une condition de son respect par les maîtrises d'ouvrage et maîtrises d'œuvre des projets. La publication du CCT apparaît donc nécessaire, sa mise en ligne sur le site intranet du SSIC y contribuera.
- **Évolutif** :
  Les choix faits correspondent à l'état de l'art, dont on sait qu'il est évolutif et, de ce fait, une actualisation au minimum annuelle du cadre est envisagée. Ces choix doivent être complétés et enrichis à partir de référentiels inter-administrations (notamment le SILL mis en ligne par la DINSIC cf. [A12]) ou de projets innovants opérationnels (conçus en central ou en initiative locale).

NB : Cette nouvelle version du CCT contient uniquement la cible devant être mise en œuvre :
- **pour les nouveaux projets ;**
- **dans le cadre de la migration des applications existantes.**

1.2. ACTEURS CIBLÉS

Les différents acteurs de l'informatique du ministère de la Justice ont des rôles et des demandes différentes par rapport au CCT :

- **Les maîtres d'ouvrage :**

  Ils sont les représentants des utilisateurs et sont les clients des concepteurs et développeurs des applications et services.

  Ils contribuent à la cohérence technique de la partie informatisée du SI en réclamant dans leurs cahiers des charges l'utilisation de produits conformes aux recommandations préconisées par le CCT.

  Ils obtiennent ainsi des solutions :

  - construites à partir d'éléments validés dont la pérennité est garantie par les architectes du SI ;
  - s'intégrant facilement dans l'informatique du ministère de la Justice et potentiellement interopérables avec ceux des partenaires ;
  - contribuant à la maîtrise des coûts de leurs projets ;
  - facilitant une meilleure réactivité des développeurs, des administrateurs et des formateurs.

- **Les utilisateurs finaux** :

  ils sont les bénéficiaires des services et des applications mis à leur disposition et sont clients des administrateurs.

  Ils sont soumis à l'utilisation de solutions préconisées par le CCT et doivent respecter les consignes de sécurité et les modes opératoires.

  Ainsi ils contribueront à :

  - garantir l'interopérabilité et le bon fonctionnement des outils et des services ;
  - faciliter une meilleure réactivité des administrateurs et des supports (centre de support) à quelques niveaux que ce soit (local, régional ou national).

- **Les concepteurs et développeurs d'applications informatiques et de services (la maîtrise d'œuvre) :**

  Ils fournissent aux maîtrises d'ouvrage et aux administrateurs des outils de travail (services, applications).

  Ils trouveront dans le CCT des solutions :

  - testées et validées : qui ont obtenu le « label » du ministère ;
  - sur lesquelles ils pourront obtenir une assistance ;
  - conduisant à une bonne intégration dans l'environnement technique du ministère et à une ouverture vers une bonne interopérabilité avec les partenaires extérieurs.

- **Les administrateurs des systèmes informatiques** :

  Ils trouvent dans les modèles du CCT :

  - la classification des services techniques de l'infrastructure logicielle utilisable,
  - les services et les outils préconisés pour soutenir leurs activités.

- **Les autres administrations et partenaires extérieurs**:

  Ils sont soit des utilisateurs finaux, soit des fournisseurs d'applications auxquels les agents du Ministère doivent accéder. Dans les deux cas, la collaboration avec les autres administrations impose la mise en place de système d'échange et d'interconnexion. La sécurité et l'interopérabilité jouent un rôle fondamental dans ces relations.

  Dans le cadre de ces communications et interfaces inter-applicative, les autres administrations trouveront dans le CCT :

  - la liste des briques logicielles utilisée par le Ministère, en particulier celles liées aux interfaces de communication,
  - des préconisations générales pour faciliter d'interopérabilité.

1.3. NIVEAUX DE PRÉCONISATION

Les règles présentées dans ce document ont différents niveaux de préconisation (inspirés de la RFC2119) :

- **OBLIGATOIRE :** ce niveau de préconisation signifie que la règle édictée indique une exigence absolue du CCT.
- **RECOMMANDÉ :** ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
- **DÉCONSEILLÉ :** ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé.
- **INTERDIT :** ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue du CCT.

Remarque : il n'existe pas de niveau de préconisation « POSSIBLE » car le CCT se veut être un référentiel de recommandations à appliquer et pas un « état de l'art » de ce qu'il est possible de faire.

CCT1	Il est OBLIGATOIRE pour toute équipe de projet interne ou externe de spécifier et justifier les points suivants : • les circonstances et justifications de non-respect d'une règle RECOMMANDÉE, • les circonstances et justifications de non-respect d'une règle DÉCONSEILLÉE, • les justifications des exceptions à toute règle absolue (OBLIGATOIRE ou INTERDIT) ; et dans ce dernier cas, le bureau SSIC/SDIDE/ETD/APT assurera la coordination des équipes du SSIC afin d'accepter ou refuser l'exception.

1.4. DOMAINE D'APPLICATION

Le cadre de cohérence technique (CCT) du ministère de la Justice tient compte des recommandations du Référentiel Général d'Interopérabilité (RGI) publié par la DINSIC (cf. [A03]). Ce référentiel est induit par l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Le RGI spécifie l'ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des SI du service public. Le RGI est de nature à simplifier l'intégration de nouveaux systèmes et à faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs. Il détermine notamment la sémantique, les normes et les standards qui doivent être utilisés par les autorités administratives.

Les recommandations du CCT sont à prendre en considération lors de la préparation de tout projet technique apportant des modifications aux SI qui les utilisent, qu'il s'agisse des applications nationales ou de celles relevant de l'initiative locale, tant pour leurs échanges internes que pour entrer en relations avec d'autres collectivités publiques, ou avec les partenaires et usagers de l'administration, citoyens, associations ou entreprises.

En conséquence, **le RGI publié par la DINSIC et le présent CCT devront être référencés dans les cahiers des charges en y intégrant la formulation suivante :**

Le ministère de la Justice a spécifié et maintient à jour un ensemble de recommandations concernant les composants techniques (logiciels et matériels) devant être utilisés dans le cadre des projets et systèmes mis en œuvre au sein du SI Justice. Ces recommandations sont rassemblées au sein du cadre de cohérence technique (CCT) joint en annexe au présent document.

Outre les détails techniques que le candidat décrira dans sa proposition, il se doit de justifier les choix logiciels par rapport à ceux présentés dans le CCT.

Le candidat, dans sa proposition, détaille de manière claire et synthétique les choix qu'il effectue, en précisant, pour chaque composant logiciel :

a) s'il s'agit d'un composant libre présent au CCT, les principaux points techniques justifiant ce choix ;

b) s'il s'agit d'un composant non libre présent au CCT, les raisons qui poussent le titulaire à le préférer au composant libre. Ces motifs doivent faire apparaître comme incontestables les gains pour l'administration, soit en termes financiers sur une perspective de long terme, soit en termes de délais de réalisation, soit en termes de risques critiques pour le projet ;

c) s'il s'agit d'un composant libre non inscrit au CCT, les raisons qui poussent le titulaire à le préférer au(x) composant(s) logiciel(s) référencé(s) par le CCT. Dans ce cas, la comparaison portera notamment avec le composant libre correspondant présent au CCT, dans le cas où le CCT référence un composant de ce type ;

d) s'il s'agit d'un composant non libre et non inscrit au CCT, les raisons qui poussent le titulaire à le préférer au(x) composant(s) référencé(s) par le CCT, suivant une présentation identique à celle du point (b) ci-dessus mais étendue à la comparaison avec le ou les éventuel(s) composant(s) non libre(s) référencé(s) par le CCT.

Dans le cas de la maintenance des applications non conformes au CCT, ces choix du candidat sont à envisager uniquement dans le cadre d'une migration progressive de l'application.

Les choix faits correspondent à l'état de l'art, dont on sait que l'environnement législatif, réglementaire ou technique est évolutif. Ainsi, à l'instar du RGI, une actualisation au minimum annuelle est effectuée. C'est pourquoi :

Toute difficulté rencontrée lors de la mise en œuvre du cadre de cohérence technique devra être signalée au bureau SG/SSIC/SDIDE/ETD/APT qui coordonnera les équipes du SSIC pour qu'une réponse y soit donné.

CCT2	Il est OBLIGATOIRE que les applications se conforment au CCT. L'adoption du CCT sera d'autant plus facile qu'il sera de qualité, maintenu à jour et mis en ligne sur l'intranet : ***nul ne peut l'ignorer***.

Pour une application s'appuyant sur des techniques encore inscrites au CCT mais qui ne sont plus recommandées, un plan de migration doit être étudié si possible à court terme.

CCT3	De même, il est OBLIGATOIRE que les applications d'initiative locale se conforment au CCT. Elles doivent être exploitées et administrées par des structures locales, également en charge de la maintenance, du support utilisateurs ainsi que de la gestion des évolutions.

CCT4	Il est OBLIGATOIRE pour toute nouvelle application non conforme au CCT de faire une demande de dérogation officielle motivée (cf. règle CCT1)

Dans le cadre d'une mutualisation des expériences, la description d'applications à contexte innovant est remontée au bureau SSIC/SDIDE/ETD/APT.

Si une application utilise un composant logiciel ou technique non référencé mais concernant un segment du SI n'ayant pas été identifié dans le CCT, une déclaration est également nécessaire et peut aboutir à une évolution du CCT.

1.5. STRUCTURATION DU CCT

Dans le CCT, la composante technique des applications est vu comme un assemblage, statique ou dynamique, de socles et de services applicatifs mutualisés qui séparent ces applications des caractéristiques propres aux matériels et aux logiciels de base offerts par les socles et les services techniques mutualisés.

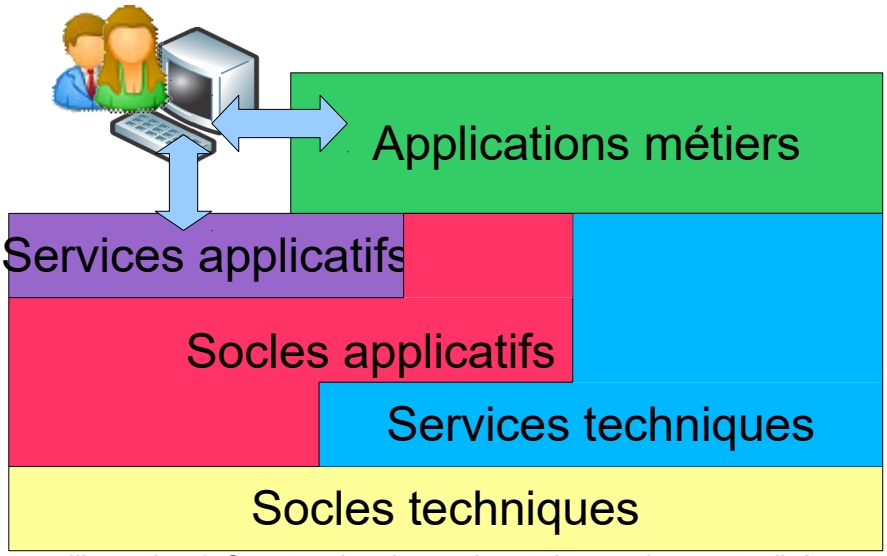

Illustration 1: Structuration des socles et des services mutualisés

Services applicatifs :

Les clients de ces services mutualisés sont les utilisateurs des différentes directions métiers.

Ce sont par exemple, un annuaire partagé, un service de messagerie qui peuvent être utilisés soit par des utilisateurs, soit par des applications métiers.

Socles applicatifs :

Ils permettent la mise en œuvre :

- des services applicatifs mutualisés et
- des applications métiers.

Ce sont par exemple des logiciels « serveurs d'application » ou des moteurs de base de données.

Services techniques :

Les services techniques correspondent à des services d'infrastructure dont les clients sont les applications métiers des différentes directions métiers ainsi que les socles applicatifs.

Ces services techniques sont par exemple un service de temps pour garantir que tous les serveurs sont à l'heure, ou un service de résolution de nom.

Socles techniques :

Les socles techniques correspondent aux couches logicielles basses relatives au système d'exploitation à utiliser.

Ils servent à la mise en œuvre :

- des socles applicatifs mutualisés et
- des services techniques mutualisés.

2. RÉFÉRENCES

2.1. DOCUMENTS DE RÉFÉRENCE

Réf	Version	Titre
[R01]		Configurations des postes de travail (Informatique/Marchés) : http://intranet.justice.gouv.fr/site/informatique-telecom/marches-6094/achat-materiels-prestations-6096/odice-2017-2019-99749.html
[R02]		Configurations des ordinateurs portables (Informatique/Marchés) http://intranet.justice.gouv.fr/site/informatique-telecom/marches-6094/achat-materiels-prestations-6096/accord-cadre-interministeriel-2015-2019-67241.html Valable jusqu'à fin décembre 2018. passé ce délai se référer à [R01].
[R03]	02/2018	Documentations liée à la solution de stockage objet /SDIT-Projets/Projets/03 Transverse/Architecture-Urbanisation/Services Applicatifs transverses/HITACHI HCP - Stockage Objet
[R04]	1.6	Manuel interface LDAP/SSO avec les applications /SDIT-Projets/Projets/AnnuaireLDAP/03 Conception/04 Conception détaillée/02 Conception technique/MANU_LDAP_SSO_InterfaceAvecApplications_v1.6.odt
[R05]	1.0	Modalité d'intégration d'une application au SSO Justice /SDIT-Projets/Projets/AnnuaireLDAP/03 Conception/04 Conception détaillée/02 Conception technique/NOTE-Modalites_Integration_Application_SSO_Justice_V1.0.odt
[R06]	V1.2	Offre de services de la PFE /SDIT-Projets/Projets/03 Transverse/Architecture-Urbanisation/Services Applicatifs transverses/PFE- Plateforme d'échange/DOSS-PFEv2_Offre_de_Services_V1.2.pdf
[R07]	V7 20/02/2018	Détail configuration serveur /SDIT/SDIT Interne/TOP/01 Commun SDIT/06 BPU marchés TOP en cours d'exécution/Econocom_2014-12-92189_Serveurs X86
[R08]		Plan d'Occupation des Sols du SI du ministère de la Justice (version détaillée) http://urbi.intranet.justice.gouv.fr/
[R09]	1.1	Cadre de référence de la méthodologie transverse de la démarche de tests du Ministère de la Justice. STR_PRBB_001-C1_Cadre de référence des tests_V1.1

2.2. DOCUMENTS APPLICABLES

Réf	Version	Titre
[A01]	1.1 ou supérieure	Charte graphique et ergonomique du ministère de la Justice /SDIT-Projets/Projets/03 Transverse/Architecture-Urbanisation/Accessibilité – ergonomie/Charte_ergonomique_MJ_V1.1.doc
[A03]	2.0 ou supérieure	Référentiel Général d'Interopérabilité http://references.modernisation.gouv.fr/interoperabilite
[A06]	2.0 ou supérieure	Référentiel Général de Sécurité - Normes et Recommandations https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/
[A07]	3 2017	Référentiel Général d'Accessibilité pour les Administrations - Normes et recommandations https://references.modernisation.gouv.fr/rgaa-accessibilite/
[A08]	1.0 ou supérieure	Charte Internet de l'État http://references.modernisation.gouv.fr/charte-internet-de-letat
[A09]	6.4 ou supérieure	Protocole de livraison des mises à jour applicatives /SDIT-Projets/Projets/03 Transverse/Architecture-Urbanisation/Centres de Production – Normes/PRO_EXP_ProtocoleLivraisonMaJAppli_V6.4.odt
[A10]	2016 V9	Politique Ministérielle de Défense et de Sécurité (PMDS) http://intranet.justice.gouv.fr/site/modernisation/art_pix/20160818_PMDS_V9.pdf
[A11]	1.5 ou supérieure	Le cadre de production : /SDIT-Projets/Projets/03 Transverse/Exploitation et Production/99 Documents Type/Validé/cadre de production v1.5.odt
[A12]	2019	Socle Interministériel de Logiciels Libres 2019 : http://references.modernisation.gouv.fr/socle-logiciels-libres
[A13]	1.0_0	Cadre commun d'urbanisation du SI de l'Etat https://references.modernisation.gouv.fr/sites/default/files/Cadre_Commun_d'Urbanisation_du_SI_de_l'Etat_v1.0_0.pdf Guide détaillé du Responsable de Zone Fonctionnelle du SI de l'État *Complément n°1 au Cadre Commun d'Urbanisation du Système d'Information de l'État version 1.0* https://references.modernisation.gouv.fr/sites/default/files/Guide détaillé du RZF v1.0_0.pdf

3. PRINCIPES GÉNÉRAUX D'ARCHITECTURE

3.1. PROPRIÉTÉS RECHERCHÉES

Les propriétés recherchées pour le SI justice à travers le respect du CCT sont principalement les suivantes :

- **performance du SI** : les applications sont construites avec des briques/composants validés, permettant ainsi de maîtriser les risques et de garantir les performances ;
- **limitation du couplage entre les applications** : afin d'assurer une plus grande agilité et une meilleure réutilisation, il convient de découpler les modules applicatifs ;
- **partage de la ressource poste de travail** : les applications et services locaux ou distants doivent être accessibles à partir d'un poste de travail unique ;
- **non-adhérence** : afin de limiter les dépendances, les interactions entre les différents composants du logiciel doivent principalement utiliser des interfaces standardisées et normalisées dont les spécifications sont publiques ;
- **homogénéité des interfaces homme / machine** : la présentation des informations doit obéir au même standard pour chacune des applications ;
- **industrialisation** : la conception, la réalisation, la mise en œuvre et l'évolution des composants du système informatique reposent sur un processus industrialisé ;
- **continuité** : les solutions préconisées doivent préserver le capital constitué par les données du ministère et le matériel qui le supporte ;
- **interopérabilité** : les interfaces respectant les normes et standards et étant connues et définies, le système doit continuer à fonctionner avec d'autres produits ou systèmes existants ou futurs;

3.1.1. Performance du SI

Le système d'information est un bien commun que doivent se partager tous les utilisateurs. Ses performances telles que perçues par les utilisateurs (temps de réponse, temps d'indisponibilité) sont la conséquence de choix techniques (bande passante, réplication de données).

Le respect d'architectures types, le choix de briques logicielles standards ainsi que le respect de méthode de développement et de test permettront de garantir de meilleures performances au SI.

3.1.2. Découplage / couplage lâche

L'agilité du SI est sa faculté à pouvoir évoluer rapidement face à l'arrivée de nouveaux besoins, de nouvelles technologiques, disparition d'un fournisseur, arrêt de support, contraintes de sécurité …

La mise en œuvre du découplage permet de faire évoluer les modules applicatifs indépendamment les uns des autres, sous réserve de respecter les interfaces définies.

3.1.3. Partage de la ressource poste de travail

Le poste de travail doit permettre de rationaliser et de fédérer les accès des utilisateurs et doit permettre l'accès à l'ensemble des applications utiles et nécessaires à l'utilisateur.

Tous les services (messagerie, intranet, partage de ressources, …), toutes les applications métiers, les suites bureautiques et les logiciels de groupe de travail doivent être accessibles à partir d'un même poste de travail. Seules des raisons de sécurité ou d'habilitation peuvent limiter la portée de ce principe.

Cela requiert pour les développeurs de s'affranchir de paramètres spécifiques de configuration du poste de travail ou tout au moins de les publier et de vérifier leur compatibilité avec l'environnement standard des futurs utilisateurs.

3.1.4. Principe de non-adhérence

Afin de limiter les dépendances, les interactions entre les différents composants du logiciel utilisent des interfaces standardisées et normalisées dont les spécifications sont publiques.

De cette manière, il sera plus facile de faire évoluer les composants matériels ou logiciels indépendamment les uns des autres, ou de les réutiliser voire de les mutualiser, c'est-à-dire d'en faire bénéficier d'autres applications.

3.1.5. Homogénéité des IHM

La présentation des informations doit obéir au même standard pour chacun des métiers.

Cela permet de fournir aux utilisateurs une interface d'accès aux services et aux applications répondant aux mêmes critères de présentation afin de réduire la phase d'apprentissage et de favoriser la productivité.

L'utilisateur est ainsi moins dépaysé lorsqu'il passe d'une application à l'autre. Les coûts de conception, de développement et de maintenance sont également réduits en raison d'une meilleure homogénéité des applications.

3.1.6. Caractère industriel des applications

La conception, la réalisation, la mise en œuvre et l'évolution des composants techniques du système informatique et de communication doivent reposer sur un processus industrialisé fondé sur le recours à des composants ou à des modules.

Ainsi, les infrastructures et les applications informatiques se présentent comme la mise en œuvre d'un ensemble de technologies dont les composants interopèrent. Chacune de ces technologies référencées est déployée et tenue cohérente par des processus maîtrisés et des acteurs identifiés et spécialisés.

Cela permet d'accroître la productivité des développements informatiques, de favoriser la réutilisation des composants, d'en faciliter la maintenance, l'exploitation et le support, et ainsi de mieux en maîtriser les coûts.

3.1.7. Principe de continuité

Les solutions techniques préconisées préserveront le capital constitué par le SI et les données du ministère et, le parc matériel et logiciel amortissable qui permet d'y accéder.

Chaque application doit intégrer un système de sauvegarde, de stockage et d'archivage des données. En vue de conférer une grande efficacité à la dernière action à intervenir, les systèmes doivent être cohérents entre eux d'une application à l'autre.

Il convient également, afin de garantir la pérennité des données, d'utiliser des formats standards et normalisés.

3.1.8. Interopérabilité

L'interopérabilité est la capacité d'un système ou d'un produit, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre.

Le SI doit se conformer aux différentes standards et normes interministériels et notamment au RGI, au RGS et au RGAA : technologies, sémantique, sécurité et accessibilité.

Pour cela, le CCT donne des préconisations en termes de protocoles, formats de fichier, interfaces publiées (API) visant à garantir un maximum d'interopérabilité.

3.2. RÈGLES GÉNÉRALES

L'utilisation de produits communs à plusieurs applications ne suffit pas à elle seule à garantir la cohérence et l'évolutivité du SI. Les règles de mise en œuvre suivantes sont valables pour les applications conformes au CCT, quel que soit leur environnement technique (plate-forme, système d'exploitation, ...)

3.2.1. Tenir compte des contraintes liées à l'infrastructure technique existante

Dans le cadre de l'élaboration de solutions techniques, ne pas omettre la prise en compte de l'existant et des moyens physiques associés. Ils peuvent devenir de réelles contraintes sur les solutions cibles.

Le SI doit faciliter et favoriser l'intégration et l'interopérabilité du patrimoine applicatif existant :

- par la mise à disposition de services standards et normalisés ;
- par la garantie de l'indépendance vis-à-vis des plates-formes technologiques (« platform agnostic »). Cela permet de développer des services dans différentes technologies (Java EE, PHP, différents progiciels) tout en garantissant l'interopérabilité.

3.2.2. Choisir des solutions techniques connues et éprouvées

Pour les aspects non couverts par le cadre de cohérence, seules des solutions techniques connues et éprouvées et dont il existe au moins une référence opérationnelle doivent être proposées.

3.2.3. Intégration dans l'infrastructure technique

Pour chaque application, il est nécessaire de définir les versions de logiciels et les types de matériel sur lesquels elle est destinée à être intégrée et qualifiée.

Les applications doivent n'utiliser que les composants logiciels inclus dans le CCT en vigueur sur les plates-formes utilisées, sauf dérogation ayant fait l'objet d'une demande spécifique.

Les applications utiliseront les fonctions standard du système et les mécanismes standard d'interface avec les logiciels de base, de façon à faciliter les portages ou les évolutions de version du système.

Les applications doivent pouvoir évoluer indépendamment d'une montée de version des composants transverses, dans le cadre de montées de version référencées de façon homogène sur l'ensemble des plates-formes.

3.2.4. Indépendance vis à vis des autres applications

Les programmes (code source et exécutables) des applications sont indépendants les uns des autres.

Aucune modification d'une application ne peut être effectuée dans le cadre du développement et du déploiement d'une autre application sauf concertation sur des données échangées.

Dans le cas où plusieurs applications partageraient des équipements communs (poste de travail, serveurs) leurs fichiers (exécutables, fichiers de données, bases de données, produits logiciels spécifiques, ...) doivent être stockés dans des partitions ou répertoires qui leur sont réservés de façon à ne pas interférer avec les procédures d'administration et d'exploitation.

Dans le cas d'échange inter-applicatif, il est préconisé de mettre en œuvre un format pivot indépendant de chaque application. (cf. chapitre 5.3.4 Plateformes d'échanges)

3.2.5. Indépendance vis à vis des données

Les données sont propres aux applications. Cela s'applique à toutes les données; de production, d'infocentre, d'habilitation et de référence.

CCT5	Il est INTERDIT à une application d'accéder directement à la base de données d'une autre application.

Les échanges de données entre les applications sont réalisés en utilisant les outils et les mécanismes définis dans le cadre de cohérence.

3.2.6. Utilisation des ressources de communication

Les applications peuvent utiliser le réseau local comme support physique, sous réserve qu'elles respectent les règles de nommage et d'adressage.

Les équipements de communication (liaisons et routeurs) sont des ressources partagées par les applications. Le dimensionnement des réseaux et la détermination des flux applicatifs doivent tenir compte des créneaux horaires libres pour les flux batch, et de l'utilisation des liaisons par les autres applications pour les flux transactionnels.

3.2.7. Facilité d'exploitation, de déploiement et d'administration

Il est recommandé, pour chaque nouvelle application, qu'elle comporte peu de fonctions d'exploitation nécessitant d'intervenir sur le site, empêchant par-là toute possibilité d'exploitation distante.

Il est également recommandé de mettre en œuvre des procédures de mises à jour nécessitant un minimum d'interventions.

L'architecture du SI évolue vers une centralisation des traitements et des données pour faciliter les évolutions organisationnelles.

Le SI doit faciliter et simplifier le déploiement et l'utilisation des fonctions par la mise en œuvre d'IHM de types « client léger » et « client riche » AJAX / RIA**.**

3.2.8. Protection des données personnelles

La Commission Nationale Informatique et Libertés est chargée de veiller à la protection des données à caractère personnel et de la vie privée. Les contraintes qu'elle impose peuvent impliquer des changements très lourds dans une application informatique, tant d'un point de vue fonctionnel que technique.

A partir du 25 mai 2018, entre en vigueur le Règlement Général sur la Protection des Données (RGPD).Il a été mis en place par l'Union Européenne pour harmoniser et normaliser les différentes lois qui existent dans les pays de l'UE, sur la protection des données personnelles.

En pratique, la plupart des formalités préalables actuelles auprès de la CNIL (déclarations, autorisations) vont disparaître, au profit d'une logique de conformité continue. Les organismes qui traitent des données personnelles devront veiller au respect des textes tout au long du cycle de vie de la donnée. En contrepartie de cette réduction du contrôle en amont, le RGPD renforce les pouvoirs de sanction des CNIL nationales.

A noter, il existe également (dans le cadre du RGPD) une Directive spécifique pour le domaine de la police et de la justice.

CCT6	**Il est OBLIGATOIRE de prendre en compte les contraintes CNIL/RGPD, ainsi que la Directive spécifique police-justice au plus tôt dans la vie d'un projet**.

3.3. VERS UNE ARCHITECTURE ORIENTÉE SERVICES

Le SI du ministère de la Justice se structure de manière progressive vers un **SI basé sur une architecture orientée services** (SOA) constituée d'une plateforme **de services normalisés, mutualisables et réutilisables**, respectant et mettant en œuvre des standards ouverts du marché (IP, HTTP, SSL, XML, Web Services).

3.4. Vers un SI urbanisé

L'urbanisation est un processus permanent qui organise la transformation progressive du système d'information existant autour d'une architecture d'ensemble et de principes, dans une optique de simplification, de rationalisation, d'agilité.

Elle permet :

- d'acquérir la souplesse et la réactivité nécessaire pour s'adapter aux contraintes de l'environnement.
- d'améliorer et de favoriser la modularité, la maintenabilité et l'agilité du SI par une approche rationalisée des demandes d'évolution en réutilisant en majeure partie le système existant.
- de faciliter l'analyse d'impacts liés aux évolutions et d'en maîtriser les risques.
- de faire porter les efforts de développement sur les nouvelles fonctionnalités à forte valeur ajoutée.
- de bénéficier des avancées technologiques sans faire table rase du passé en maintenant une continuité de service.

L'urbanisation est donc un outil d'aide à la décision qui facilite les choix stratégiques et tactiques liés à l'évolution du SI.

3.5. LA MODÉLISATION DU SI

Le dispositif méthodologique de spécifications et de conception du Système d'Information Justice, notamment du point de vue des activités d'architecture et de modélisation, s'articule selon quatre vues : Métier, Fonctionnelle, Applicative et Technique.

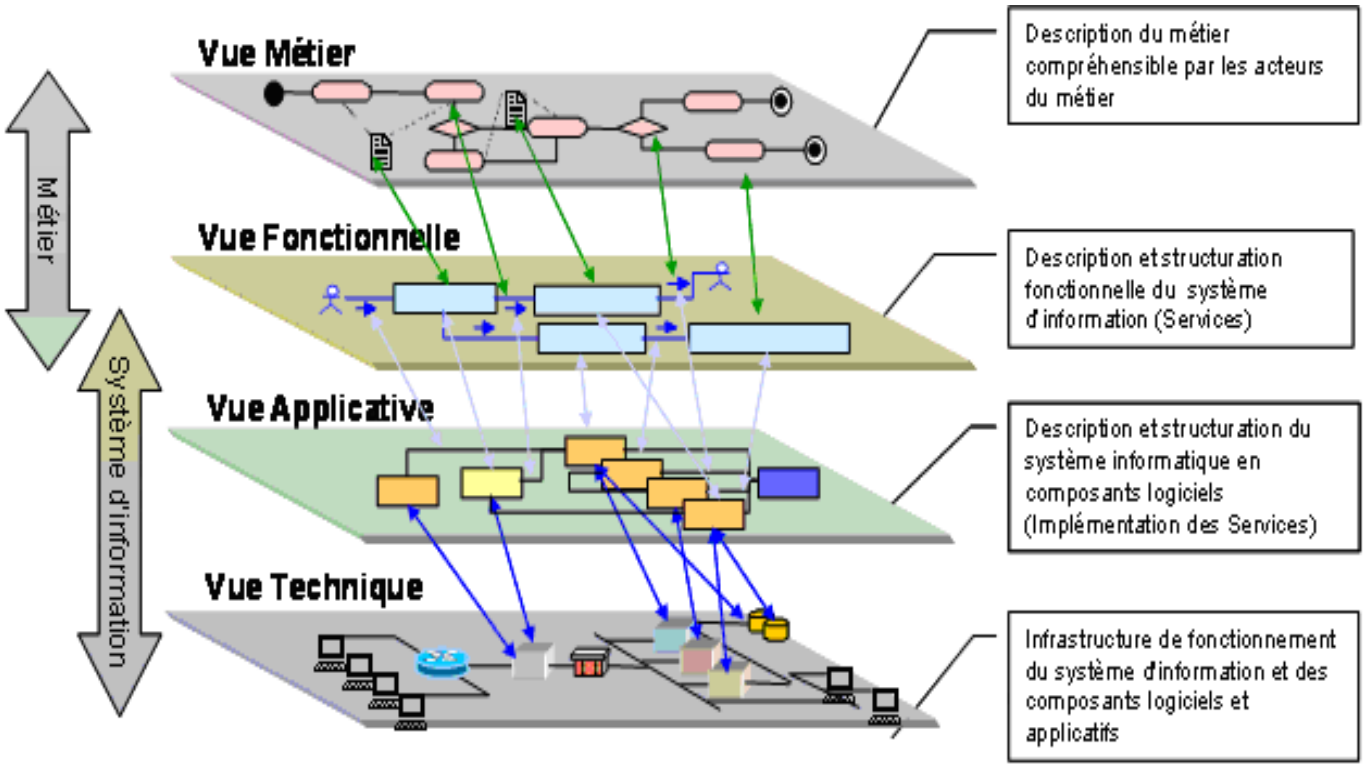

Illustration 2: Structuration du SI Justice suivant les quatre vues

La vue **Métier** est une description du métier et de son organisation compréhensible par les acteurs impliqués. Elle permet l'identification des acteurs, des processus métiers, des événements et de leurs interactions. Elle décrit le métier comme une suite d'activités, s'intéressant aux finalités des processus justice indépendamment de toute orientation informatique.

La vue **Fonctionnelle** est une description fonctionnelle du système d'information qui permet d'identifier les concepts, les services et les flux qui participent aux processus métiers. Elle précise également leur organisation dans une architecture de services urbanisés.

La vue **Applicative** est une description du système informatique en terme de composants logiciels et d'applications (développements spécifiques, briques logicielles, interfaces) regroupés en fonction de critères fonctionnels et/ou organisationnels. Elle décrit l'implémentation des services et leur utilisation sous forme de composant applicatifs au sein du SI.

La vue **Technique** décrit l'infrastructure de fonctionnement du système d'information et des composants logiciels et applicatifs. Elle indique comment les services et les concepts sont mis en œuvre de manière à garantir la qualité de service et d'assurer l'exploitabilité des logiciels de base (OS et utilitaires) ainsi que des matériels (SAN, stations de travail, réseau, firewall).

A ces quatre vues « classiques », peut s'ajouter une vue **stratégique** de l'urbanisation.

3.5.1. Plan d'Occupation des Sols du SI du ministère de la Justice

Le POS du SI du ministère de la Justice repose sur les principes décrit dans la Nomenclature de Référence Fonctionnelle (NRF) du SI de l'État (cf. document référencé [A13]).

Ce POS est organisé selon 5 grands domaines : un domaine « Opération » et 4 domaines transverses.

Un domaine « coeur de métier » :

- Le domaine « **Opération** » regroupe l'ensemble des fonctions et des objets métiers qui ont une orientation, une finalité, au service des usagers (particulier, professionnel, association, etc.), de la société, de l'Union européenne, ou d'acteurs internationaux

Quatre domaines « transverses » :

- Le domaine « **Pilotage & Contrôle** » regroupe l'ensemble des fonctions et d'objets métiers de pilotage transverses des activités de l' État, ainsi que des fonctions de contrôle (audit, inspection...).
- Le domaine « **Ressource & Support** » regroupe l'ensemble des fonctions et des objets métiers d'appuis ou de support aux autres domaines. Il s'agit principalement des fonctions de gestion des ressources : RH, Finances, Immobilier, Moyen Généraux, IT...
- Le domaine « **Échange & Relations** » regroupe l'ensemble des fonctionnalités et des objets métiers relatifs aux échanges entre les différents acteurs contributeurs, utilisateurs, partenaires, clients du SI de l' État . Les échanges présentent un caractère particulier qu'il convient d'une part de tracer mais aussi de gérer de manière plus globale en les regroupant par thème : usager, agent , autorités administratives , collectivités territoriales, relations européennes, internationales... La séparation fonctionnelle entre la gestion de la relation avec les usagers, et la gestion de la relation

avec les agents tend à se réduire. Le parti pris ici est de rapprocher l'ensemble de ces types d'échanges en un seul grand domaine.

- Le domaine « **Données transverses** » regroupe et isole l'ensemble des données, et des fonctions qui les manipulent, transverses ou communes à la plupart, voire la totalité des zones des autres domaines. Ces données transverses sont organisées par thèmes : usager, administration, informations géographiques, etc.

Chaque domaine est découpé en zones, elles-mêmes décomposées en quartiers et en blocs.

Les éléments de découpage fonctionnel du SI sont appelés des « secteurs fonctionnels ». Le premier niveau de découpage est appelé « domaine » (les 5 grands domaines décrits précédemment), le second, qui est réellement le premier niveau fonctionnel significatif est appelé « zone », le suivant « quartier » et enfin « bloc ».

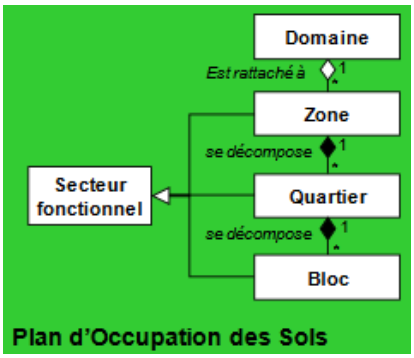

Illustration 3: Décomposition du POS du SI

La structuration du POS du SI permet de rationaliser les composants applicatifs et les référentiels.

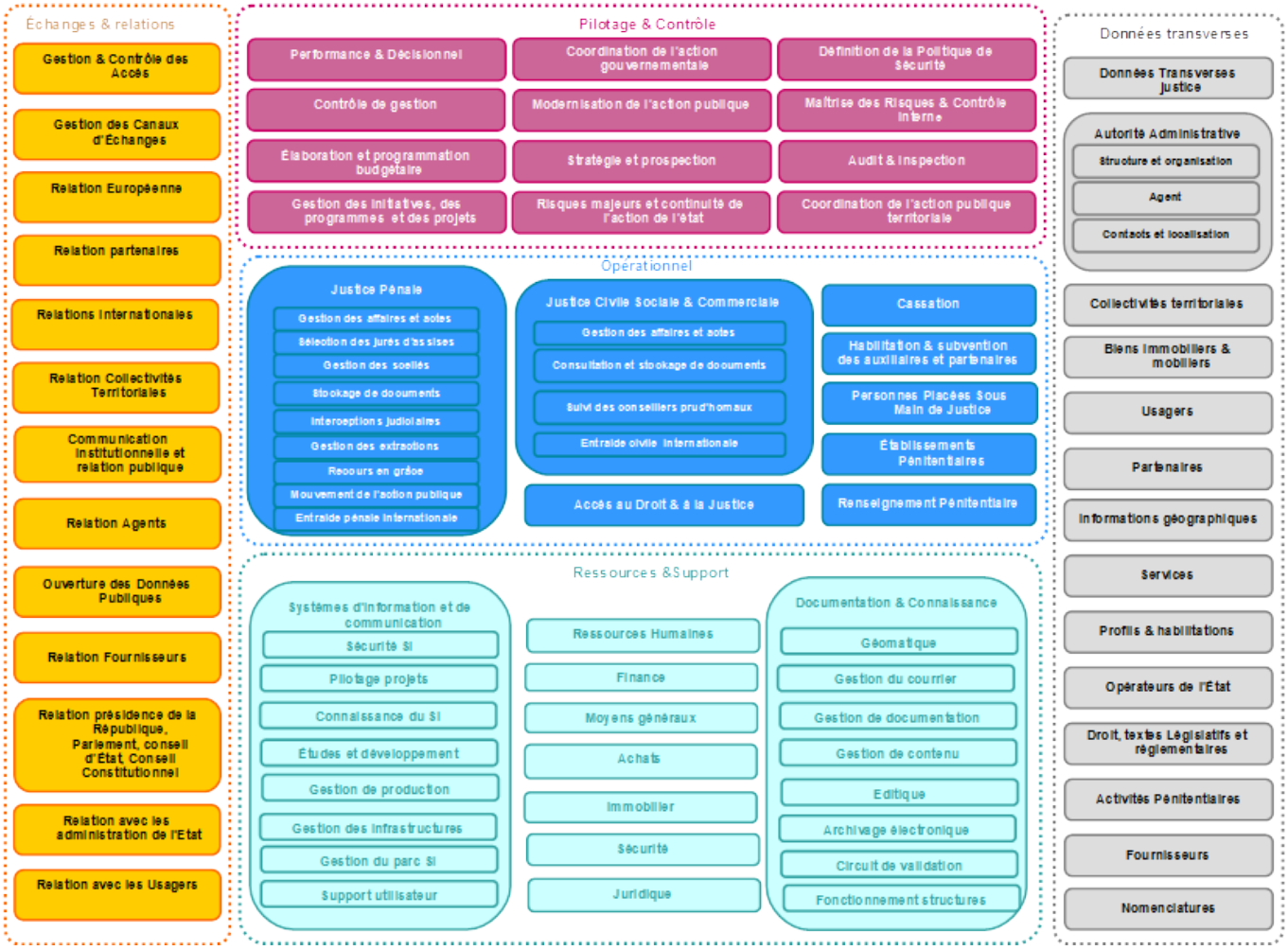

Illustration 4: POS du SI du ministère de la Justice

Cette structuration met au centre du SI les services cœur de métier avec les 8 zones métiers suivantes:

- Activités juridictionnelles pénales ;
- Activités juridictionnelles civiles, sociales et commerciales ;
- Accès au droit et à la justice ;
- Cassation ;
- Habilitation et subvention des auxiliaires et partenaires ;
- Gestion des personnes placées sous main de justice ;
- Établissements pénitentiaires ;
- Renseignement pénitentiaire.

Ces zones « métiers » s'appuient sur le domaine « Données transverses » qui fournit les données partagées comprenant à la fois les nomenclatures et les données communes à différentes fonctions métier comme les adresses, les individus, etc.

Le SI fournit également, via la zone « Documentation & Connaissance » du domaine « Ressources & Support », des services transverses et mutualisés :

- gestion de processus métier ;
- moteur de recherche ;
- éditique ;
- gestion électronique de document / numérisation ;
- système d'information géographique ;
- etc.

Le quartier « Sécurité SI » de la zone « Système d'information et de communication » du domaine « Ressources & Support » fournit différents services de sécurité du SI (Sécurisation des flux, IGC, services de chiffrements/signatures, traçabilité,...).

Le domaine « Echange & Relations » permet d'isoler et de rationaliser les échanges entre le SI et les SI externes et la zone d'accès permet de fournir aux différents acteurs (citoyens, justiciable, agent, partenaires, etc.) l'accès aux services du SI. C'est dans ce domaine fonctionnel que l'on trouve les briques d'authentification , d'habilitations, de gestion de messagerie électronique, l'annuaire ministériel, la plateforme d'échange, etc...

Le domaine « Pilotage & Contrôle » permet de réaliser des infocentres par métier ou transverses de façon découplée des applications opérationnelles.

Pour obtenir une vision détaillée du POS du SI, se référer à l'url [R08].

3.5.2. Trajectoire pour parvenir à un SI plus urbanisé

Référentiels et dictionnaire partagés

La structuration du SI permet de mettre en œuvre des référentiels de données et de services partagés. Cette utilisation de référentiels et de services mutualisés, en généralisant l'accès direct aux données via des services de consultation, évite de dupliquer les données et permet ainsi de rationaliser les flux et les échanges de données au sein du SI. Toutefois pour répondre aux besoins et contraintes de performance, il doit être possible de faire des copies de données en dernier recours en récupérant les données à la source tout en laissant l'application source maître des données.

Le SI s'appuiera sur un dictionnaire des concepts/données normalisé et partagé permettant de définir une sémantique et une structuration des concepts uniques pour tout le SI.

Ces référentiels sont par exemple :

- un référentiel de nomenclatures (SRJ par exemple, cf. chapitre 4.2.1)
- un référentiel d'identité (annuaire Ministériel)
- un dictionnaire de données.

CCT7	Il est OBLIGATOIRE d'utiliser les référentiels ministériels pour les applications.

CCT8	Il est OBLIGATOIRE de mettre en œuvre un processus de mise à jour régulière du référentiel pour les applications utilisant une copie du référentiel.

CCT9	Il est INTERDIT de faire des modifications locales sur des données provenant d'un référentiel.

Mutualisation et modularisation des applications

La structuration du SI permet de mettre en place des sous-ensembles homogènes, cohérents et faiblement couplés les uns aux autres. Ces sous-ensembles se matérialisent par des blocs de services autonomes et faiblement couplés. Chaque bloc de service est responsable de la cohérence de ses données et ne présente aux autres blocs qu'une interface composée de méthodes. Seule l'application maître de ses données peut y accéder directement .

Le schéma suivant illustre ce principe :

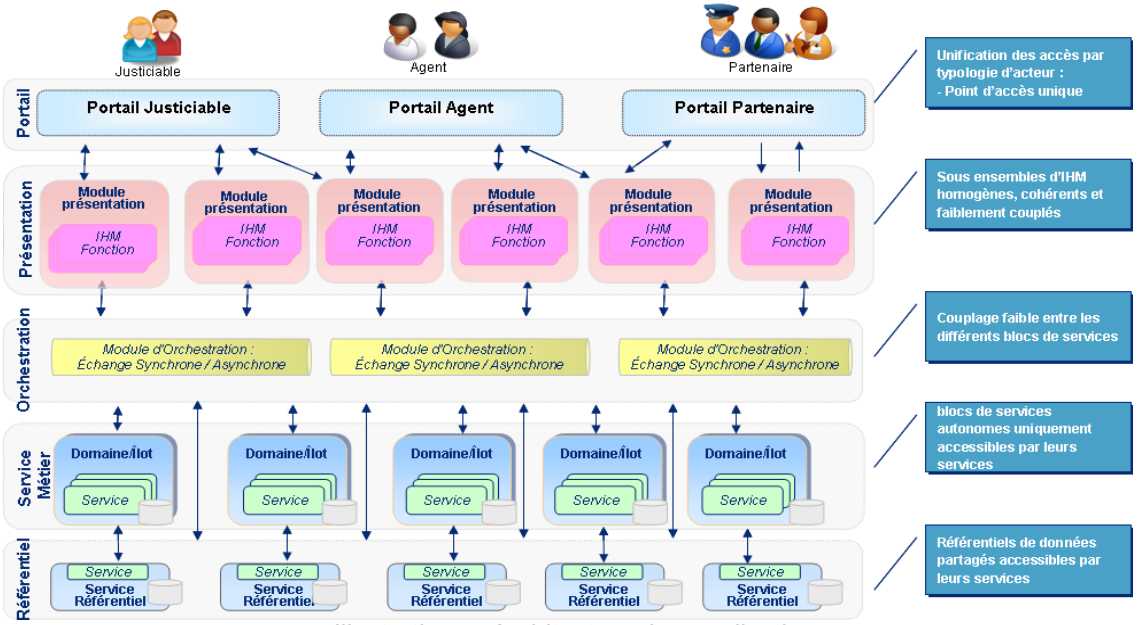

Illustration 5: Architecture des applications

Rationalisation des échanges internes et externes

Les échanges sont régulés par la mise en œuvre d'une plateforme d'échanges mutualisée. Cette plateforme gère les échanges internes pour découpler les sous-systèmes du SI en s'appuyant, par exemple, sur un bus de service synchrone/asynchrone. Cette régulation s'applique aussi pour les échanges avec les SI externes pour mutualiser les extractions et les traitements de transformations et de routage.

Les échanges entre les sous-systèmes opérationnels et les sous-systèmes de statistique et de pilotage doivent être découplés afin de diminuer et unifier les traitements d'extractions des données. Ces informations doivent être déversées dans un sas commun appelé aussi ODS (Operational Data Store). Ce sas permet d'intégrer les données de différentes sources et d'alimenter des infocentres et des outils décisionnels. Ce sas permet d'autre part de disposer de l'ensemble des données déjà extraites pour des besoins ultérieurs sans avoir à mettre en œuvre de nouvelles extractions.

3.6. RESPECT DES NORMES ET STANDARDS

Afin de parvenir aux objectifs d'interopérabilité, de pérennité et de découplage des applications (cf. chapitre 3.1 Propriétés recherchées), le présent CCT préconise l'utilisation de normes et standards.

Les recommandations portant sur les normes et standards à respecter sont précisées dans la suite du document dans les chapitres :

- « § 4 - Applicatifs - page 42 »,
- « § 5 - Infrastructure - page 67»,
- « § 6 - Exploitation - page 94 »,
- « § 7 - Description des environnements - page 103 »,
- « § 8 -Cadre de développement - page 104 ».

3.7. RÉFÉRENTIELS GÉNÉRAUX : RGI, RGS, RGAA ET CHARTE ERGONOMIQUE DES SITES PUBLICS

3.7.1. Référentiels généraux

Les référentiels généraux fixent les obligations, recommandations et interdictions à respecter dans le cadre des échanges avec les autres administrations, collectivités territoriales et établissements publics à caractère administratif.

L'alignement au regard des contraintes du RGI (Référentiel Général d'Interopérabilité) présente un caractère obligatoire sur le plan réglementaire. Il s'applique aux administrations, collectivités territoriales et établissements publics à caractère administratif.

Le RGI est composé de trois volets : organisationnel, technique et sémantique.

CCT10	Il est OBLIGATOIRE de respecter les recommandations du RGI (cf. [A03]).

3.7.2. Ergonomie et accessibilité

Le Référentiel Général d'Accessibilité pour les Administrations (RGAA) possède des impacts structurants sur les applications et sur les choix technologiques de la partie IHM (Interface Homme-Machine).

La MOA doit définir suivant les besoins ou les contraintes, le niveau d'accessibilité attendu (A / AA / AAA).

Les locaux et les sites du ministère sont hétérogènes et certains sites historiques sont classés. L'organisation et l'installation des postes de travail et des imprimantes doivent prendre en compte ces contraintes. Cette situation engendre des difficultés au niveau de l'ergonomie du poste de travail.

Les principes du Référentiel Général d'Accessibilité pour les Administrations (RGAA) doivent être mis en œuvre : « Les responsables des sites veilleront tout particulièrement à favoriser l'accessibilité de l'information à tous les internautes, notamment les personnes handicapées, non voyantes, malvoyantes ou malentendantes. ».

CCT11	Il est OBLIGATOIRE, pour les applications publiées sur internet, de respecter les recommandations du RGAA (cf. [A07]) et de la charte ergonomique des sites publics (cf. [A08]). Il est nécessaire de définir le niveau d'accessibilité désiré dès la phase de cadrage du projet.

CCT12	Il est RECOMMANDÉ d'optimiser les applications pour une résolution d'affichage en 1024*768.

CCT13	Il est RECOMMANDÉ, pour les applications nationales, de respecter la charte graphique du Ministère. (cf. [A01])

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	**Version**	**Logiciel**	**Version**
Lecteur d'écran pour Windows	NVDA	2017.4+	Jaws Pro (Acces'Solutions)	18+
Logicel atténuation lumière bleue			f.lux	4.75
Terminal braille			Esytime	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

3.8. STRATÉGIE « DOUBLE SOURCE »

Les paragraphes suivants du CCT (4 Applicatifs et 5 Infrastructure, notamment) listent les produits à mettre en œuvre par typologie de besoin.

Les objectifs de rationalisation du SI peuvent, à première vue, mener à ne promouvoir qu'un seul produit par typologie de besoin, afin de garantir l'homogénéité et de la disponibilité des compétences internes au Ministère. Toutefois, cette solution a montré ces limites dans le passé, en particulier du fait de se retrouver pieds et main liés avec un seul fournisseur.

La solution inverse, « tout open-source », est trop dogmatique et ne peut répondre à tous les besoins du ministère. De plus, elle peut présenter des risques équivalents, certains produits open-source étant développés par une seule entreprise.

La mise en œuvre de **la stratégie « double source »** consiste à **proposer pour tout choix technologique une solution open source et une solution propriétaire** permettant de répondre aux **principes de non adhérence** et de **substitution** dans le **respect de la standardisation et de l'interopérabilité**.

Cette position, permet de mettre en avant les avantages habituels liés aux solutions open-source (interopérabilité, respect des normes et standards, ouverture du code source, faible coût) tout en pouvant s'affranchir de ses limites dans les cas de contraintes fortes.

Le choix entre ces 2 types de produits doit toutefois se faire en respectant la règle suivante :

CCT14	Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source dans le cadre du projet étudié.

3.9. ARCHITECTURE APPLICATIVE

Les paragraphes suivants présentent les grandes règles d'architecture applicative à appliquer.

3.9.1. Structuration des « applications » en couches

La structuration des applications en couches permet :

- de maîtriser la complexité des applications (développement, échanges entre les applications, interactions entre objets) ;
- d'améliorer le découplage de l'application (interface) ;
- d'optimiser les temps de développement, en factorisant certaines briques applicatives ;
- de favoriser la communication :
  - à l'intérieur d'une application, en structurant les échanges entre les différentes couches ;
  - entre les applications en précisant les principes de communication.

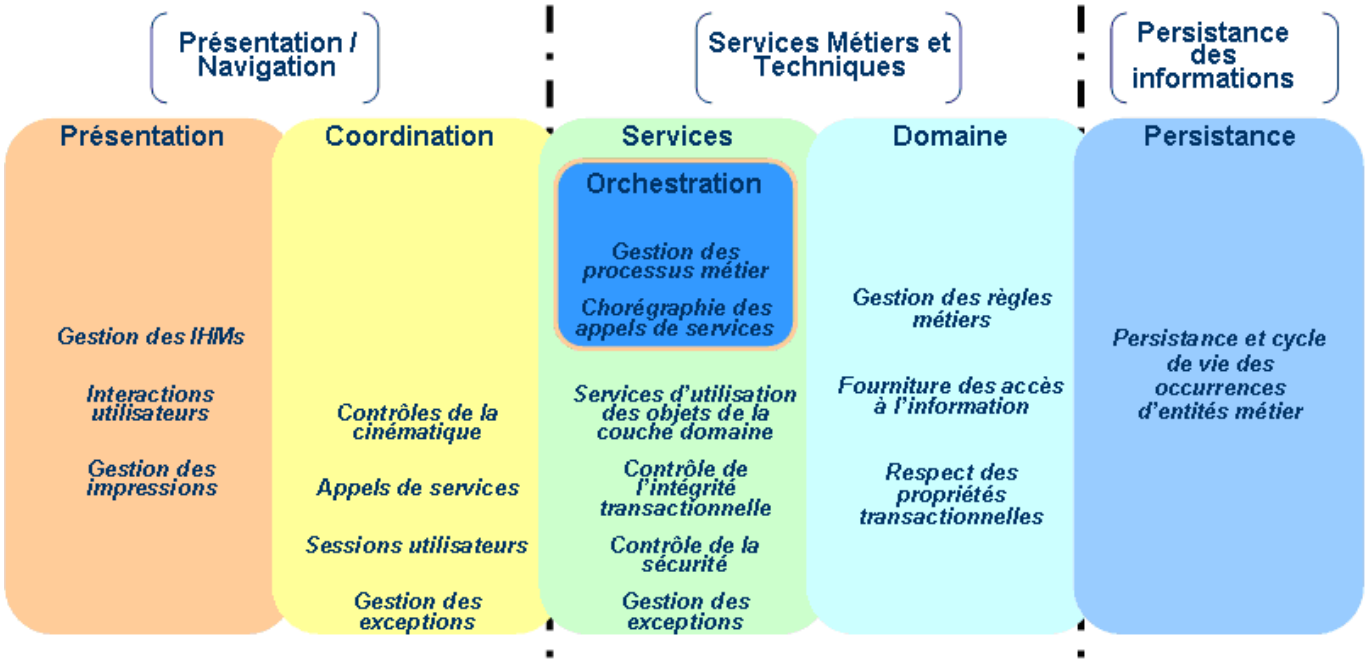

Illustration 6: Exemple de structuration des applications en cinq couches

La structuration en couches donne les règles d'implémentation de différents blocs de services lors de la conception d'une application. Les blocs de présentation sont réalisés avec les couches de présentation et de coordination, les blocs de services, qu'ils soient métiers ou référentiels, sont réalisés avec les couches service, domaine et persistance.

CCT15	Il est RECOMMANDÉ de structurer les applications en couches.

3.9.2. Technologies des applications

CCT16	Il est OBLIGATOIRE de se conformer au cadre de développement (cf. « §8 - Cadre de développement - page 104 »).

Banalisation de l'interface utilisateur

Afin de faciliter l'utilisation des applications sur le poste de travail, les technologies des applications doivent mettre en œuvre des IHM de types « client léger » et « client riche » RIA (Rich Internet Application) et respecter une charte graphique et ergonomique cohérente et homogène.

Client « léger » ou client « riche »

Ce type d'application client/serveur possède les caractéristiques suivantes :

- client « léger » ou client « riche »,
- serveur local ou distant,
- les données sont stockées sur un serveur local ou distant,
- l'application s'exécute pour sa partie serveur sur le serveur local ou distant, et pour sa partie cliente, celle-ci étant réduite à la **présentation via un navigateur** sur le poste de travail,

- les programmes sont stockés sur le serveur.
- Ce type de client facilite le déploiement des applications.

CCT17	Il est OBLIGATOIRE de mettre en œuvre des architectures client « léger » ou client « riche » basées sur l'utilisation d'un navigateur, aussi bien pour les applications à façon que basées sur des progiciels.

Application C/S « lourd »

Ce type d'application client/serveur possède les caractéristiques suivantes :

- un client lourd spécifique doit être déployé sur les postes de travail,
- des flux importants de données transitent entre le client et le serveur,
- le client a en charge la présentation et toute la logique de l'application,
- les données sont stockées sur le serveur, nécessairement local,

Ce type d'application pose d'importants problèmes de déploiement.

CCT18	Il est INTERDIT de développer de nouvelles applications en architecture client « lourd ».

CCT19	Il est RECOMMANDÉ d'utiliser CITRIX en phase transitoire en mettant en œuvre un client « lourd » déporté.

Les bases de données sont alors stockées sur des serveurs déportés ou centralisés, les traitements s'exécutent sur des serveurs déportés mixtes ou dédiés sous Microsoft Windows 2012 Server avec la couche XenApp de CITRIX.

Une attention particulière doit être porté sur le système d'éditique. Des tests, application par application, sont indispensables pour valider la faisabilité et les performances.

Local de type monoposte

Pour ce type d'application, l'application et les données se trouvent sur le poste de travail.

CCT20	Il est INTERDIT de développer de nouvelles applications en local de type monoposte.

3.10. SÉCURITÉ

Tous les éléments mentionnés dans ce paragraphe sont subordonnés au contenu de la Politique ministérielle de défense et de sécurité (PMDS) (cf. document référencé [A10]).

La mise en œuvre de la politique de sécurité du SI doit garantir un niveau minimal de sécurité des applications. Toutefois, la technique informatique ne représente qu'une partie des risques ou solutions liés aux problématiques de sécurité.

3.10.1. Cycle de vie des applications

Dès les premières phases du projet (création ou évolution), la MOA se doit de contacter le RSSI afin de prendre en compte les aspect sécurité de l'information. Le RSSI aide à constituer un dossier sécurité permettant de définir le niveau attendu. Quel que soit le niveau du dossier, une évaluation EBIOS (plus ou moins forte en fonction du niveau) a lieu. La MOA doit s'appuyer sur la matrice d'exigences de sécurité du ministère (cf. chapitre 8.7 Matrice d'expression de besoins Sécurité).

Pour plus de détail se référer au document [A10].

CCT21	Il est OBLIGATOIRE de constituer un dossier de sécurité pour tout projet (auquel un niveau de 1 à 3 sera attribué) conformément à ce qui est décrit dans la PMDS (cf. document [A10]).

Au cours du cycle de vie d'une application, les évolutions « métiers » plus ou moins contraignantes (évolution du besoin ou du cadre législatif) sont très souvent prioritaires sur les évolutions techniques. Or, seules ces dernières (en installant les dernières versions logicielles ou en appliquant les correctifs de sécurité) permettent de garantir un bon niveau de sécurité des applications.

CCT22	Il est OBLIGATOIRE pour toutes les applications centralisées de prévoir une mise à niveau du socle technique tous les 18 mois. Ainsi pour toute application, il est nécessaire de prévoir un plan de migration technique et le présenter au BAPT.

3.10.2. Gestion de l'identité numérique

Des services de gestion de l'identité numérique existent à ce jour dans le SI. Le Ministère possède sa propre Infrastructure de Gestion de Clés : IGC PEKIN.

3.10.3. Identification et authentification

Tout accès à un système d'exploitation, un réseau ou une application, doit être précédé d'une authentification. En fonction de la sensibilité des informations traitées, de la vulnérabilité du réseau utilisé, plusieurs niveaux d'authentification sont à envisager :

- **simple mot de passe** : pour être sécurisé, il doit être au minimum composé de 8 caractères et doit comporter au moins 1 minuscule, 1 majuscule, 1 chiffre et 1 caractère spécial. Ex : !tO-t014 ;

CCT23	Il est OBLIGATOIRE, dans le cadre de l'authentification par simple mot de passe, de respecter les règles présentées dans le document intitulé « Politique ministérielle de défense et de sécurité » (cf. document [A10]).

- **objet détenu par l'utilisateur** : token, calculette, clé USB, ... permettant l'élaboration à la volée du mot de passe qui ne sera plus rejouable. De même la fonctionnalité de « call back » sur les éléments de connexion à distance ;
- **carte à puce** : permet à la fois l'authentification forte et le chiffrement.

L'authentification au démarrage du poste (mot de passe au boot ou mot de passe setup) doit être systématique.

CCT24	Il est OBLIGATOIRE de faire reposer l'authentification des applications du Ministère sur le Web SSO ministériel.

CCT25	Il est OBLIGATOIRE, pour les applications non-Web ou celles qui seraient incompatibles avec le Web SSO, de faire reposer leur système d'authentification sur l'annuaire LDAP ministériel.

CCT26	Il est DÉCONSEILLÉ de dupliquer tout ou partie d'un annuaire ministériel (LDAP, AD) pour les besoins propres d'une application.

3.10.4. Habilitations et profils

Les habilitations aux applications peuvent se subdiviser en deux catégories :

- les habilitations de premier niveau (macroscopique) définissant le type d'accès à l'application (administrateur, gestionnaire ...)
- les habilitations fines (microscopique), définissant dans le détail les droits d'accès aux différents écrans.

CCT27	Il est OBLIGATOIRE de faire gérer les habilitations de premier niveau par l'annuaire LDAP ministériel.

CCT28	Il est OBLIGATOIRE de faire gérer les habilitations fines par les applications.

Remarque :

Pour en savoir plus sur les habilitations de premier niveau (macroscopiques), se référer au document [R04].

3.10.5. Architecture réseau multi zones

Les applications installées dans un centre de production doivent se conformer à un découpage du réseau en zones visant à garantir la sécurité.

Ces zones en termes de sécurité sont organisées de la façon suivante :

- zone d'accès,
- zone présentation,
- zone applicative.

Ces zones, séparées par des firewalls permettent de sécuriser les données, situées dans la zone la plus sûre.

Il est à noter que les applications internet et intranet sont séparés physiquement en terme d'hébergement. Ainsi les zones de sécurité sont dupliquées pour les sites intranet et internet.

CCT29	Il est OBLIGATOIRE de placer toute application contenant des données sensibles dans une zone réseau sécurisée.

3.10.6. Sécurisation RPVJ

La sécurisation du RPVJ passe par :

- le cloisonnement vertical du RPVJ par des VPN par classe d'utilisation
- le cloisonnement horizontal du RPVJ des réseaux locaux géographiques ou hiérarchiques

Ces deux types de cloisonnement sont en cours de mise en place par des pare-feux.

Afin d'en améliorer la sécurité, d'autres évolutions du RPVJ sont envisagées dans le futur, en particulier, l'adoption d'une structure plus hiérarchique.

CCT30	Il est RECOMMANDÉ de concevoir les applications décentralisées de manière à minimiser les flux directs inter-site (privilégier le passage via la PFE cf. ci-dessous).

Ainsi, les échanges de données entre 2 instances d'applications décentralisées doivent privilégier le passage par un serveur intermédiaire (Plateforme d'échange, cf. chapitre 5.3.4 Plateformes d'échanges) plutôt qu'un échange direct.

3.10.7. Confidentialité / Chiffrement

Postes de travail

La protection des postes de travail par mot de passe (au démarrage et en cas de non-activité prolongée) permet d'assurer un premier niveau de confidentialité du système d'information Justice.

Pour des besoins plus impérieux, des moyens de chiffrement sont requis. La réglementation étant aujourd'hui restrictive, il convient de prendre contact avec le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI).

3.10.8. Mobilité (nomadisme et télétravail)

Postes de travail (PC portables)

CCT31	Il est RECOMMANDÉ de chiffrer les données de tous les postes de travail nomades (PC portable).

CCT32	Il est OBLIGATOIRE de brancher régulièrement les postes de travail nomades sur le RPVJ pour procéder aux mises à jour de sécurité.

Lors d'une connexion filaire au RPVJ, toutes les autres interfaces réseau doivent être désactivées (WiFi, 3G, …)

CCT33	Il est OBLIGATOIRE que la configuration réseau du pc portable interdise toute connexion à internet en dehors de la solution de VPN mise en oeuvre par le Ministère.

On pourra se référer à la PMDS pour plus de précisions (cf. document référencé [A10]). En particulier, on lira dans ce document la procédure d'exploitation de la sécurité (PES) pour l'ensemble des moyens liés à la mobilité intégrés aux systèmes d'information du ministère de la Justice.

3.11. MATRICE DE CLASSES D'APPLICATIONS

Les applications doivent pouvoir être catégorisées en fonction notamment de :

- la sensibilité des informations manipulées ;
- la qualité de service et la disponibilité requise ;
- le nombre d'utilisateurs ;
- le volume d'informations gérées (bande passante réseau, espace de stockage) ;
- le nombre d'interfaces;
- le public concerné;

En fonction de ces critères, on peut, par exemple et en première approche, classer les applications en quatre catégories :

1. les applications grand public publiées sur internet
2. applications destinées à un grand nombre d'utilisateurs, devant être sécurisées sans nécessiter de transferts d'information importants : ces applications pourraient être prévues en exploitation centralisée.
3. applications susceptibles de générer des échanges massifs de volumes de données, ces applications pourraient être prévues en exploitation déconcentrée afin de limiter les échanges réseau. L'exploitation doit alors impérativement pouvoir se faire en télé-administration.
4. applications bureautiques, ces applications doivent alors pouvoir être mises en œuvre en mode LAMP/WAMP pour exploitation locale.

Le SSIC pourrait, dans un futur proche, proposer, pour chacune de ces classes d'application, une architecture applicative et technique générique qui puisse être utilisée lors d'un nouveau projet ou lors de la refonte d'un projet.

En termes de sûreté de fonctionnement, les différentes alternatives sont présentées dans le paragraphe suivant.

3.12. SÛRETÉ DE FONCTIONNEMENT

L'objectif de ce chapitre est de présenter les différentes caractéristiques relatives à la sûreté de fonctionnement des applications.

3.12.1. Stratégie « double cœur »

La stratégie « double cœur » permet d'offrir aux applications une offre de service et des mécanismes permettant la reprise informatique et la continuité informatique.

Ce mode d'exploitation est décliné :

- en secours réciproque avec reprise (quasi-)instantanée en cas de perte d'un site pour les applications nécessitant une haute disponibilité ;
- en mode actif/passif pour les autres.

CCT34	Il est RECOMMANDÉ que les applications disposant d'une architecture et d'une exploitation centralisées soient : • exploitables en « double cœur » ou • progressivement adaptées afin de pouvoir être exploitées en « double cœur ».

3.12.2. Plan de Reprise Informatique (PRI) / Plan de Continuité Informatique (PCI)

La mise en place d'un Plan de Reprise Informatique / Plan de Continuité Informatique permet de garantir la continuité de service en cas d'incident majeur sur ses sites de production nationaux et sur ses sites déconcentrés.

La mise en place d'un PCI/PRI peut se faire de diverses manières avec différents niveaux de sécurité.

C'est une solution coûteuse qui doit correspondre à un compromis entre :

- les besoins de la MOA en termes de **durée maximale d'interruption admissible** (DMIA ou RTO) et de **perte de données maximale admissible** (PDMA ou RPO),
- les limites techniques et les coûts de mise en œuvre (technique et humain)

CCT35	Il est OBLIGATOIRE de prendre en compte la nécessité d'un PRI/PCI dès la phase de conception des applications critiques.

3.12.3. Qualité de service

Disponibilité

La nécessité de **haute disponibilité** en 24 heures sur 24, 7 jours sur 7 ou de plages de disponibilité étendues, pour certaines applications, présente des impacts organisationnels et technologiques. **Ce besoin est issu de l'expression de besoins métiers.**

Le niveau de disponibilité possède notamment des impacts sur :

- l'architecture applicative,
- l'infrastructure réseau,
- l'infrastructure des bâtiments,
- l'organisation.

CCT36	Il est OBLIGATOIRE de traiter la problématique de disponibilité de l'application **dès les phases d'architecture et de conception de l'application.** Ces phases permettent d'identifier les points de faiblesse (« SPOF : Single Point Of Failure ») et les points de contention (« SPOC : Single Point of Contention ») qu'il faut sécuriser.

CCT37	Il est OBLIGATOIRE de faire participer **les équipes de production** à ces phases afin d'avoir le temps de préparer et d'apporter la solution adéquate.

La disponibilité de la chaîne est dépendante de celle du maillon le plus faible. Il est primordial de formaliser pour les applications le niveau de criticité des différentes fonctionnalités.

Il est à noter que le coût total de mise en œuvre et d'exploitation d'une infrastructure haute-disponibilité est exponentiel, plus on s'approche d'une disponibilité de 100 %.

Les fonctionnalités les moins critiques pourront alors faire l'objet de mesures organisationnelles particulières, afin de limiter l'impact budgétaire.

Répartition de charge

La répartition de charge permet :

- d'augmenter la capacité de traitement en dupliquant les équipements (mise en place de « ferme » de serveurs par exemple), cf. chapitre 3.12.4 Gestion de l'extensibilité (« scalability »)
- d'augmenter la disponibilité en cas de défaillance d'un des éléments de la ferme.

La réparation de charge peut se faire de façon logicielle ou matérielle.

Les notions clés liées à la répartition de charge sont :

- l'affinité de session : elle permet à un utilisateur d'être de préférence redirigé vers le même serveur de la ferme (indispensable lorsque les services déployés sur les serveurs sont sans état ou « stateless »)
- le partage de cache (cluster) : en cas de défaillance d'un des éléments de la ferme, le partage de cache permet aux autres éléments de continuer la requête de façon transparente pour l'utilisateur. Sans partage de cache, la requête en cours est perdue et l'utilisateur doit la soumettre de nouveau.

CCT38	Il est RECOMMANDÉ de mettre en œuvre une répartition de charge pour les applications critiques.

Tolérance aux pannes

Afin de garantir une bonne tolérance aux pannes, deux solutions sont envisageables :

- les architectures actif-passif : on parle alors de reprise d'activité ou « fail-over ». En cas de défaillance, le serveur passif peut prendre le relais du serveur actif. Cela nécessite la plupart du temps une intervention technique et occasionne donc une petite indisponibilité,
- les architectures actif-actif : on parle alors de partage de charge

CCT39	Il est RECOMMANDÉ de mettre en œuvre l'actif-actif sur les machines d'un même centre de production.

Il est nécessaire de dimensionner l'architecture de manière adéquate afin de ne pas surdimensionner l'architecture en fonction du besoin. Par exemple, si la criticité de l'application et le nombre d'utilisateur simultanée sont très faibles, il n'est pas envisageable de concevoir une application haute disponibilité en mode actif-actif si l'on peut se contenter de fonctionnalité HA Vmware pour les applications hébergées sur des machines virtuelles (au détriment d'une petite indisponibilité).

CCT40	Il est DÉCONSEILLÉ de mettre en œuvre l'actif-actif sur deux sites distants s'il doit exister des interactions applicatives/fonctionnelles entre les deux nœuds actifs.

3.12.4. Gestion de l'extensibilité (« scalability »)

Afin d'assurer une conservation de la qualité de service en cas d'augmentation imprévue du nombre d'utilisateurs, l'architecture d'une application doit être extensible.

Deux types d'extensibilité sont envisageables :

- extensibilité « verticale » : ajout de ressources à un serveur (mémoire, CPU, stockage, carte réseau).
- extensibilité « horizontale » : ajout d'un autre serveur qui vient en partage de charge d'un serveur saturé.

CCT41	Il est OBLIGATOIRE de concevoir les applications métiers permettant une extensibilité horizontale.

4. APPLICATIFS

Ce chapitre :

- définit les briques logicielles pour le poste de travail et les différents types de serveurs (socle applicatif),
- définit les règles relatives à l'utilisation des services applicatifs transverses.

Pour les aspects relatifs aux couches de plus bas niveau (système d'exploitation), on se référera au chapitre 5 Infrastructure

4.1. SOCLES DES APPLICATIONS

La portabilité des applications et des données, l'interopérabilité de ces applications entre elles et avec les applications externes au ministère de la Justice, seront d'autant plus facilitées qu'elles seront développées ou acquises en prenant en considération les recommandations en matière :

- de système d'exploitation et matériel associés,
- de logiciel de base de données,
- de logiciel de développement,
- de sécurité des accès et des données.

4.1.1. Poste de travail

Description

Les **postes de travail** sont des PC connectés à un réseau local, sur lesquels se trouvent un certain nombre d'applications, d'outils bureautiques et d'outils de communication activés de façon unifiée par les utilisateurs via un environnement de type bureau. Ces applications et ces outils accèdent à des données locales ou distantes, personnelles ou partagées. Une fois que l'utilisateur a été identifié et authentifié, le bureau lui restitue son environnement de travail.

En pratique, on distingue deux grands types de configuration de poste :

- les **postes standards (multifonctions)** qui accueillent les suites bureautiques, les applications métiers autorisées, les services de communication (messagerie, intranet, ….) ;
- les **postes dédiés** à un outil ou une fonction particulière technique (ex administration, configuration, réseau,...) ou métier (comptabilité, …). Ce type de poste peut être mis en œuvre dans un contexte où la sécurité joue un rôle primordial (station de décontamination antivirale, accès restreint en zone publique ou pédagogique…).

CCT42	Il est OBLIGATOIRE de banaliser les postes de travail.

CCT43	Il est OBLIGATOIRE d'intégrer les postes de travail dans l'Active Directory national.

Ces configurations se combinent avec deux types de raccordement au réseau:

- les **postes connectés** en permanence au réseau local (et au-delà, au réseau national),
- les **postes nomades**, fonctionnant soit en mode autonome, soit connectés au réseau local via une station d'accueil au sein d'un site justice, soit connectés au RPVJ via un modem.

Toutefois, on peut signaler qu'à titre transitoire (en attente de la fin du câblage du site), ou dans certaines circonstances particulières où la sécurité joue un rôle capital (décontamination par exemple) quelques postes de travail, en nombre résiduel, peuvent être fixes et physiquement isolés du réseau local.

CCT44	Il est INTERDIT de partager des fichiers et des ressources entre postes de travail.

CCT45	Il est OBLIGATOIRE de stocker les fichiers dans un SLR ou dans une GED.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	**Version**	**Logiciel**	**Version**
Bureautique	LibreOffice.org Writer	5.x	Microsoft Office Word	
	LibreOffice.org Calc	5.x	Microsoft Office Excel	
	LibreOffice.org Pres	5.x	Microsoft Powerpoint	
Navigateur[1]	Mozilla Firefox	ESR 31 à ESR 52	Microsoft Internet Explorer, Edge	8 à 11
Client de messagerie	Thunderbird		Microsoft Outlook	2010
Outil de compression	7Zip	16.x	Winrar	5.5
Visualiseur PDF			Acrobat Reader	11.x ou plus
Annotations PDF	——		Acrobat Reader, PDF Xchange Viewer	11.x ou plus 2.5.20.10
Imprimante pdf	PdfCreator	2.3.1.x	Microsoft Print to PDF	Inclus dans Win10
Fractionner et fusionner des fichiers PDF	PDFSam basic	3.30.5.x		
Antivirus	—		Projet PRIAM TrendMicro OfficeScan	 10.5 (win7) 11.0.6496 (win10)
Client « thin-client »	—		CITRIX	4.1
Lecteur Multimédia	VLC	2.1 ou plus	Windows Media Player	12.x
Transfert FTP	FileZilla	3.31.x		
Gestion des mots de passe	Keepass	2.38 +		

1 Les applications intranet du ministère de la Justice doivent obligatoirement être compatibles avec les navigateurs Firefox, Internet Explorer et Edge. Les applications extranet/internet doivent en sus être compatibles avec les navigateurs Chrome et Safari.

Cartographie mentale	Freemind Freeplane	1.0.1 1.6	Xmind Pro	8
Diagramme de gantt	GanttProject	2.8.x		
Dictée vocale			Dragon Naturally Speaking (De nuance)	13
Traitement postscript & PDF	GhostScript	9.22		
Chiffrement anti-vol de poste			Cryhod (primX)	3.0.1572
Chiffrement de conteneur			Zed!(primX)	6.1.2208
Chiffrement de données			Zonecentral (primX)	6.x

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / points complémentaires

Client de messagerie

Les échanges entre le client de messagerie Outlook configuré en mode « Exchange Server » et le serveur de messagerie s'exécutent dans le protocole RPC encapsulé HTTPS. Dans le cadre d'un accès distant, si le client n'est pas compatible avec le mode RPC encapsulé, le recours à Outlook Web Access (fonctionnalité équivalente, mais via le protocole HTTPS) est nécessaire.

CCT46	Il est OBLIGATOIRE de configurer le client Outlook en mode RPC encapsulé à chaque fois que cela est possible.

Suite bureautique et format d'échange pour les pièces jointes

Lors d'échange de textes, de tableaux ou de présentations, notamment par la messagerie interpersonnelle, pour des raisons d'interopérabilité, l'émetteur devra transmettre des documents aux formats (au choix):

- PDF (Adobe) (pas de modification ultérieure de son contenu hors utilisation d'outils spécifiques, garantie de conservation de la mise en page initiale)
- ODF (Open Document Format) pour récupération dans un traitement de texte, tableur ou outil de présentation.

CCT47	Il est OBLIGATOIRE pour les outils de bureautique de mettre en œuvre le format pivot standard et ouvert Open Document Format (ISO/IEC 26300) permettant : • de supprimer l'adhérence vis-à-vis d'un choix d'outil de bureautique, • de s'aligner sur les préconisations et recommandations du RGI.

Compression/décompression

CCT48	Il est RECOMMANDÉ d'utiliser le format de compression/décompression ZIP pour échanger des données entre utilisateurs.

Antivirus

Pour des raisons de sécurité, certains types de pièce jointe sont proscrits et filtrés sur les serveurs de messagerie.

Sécurisation du poste de travail

Le poste de travail doit garantir la sécurité de l'accès aux applications et s'appuyer sur des services de sécurité mutualisés : carte à puce, SSO, authentification, habilitation, chiffrement, signature.

Le poste de travail doit permettre différents niveaux de sécurité en fonction du contexte d'utilisation :

- authentification faible : simple mot de passe ;
- authentification forte : en utilisant un objet détenu par l'utilisateur : token, calculette, clé USB, etc. ;
- confidentialité avec signature et chiffrement : utilisation d'une carte à puce.

Non adhérence des applications avec le poste de travail

Les applications doivent être indépendantes des infrastructures « poste de travail » et ne doivent pas avoir d'adhérence avec des composants logiciels ou matériels du poste de travail. Les applications doivent être accessibles à partir de n'importe quel navigateur Web sans déploiement de composant au préalable (ActiveX, Suite bureautique, etc.).

CCT49	Il est INTERDIT de développer ou de mettre en œuvre des applications web faisant appel : • à un module ActiveX du navigateur, • à un applet Java dans le navigateur, • à un module silverlight dans le navigateur. • à un plugin Flash player

Fin du support Flash :

Adobe déclare ***arrêter la mise à jour et la distribution*** *de son plugin Flash Player à la* ***fin de l'année 2020*** *et encourage les créateurs de contenus à migrer tout contenu Flash existant vers de nouveaux formats ouverts.*

Microsoft déclare mettre à jour son navigateur Edge vers la fin de l'année 2018 pour exiger des autorisations d'exécution de Flash pour chaque session. En 2019, Flash sera désactivé par défaut dans Microsoft Edge et Internet Explorer. Les utilisateurs qui le souhaitent pourront les réactiver manuellement dans chaque navigateur. Et **à la fin de l'année 2020, il ne sera plus possible d'exécuter Flash sur toutes les versions de Microsoft Edge et Internet Explorer.**

Mozilla déclare que Flash sera désactivé par défaut pour la plupart des utilisateurs en 2019, et seuls les utilisateurs exécutant la version de support étendu (ESR) de Firefox pourront continuer à utiliser Flash **jusqu'à l'arrêt complet en fin d'année 2020.**

CCT50	Il est RECOMMANDÉ aux projets existant utilisant des fonctionnalités liées au plugin Flash de prévoir un plan de migration technique dès à présent afin de prendre en compte la fin du support de ce plugin.

Fin des applets java et du support de son plugin au sein des navigateurs

Fin 2015, de nombreux fournisseurs de navigateur ont mis un terme à la prise en charge de plug-in reposant sur des normes ou ont annoncé des dates pour la fin de cette prise en charge, ce qui empêche d'imbriquer Silverlight, Java, Flash et d'autres technologies de plug-in reposant sur des normes.

En conséquence, Oracle a fait passer en phase d'abandon (deprecated) le plug-in de navigateur Java dans le kit de développement Java Standard Edition 9 (JDK 9). La phase d'abandon est un avertissement pour que les développeurs cessent d'utiliser cette technologie. JRE 9 continuera à fournir le plug-in Java et à prendre en charge les applets de lancement **sur les navigateurs proposant encore une prise en charge du plug-in standard**, **mais est disponible uniquement pour une utilisation limitée et n'est pas recommandé.** Le plug-in de navigateur sera enlevé d'Oracle JDK et JRE dans une version ultérieure de Java SE.

Plugin java dans **Firefox** :

Chez Mozilla-Firefox, le plugin java s'appuit sur NPAPI (Netscape Plugin Application Programming Interface). **Fin 2016,** Mozilla **met un terme au support des plugins Java**, Silverlight et consorts au sein de son navigateur. **La dernière version de Firefox qui permettra l'usage d'applet Java sera la version 52 ESR** (la **dernière mise à jour** de la 52ESR est prévu **fin mai 2018**). A partir de Firefox 53, il n'y a plus de prise en charge du NPAPI et donc plus de possibilité de faire fonctionner les applets java.

Plugin java dans **Internet Explorer** :

A partir de janvier 2017, seul IE11 est encore supporté par Microsoft.

Microsoft Edge (windows 10) ne prend pas en charge NPAPI, il n'y a donc pas de possibilité d'exécuter un applet java dans ce navigateur.

Plugin java dans **Chrome** :

Plus de possibilité depuis 2015.

En conséquence :

CCT51	Il est RECOMMANDÉ aux projets existant utilisant des applets Java de prévoir un plan de migration technique dès à présent afin de prendre en compte la fin du support de ce plugin.

Dans la mesure du possible, il faut éviter l'usage de machine virtuelle, mais surtout à minima éviter l'adhérence des applications Web avec une version spécifique de JVM en qualifiant l'utilisation d'une seule version de JVM sur le poste client.

CCT52	Pour des raisons de sécurité, il est INTERDIT d'utiliser des Applets Java dans le navigateur.

CCT53	Il est DÉCONSEILLÉ aux applications Java s'exécutant sur le poste de travail d'avoir une adhérence vis-à-vis d'une version de JRE.

CCT54	Il est INTERDIT, pour les applications métiers, d'avoir une adhérence directe avec les applications bureautiques et collaboratives. Les API des applications bureautiques et collaboratives déployées sur les postes de travail ne doivent pas être utilisées.

OpenJDK et changement de stratégie commerciale d'Oracle atour de Java

Depuis janvier 2019, Java (Oracle JDK/JRE) devient Payant.

Le cycle de release de Java a également changé, il y a dorénavant une version LTS (Long Term Support) tous les 3 ans et une version majeure tous les 6 mois (en Mars et en Septembre).

Les versions Oracle Java LTS sont payantes à partir de la 11 (parue en septembre 2018). Par contre, il est possible d'utiliser gratuitement Oracle Java 8 au delà de janvier 2019, **mais sans aucun support d'Oracle**.

Toutefois, Redhat assure le support des versions LTS d'OpenJDK sur ses serveurs RHEL.

OpenJDK est l'alternative open source de l'oracle JDK, maintenue par Oracle et constitue la version «communautaire» de Java.

OpenJDK est disponible sous licence GPL avec la « Classpath Exception » qui en permet une utilisation commerciale sans obligation de publier les sources.

La communauté java AdoptOpenJDK propose des builds à partir des sources d'OpenJDK (depuis la version Java 8) pour plusieurs plateformes (dont Windows10). Elle est sponsorisée par IBM, Microsoft Azure, Azul.

En conséquence, les préconisations au Ministère sont :

Coté serveur, il faut utiliser OpenJDK 11. La distribution à installer est celle fournie par RedHat qui en assure le support sur ses serveurs RHEL dans le cadre contractuel déjà existant au Ministère.

Coté poste de travail, et vu l'absence de JavaFX dans Java 11 et les dépendances vers des applications bureautiques existantes non encore qualifiées sur Java 11, il faut utiliser au moins la version OpenJDK8.

Exception : coté poste de travail, pour les applications nécessitant les technologies « obsolètes » que sont les Applets et JavaWebStart, il est prévu d'utiliser OracleJDK 8.

NB : Dans la version 11 de Java (OpenJDK ou Oracle Java), certaines technologies ont été supprimées: Applets, JavaWebStart, JavaFX, JAX-WS, JAXB, JAF, JTA, CORBA.

4.1.2. Développement spécifique d'applications

Ce chapitre s'applique aux logiciel « à façon » développés pour les besoins spécifiques du Ministère.

CCT55	Il est OBLIGATOIRE de développer les applications **cœur de métiers ou d'envergure nationale** en technologie Java EE.

CCT56	Il est OBLIGATOIRE de développer les applications **non cœur de métiers ou d'envergure locale** en technologies Java EE et à défaut en PHP (LAMP ou WAMP).

Pour plus de détails, on se référera au chapitre 8 - Cadre de développement - page 104 .

Produits / composants

Solution	Open source		Propriétaire[1]	
	Logiciel	Version	Logiciel	Version
Langages	Java[2]	11		
	PHP	7.2.x +		
Couches présentation / coordination	JSF : myfaces et primefaces	2.2 et +		
	Angular	7		
Couche services	Apache CXF (JAXRS)	3.2.x		
Couche persistance	Hibernate JPA	5.3.x +		
	mybatis	3.4.x		
	JDBC	4.x		
IoC / AOP	CDI	version JEE la plus récente		
Logs	SLF4J	1.7.x		
Sécurité	JAAS	Intégré au JRE		
Transaction	JTA	version JEE la plus récente		
XML	JAXB	version JEE la plus récente		
Librairies	Apache Jakarta commons			
	PEAR (PHP)			
Moteurs de règles			Red Hat JBoss BRMS	6.4.0
Ordonnanceur	Quartz	2.3.x		
Scripting shell	Bash			
Javascript	JQuery	3.x		
CSS Dynamique	Less	3.9.x		
	Sass			
Optimisation des ressources	Technique Css Sprite			
Micro services	Spring boot	2.x		
Alternative Java à la pile Java EE[3]	Spring framework	4.3.x (java 8) 5.x		

1 *cf. CCT14* - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.
2 Les nouvelles applications ayants une dépendance Java sur le poste client doivent être qualifiées sur les versions 8 ou 11.
3 Toute nouvelle application doit prioritairement être développée selon la spécification Java EE la plus récente. Toute dérogation à cette règle devra faire l'objet d'une justification.

Solution	Open source		Propriétaire	
	Logiciel	Version	Logiciel	Version
Alternative PHP à la pile Java EE	Symfony	Symfony 3.4 : fin du support 2020 et 2021 pour les security fixes Fin du support pour la version 3.3 en juillet 2018		
Migration de base de données	Flyway	5.2.x+		
	Liquibase	3.6.x		
Mapping d'objets Java	MapStruct	1.x +		
Sécurisation des mots de passe	JBoss Vault	Intégré à JBoss EAP		
	Tomcat Vault	1.1.7+ (compatibilité Tomcat 9 +)		
	Spring Vault			

4.1.3. Serveurs de présentation (Web ou CITRIX)

Description

Les serveurs de présentation sont utilisés pour gérer l'interface entre le poste de travail et les serveurs d'application, qui traitent la logique métier. Les serveurs de présentation, eux prennent uniquement en charge l'affichage de l'interface graphique. A ce titre, ils permettent :

- d'améliorer les performances grâce aux mécanismes de mise en cache des contenus statiques
- d'améliorer la sécurité en évitant les accès directs du RPVJ sur les serveurs applicatifs ou de données.

Citrix permet d'exécuter un client lourd à proximité du serveur et déporte l'affichage vers l'utilisateur.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Serveur Web	Apache Web Server HTTP	2.4.x		
Déport d'affichage			CITRIX XenApp	7.5 LTSR

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / points complémentaires

CCT57	Il est RECOMMANDÉ d'utiliser le système d'exploitation Linux avec le serveur Web Apache.

CCT58	Il est OBLIGATOIRE de concevoir les applications web pour qu'elles fonctionnent sans couche Citrix en utilisant un débit réseau raisonnable.

CCT59	Il est OBLIGATOIRE de réaliser une étude poussée (analyse de la bande passante, système d'impression, compatibilité citrix, consommation de ressources système) sur l'application destinée à être « CITRIXifiée ».

CCT60	Il est RECOMMANDÉ d'utiliser Citrix, dans le cas des applications client lourd, lorsque : • on souhaite s'appuyer sur le service de transport de données offert par le RPVJ (ce type d'architecture est nettement plus économe en termes de ressources réseau que les applications client-serveurs classiques) ; • on souhaite limiter les efforts de déploiement sur les postes clients.

4.1.4. Serveurs d'applications

Description

Un serveur d'applications est un serveur sur lequel sont installées des applications et/ou des services (Java EE ou PHP). Ces applications et services sont exécutés sur le serveur d'applications, les clients y accèdent à distance par le RPVJ via l'utilisation d'un « client léger » ou d'un « client riche », la plus souvent par l'intermédiaire d'un serveur de présentation.

Les serveurs locaux de ressources et les serveurs d'applications ont des rôles distincts. Ils ont des contraintes de performance, de disponibilité, d'exploitation, d'évolutivité et de sécurité différentes. Il est donc délicat de configurer un serveur pour qu'il soit à la fois serveur d'application et serveur local de ressources.

CCT61	Il est DÉCONSEILLÉ d'utiliser une même machine à la fois comme serveur local de ressources et comme serveur d'applications.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Serveur d'applications Java EE			RedHat Jboss EAP	7.1.x
Conteneur Web Java	Apache Tomcat	9.x+	—	
« Serveur d'applications » PHP	module PHP du serveur web apache. (**)	Apache 2.4.x PHP 7.1	—	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

(**) : les offres packagées de type lamp, wamp, xamp ou easyphp ne doivent être utilisées que sur les environnements de développement.

Remarques / points complémentaires

CCT62	Il est RECOMMANDÉ d'utiliser Tomcat si l'application n'utilise pas de conteneur d'EJB .

4.1.5. Serveurs de base de données

Description

Les serveurs de données hébergent des bases relatives à des applications nationales ou celles de portée départementale.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
SGBDR	PostgreSQL	9.x	Oracle	12.1 +

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / points complémentaires

Conformité SQL :

CCT63	Il est OBLIGATOIRE d'être conforme à SQL (Structured Query Language) dans le cadre d'une SGBDR. A minima la norme SQL-92 doit être respectée, au mieux la norme SQL :2011 doit être suivie (Oracle comme PostGreSQL ne respecte pas en totalité cette dernière).

Utilisation de database link prohibé :

Dans un système de gestion de base de données (SGBD), un database link (Dblink) est un objet d'une base de données permettant d'exécuter des requêtes sur une autre base de données, qu'elle se trouve physiquement sur la même machine ou qu'elle soit distante. **Cette pratique est strictement interdite au sein du SI Justice**

CCT64	Il est INTERDIT d'utiliser un système de type Dblink (database link) au sein d'une SGBDR.

Non utilisation de Trigger :

Par le biais des Triggers, il peut être tentant de mettre à jour des informations dépendant d'autres informations au sein d'un schéma ; Déportant ainsi une partie de la logique métier de l'application directement dans la base de données, plutôt que du côté applicatif. **Cette pratique est strictement interdite au sein du SI Justice.** Ainsi l'utilisation des triggers est soumise à conditions, explicitement autorisées par le Ministère.

CCT65	Il est INTERDIT d'utiliser des Triggers au sein d'une SGBDR **sauf** contrainte majeure et **sous autorisation écrite du Ministère. Au préalable le projet devra soumettre à validation cette utilisation et fournir sa justification.**

Non utilisation de Procédure Stockée :

CCT66	Il est INTERDIT d'utiliser des procédures stockées au sein d'une SGBDR **sauf** contrainte majeure et **sous autorisation écrite du Ministère. Au préalable le projet devra soumettre à validation cette utilisation et fournir sa justification.**

4.1.6. Progiciels

Description

Pour certains besoins spécifiques, le ministère de la Justice à recours à des progiciels du marché.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Gestion des ressources humaines			SAP Netweaver + noyau SIRH interministériel	
Gestion des emplois du temps			Chronogestor (projet ORIGINE) Editeur GFI Chrono Time	3.3
Gestion des concours			ATPlus® (projet CONCOURS) Editeur escort informatique	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

4.2. SERVICES APPLICATIFS

Description

Ce chapitre présente les services applicatifs mutualisés pouvant être mis en œuvre sur l'ensemble des projets du ministère de la Justice.

Sur le plan d'occupation des sols de la cartographie du système d'information du Ministère, ces services applicatifs transverses figurent à la périphérie. Ce sont des services sur lesquels les différentes applications métier peuvent s'appuyer.

4.2.1. Services référentiels et nomenclatures

Le système de référence de Justice (SRJ) est constitué de tables de références regroupées au sein de cinq grands domaines (natures d'infraction, peines et mesures, éléments de structure, tables élémentaires, événements).

Le SRJ alimente aujourd'hui les principales applications du Ministère :

- la chaîne pénale (Cassiopée),
- le système d'information des ressources humaines (H@rmonie),
- le système pénitentiaire (GENESIS),
- le pilotage des services judiciaires (Pharos),
- le casier judiciaire national,
- ...

4.2.2. Annuaire ministériel

Description

Le ministère de la Justice a fait le choix du produit libre « 389 Directory Server » comme infrastructure nationale de serveurs d'annuaire sur les sites de production. Il contient des données consolidées des applications Ressources Humaines et de l'Active Directory. Les applications s'appuient sur le LDAP pour gérer l'authentification et les profils applicatifs.

Les serveurs de fichiers utilisent plutôt l'annuaire Active Directory.

Cf. « § 5.3.3 - Annuaires de ressources - page 83 ».

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Annuaire ministériel	389 Directory Server	1.3.x	Active Directory	2008R2/2012
Alimentation des annuaires			Meibo Provisionning	
Gestion de contenu des annuaires			Meibo Publisher	

4.2.3. Messagerie et travail collaboratif

Description

Ces outils regroupent l'ensemble des logiciels permettant l'utilisation des NTIC pour faciliter le travail collaboratif au sein du Ministère.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Messagerie			Microsoft Exchange	2010
Messagerie instantanée				
Portail collaboratif	Drupal	8.x		
Gestion de cache	Varnish, Memcache	5.x, 1.5.x		
Wiki	MediaWiki dokuWiki	1.30.x Release 2017-02-19e		
Forum	phpBB	3.x+		
Liste de diffusion ou de discussion	Sympa	6.0.1		
Blog	Drupal	8.x		
Serveurs de documents	Alfresco	5.0.x	Alfresco Enterprise	5.0.x
Visioconférence				
Sondage	LimeSurvey		Sphinx	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Pile CMS préconisée : Drupal, Apache, Varnish, Memcache, Elasticsearch, PostgreSQL

Service national de messagerie électronique

CCT67	Il est INTERDIT de mettre en place les messageries Lotus Notes et GroupWise. La mise en œuvre de systèmes locaux de messagerie, souvent associés à des fonctionnalités de type « travail collaboratif », les contraintes d'administration et d'exploitation (lié à l'interconnexion transparente avec le service national de messagerie) imposent, pour des raisons liées aux ressources humaines disponibles, de ne retenir qu'un seul système homogène avec le niveau national.

Remarques / points complémentaires

Microsoft Exchange

La plateforme de messagerie est hébergée en centre de production.

Les pré-requis de normes de déclarations de BALs ou liste de diffusion sont accessibles à l'url suivante :

http://intranet.justice.gouv.fr/rpvj/ (rubrique Documentation → Documentation par domaine)

Visioconférence

Les outils de visioconférence font partie des applications de travail en groupe.

CCT68	Il est RECOMMANDÉ de mettre en œuvre la visioconférence sur IP

CCT69	Il est OBLIGATOIRE d'utiliser les normes H320 (RNIS) ou H323 (IP) pour la mise en œuvre de la visioconférence.

4.2.4. Agenda partagé

Description

Il permet aux agents de publier leur agenda, ce qui facilite en particulier la planification des réunions.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Client agenda partagé			Microsoft Outlook	2010
Serveur agenda partagé			Microsoft Exchange	2010

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

4.2.5. Gestion de contenus d'entreprise (ECM) / GED

Description

il est à noter qu'il ne faut pas confondre ECM (Enterprise Content Management) et CMS (Content Management System) : l'ECM gère du contenu , le CMS permet d'en produire. La Gestion Electronique de Documents (GED) est à inclure dans l'ECM.

Un outil de gestion électronique de documents (GED) comporte en général les fonctionnalités suivantes :

- fonction de requêtes : recherches multicritères, croisées, opérateurs booléens, opérateurs de distance, recherche floue, recherche plein texte , gestion de thésaurus et de dictionnaire, recherche sémantique,
- fonction de sécurité : contrôle d'accès,
- fonction d'affichage : utilisation de bibliothèques de visualiseur (viewer) permettant l'affichage à l'écran, la manipulation de l'image obtenue, les possibilités d'impression (qui peuvent être le cas échéant désactivées en fonction de la qualité de l'utilisateur),
- fonction de journalisation des accès avec tenue de statistiques,
- intégration dans la base documentaire de nouveaux documents: numérisation à partir d'un scanner, reconnaissance de caractère (« *océrisation* »),
- gestion de flux (Workflow) .

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	**Version**	**Logiciel**	**Version**
Gestion de contenu (ECM)	Alfresco community edition	5.0.x	Alfresco Enterprise	5.0.x
GED / Workflow	Alfresco community edition	5.0.x	Alfresco Enterprise	5.0.x
GED / Repository	Alfresco community edition	5.0.x	Alfresco Enterprise	5.0.x
WCM			—	
Workflow	Alfresco (avec Red Hat JBoss jBPM), Bonita		Alfresco Enterprise	5.0.x

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / points complémentaires

CCT70	Il est OBLIGATOIRE de prendre en compte dès le début du projet les aspects conservation / archivage des documents : • combien de temps doit-il être conservé ? • quand doit-il être détruit ou basculé sur un serveur d'archivage dans un format pérenne ? • ….

Formats d'affichage

CCT71	Il est RECOMMANDÉ pour l'affichage des documents d'utiliser les formats PDF, TXT et XML. Le format HTML est possible mais non recommandé.

CCT72	Il est RECOMMANDÉ d'utiliser Acrobat Reader (≥ 11.x) pour manipuler le format PDF, qui offre des possibilités de visualisation, d'impression ou d'échange.

Formats d'échange d'images fixes

CCT73	Il est RECOMMANDÉ d'utiliser le format PNG v1.2 ou ultérieure, JPEG (illustrations photographiques). Le format TIFF v6.0 ou ultérieure (images non compressées) est possible mais non recommandé.

Poste client GED

Il convient de distinguer les postes de saisie (pilotage des scanners, retouche d'image, pilotage de la chaîne d'intégration, « océrisation », contrôle qualité), qui doivent privilégier le confort d'utilisation, des postes de consultation.

Dans le premier cas, les produits actuels continuent de privilégier une approche « client lourd » ou « client riche » nécessitant de déployer des composants (à minima les pilotes des scanners) sur le poste de travail, pertinente notamment au regard de la puissance informatique nécessaire, qu'il serait déraisonnable de déporter sans contrôle rapproché sur un serveur potentiellement distant.

Dans le second cas – postes de consultation ou de traitement hors chaîne d'intégration documentaire – il convient de privilégier des mises en œuvre sous forme de « client léger » ou de client « client riche ».

4.2.6. Editique

Description

Les logiciels d'éditique permettent :

- de fusionner des données issues d'applications métier à des trames types
- de mettre le résultat de la fusion à disposition de l'utilisateur ou de l'adresser directement à une imprimante.

CCT74	Il est OBLIGATOIRE d'utiliser les services d'éditique mutualisés (ARCHIMED ou BDOC Suite) pour toute application nécessitant de fusionner des trames avec des données métier. L'utilisation de BDOC Suite est soumise à licence et doit donc être justifiée auprès du Ministère (cf. CCT14).

CCT75	Il est RECOMMANDÉ d'utiliser le format PDF (Portable Document Format) pour la présentation des impressions à la demande.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Service éditique mutualisé	ARCHIMED (ARCHItecture Mutualisée d'EDitique)		BDOC Suite (Business Document , groupe GFI)	6.x

*(*) : cf . CCT14 - **Il est OBLIGATOIRE de justifier** le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.*

4.2.7. Moteur de recherche

Description

Les moteurs de recherche peuvent être utilisés pour :

- indexer le contenu d'un site web (côté serveur)
- indexer le contenu d'un poste de travail

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Indexation de contenu web (serveur)	Elastic Search	7.x		
	Solr	8.x		
Indexation de poste de travail			Windows Desktop Search (gratuit inclus dans windows)	4.0
			Copernic Desktop Search (payant)	7.x

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Points particuliers

Attention, certains outils gratuits, comme google desktop, présentent des risques de confidentialité par rapport aux données indexées sur le poste de travail. En effet, il n'est pas impossible que certaines informations du poste de travail soient envoyées sur le réseau, voire sur Internet.

4.2.8. Acquisition

Description

L'acquisition de données consiste à rendre numérique des données initialement non-numérique. Dans le contexte du ministère de la Justice, cela se traduit principalement par l'acquisition de données initialement au format papier :

- La numérisation consiste à transformer le document papier en fichier informatique de type « image »
- L'océrisation (OCR , reconnaissance de caractère) extrait le texte des images.
- La Lecture Automatique des Documents (LAD) et de Reconnaissance Automatique des Documents (RAD) permet d'extraire l'information contenue dans des formulaires papiers

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Numérisation	—			
OCR	—		Nuance Omnipage pro	19.2
RAD	—			
LAD	—			

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

4.2.9. Services de gestion de l'identité numérique

Le contrôle de l'identité numérique d'une personne est en général basé sur la connaissance d'un secret que la personne est la seule à connaître.

Ce secret peut-être :

- un simple mot de passe
- un mot de passe valable une seule fois (basé sur un token, par exemple)
- une caractéristique physique de la personne (biométrie)
- un certificat placé sur un support physique dont il est propriétaire (clé USB, carte à puce)

Service d'authentification

L'annuaire LDAP du ministère contient aujourd'hui une empreinte du mot de passe des utilisateurs.

Le Ministère a également mis en place un portail d'authentification unique (SSO) couplé à l'annuaire LDAP. Ces briques permettent d'assurer un premier niveau d'authentification des utilisateurs.

CCT76	Il est OBLIGATOIRE d'utiliser le portail d'authentification Unique (SSO) pour toute application web centralisée installée dans un centre de production.

Remarque :

Pour connaître les modalités d'intégration des applications avec le SSO et son interfaçage vous référer aux documents [R04] et [R05].

4.2.10. Décisionnel

Description

Le système d'information décisionnel est un ensemble de données agrégées, organisées de façon spécifique, facilement accessible et appropriées à la prise de décision ou encore une représentation intelligente de ces données au travers d'outils spécialisés. La finalité d'un système décisionnel est le pilotage de l'entreprise.

Un infocentre est une application décisionnelle qui apporte aux utilisateurs la visibilité dont ils ont besoin sur des données du système pour étayer leurs décisions.

L'utilisateur peut interroger l'infocentre avec ses propres requêtes sans connaître le langage informatique de manipulation des données. Il peut également utiliser des requêtes prédéfinies. Les résultats sont présentés de façon attractive dans des documents que l'on peut rafraîchir et partager avec d'autres utilisateurs.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	**Version**	**Logiciel**	**Version**
Décisionnel (ODS, datawarehouse, datamart, infocentre)			SAS	
	Jasper Reports	6.4.x	Business Objects BI	4.1
Alimentation (ETL)	Talend Data Integration	6.3.x	Business Object Data Integrator	4.2

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / points complémentaires

Un ETL permet de réaliser l'Extraction, la Transformation, et le Chargement (Load) des données dans l'infocentre, à partir des applications source. Pour ce faire, il utilise une base de données de travail appelée ODS (operationnal data store).

CCT77	Il est RECOMMANDÉ d'utiliser un ETL afin d'homogénéiser les procédures de chargement.

Les outils opensource n'ont pas été testés. Il conviendra donc de réaliser une étude comparative plus poussée lors de la première mise en oeuvre.

4.2.11. Systèmes d'Information Géographique

Description

Un Système d'information Géographique permet de :

- mettre à disposition des cartes géographiques
- transformer des adresses en position géographique
- superposer des zones/itinéraires sur les cartes

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
SIG	Geoserver	2.15.x	Mapinfo	17
Service de cartographie	openstreetmap			

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

4.2.12. Portail

Description

Un portail est un site web qui réunit différentes ressources, soit autour d'un même thème (portail services publics, portail d'emploi…) soit sans thème particulier, on parle alors de portail généraliste (ex : Yahoo).
Un portail donne accès à des ressources qui ne lui appartiennent pas toutes : il propose des services relevant d'autres sites, sa valeur ajoutée propre étant dans la sélection et la réunion de ces outils.
Enfin, un portail intègre aussi une dimension de personnalisation, plus ou moins élaborée.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Portail personnalisé	LifeRay	7.x+	Red Hat JBoss Portal	6.2.0
			eXoPlateform	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Les outils cités n'ont pas été testés. Il conviendra donc de réaliser une étude comparative plus poussée lors de la première mise en œuvre.

4.2.13. E-formation

Description

La formation en ligne (e-formation ou e-learning) est l'utilisation des nouvelles technologies du multimédia et de l'Internet afin d'améliorer la qualité et de réduire les coûts de la formation à travers l'accès à distance à des ressources et des services, ainsi qu'à des collaborations et des échanges.
La formation en ligne résulte donc de l'association de contenus interactifs et multimédia, de supports de distribution (PC, internet, intranet…), d'un ensemble d'outils logiciels permettant la gestion d'une formation en ligne et d'outils de création de formations interactives (Cf. http://eduscol.education.fr/numerique/dossier/archives/eformation (archives)).

Trois fonctions de base sont concernées :

- l'hébergement technique,
- la plateforme technique,
- les cours.

Ces derniers peuvent être développés en interne, en externe ou acquis sous forme de modules pour être mis en place sur la plateforme.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
	MOODLE	>=3.4.x	Ganesha (Société anema)	>= 3

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

CCT78	Il est RECOMMANDÉ de respecter les standards **SCORM** (issu de l'administration fédérale des Etats-Unis) et **AICC** (issu des professionnels de l'aviation civile) afin : • d'assurer le portage sur la majorité des plates-formes d'e-formation du marché formation, • d'être ouvert et de faciliter l'intégration des modules de formation.

4.2.14. Orchestration de services

Description

Dans une architecture orientée service, il peut être utile de mettre en oeuvre des outils capables d'ordonnancer l'appel à différents services unitaires afin d'effectuer une tâche plus globale. C'est ce qu'on appelle l'orchestration de services.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
BPM	Bonita	7.5.x		
	Red Hat JBoss jBPM			

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Les outils cités n'ont pas été testés. Il conviendra donc de réaliser une étude comparative plus poussée lors de la première mise en œuvre.

5. INFRASTRUCTURE

Ce chapitre définit les règles relatives aux socles techniques de bas niveau mis en oeuvre dans le Système d'information Justice.

5.1. SOCLES TECHNIQUES

5.1.1. Poste de travail

Logiciel

Description

L'objectif de ce thème est de définir les systèmes d'exploitation utilisables sur le poste de travail justice et leurs conditions de mise en œuvre.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Système d'exploitation	Linux Ubuntu Workstation (**)		Microsoft Windows	10 (64 bits)

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

(**) : l'utilisation d'Ubuntu sur son Poste de travail est autorisée à titre expérimental.

CCT79	Il est INTERDIT d'utiliser un OS Windows autre que Windows7 ou Windows10

CCT80	Il est RECOMMANDÉ que les applications déployées sur les postes de travail aient la double compatibilité Windows 7 x86 (32bits/64bits)/Windows 10 x86(32bits/64bits).

Matériel

Description

Les supports juridiques destinés à l'acquisition de poste de travail au plan national spécifient, sous forme de configurations types, différents modèles de postes de travail adaptés à différents types de mission. Ces composants peuvent varier dans le temps en fonction de l'évolution du marché et, en corrélation, du support juridique ainsi que de celle du présent référentiel technique.

Remarques / points complémentaires

Configurations

Le détail des configurations des postes de travail est publié sur l'Intranet SG (Informatique/Marchés) : cf. URL référencée en [R01].

Le détail des configurations des ordinateurs portables est publié sur l'Intranet SG (Informatique/Marchés) : cf. URL référencée en [R02].

CCT81	Il est OBLIGATOIRE de passer par les marchés nationaux pour l'acquisition des postes de travail, sous risque de ne pas être maintenu par le SNM (voir paragraphe suivant).

Maintenance matérielle

La relève des incidents matériels sur les postes de travail et leurs principaux périphériques [mais pas sur les consommables] est assurée par le service national de maintenance – SNM –, piloté au niveau des Antennes régionales du Système d'Information.

Sécurité

CCT82	Il est OBLIGATOIRE de sécuriser le poste de travail: - en mettant en oeuvre l'antivirus national (PRIAM) - en automatisant les mises à jour du système d'exploitation avec WSUS - en intégrant les postes dans l'Active Directory

5.1.2. Serveurs

Logiciel

Description

L'objectif de ce thème est de définir les systèmes d'exploitation utilisables sur les serveurs et leurs conditions de mise en œuvre.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Système d'exploitation	Linux CentOS	≥ 7.x	Red Hat Enterprise Linux	7.6
			Microsoft Windows Server	2012 R2 2016

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Les critères de choix entre Linux et Microsoft Windows pour les serveurs d'applications sont avant tout dictés par la compatibilité avec les applications à héberger : certains systèmes de gestion de bases de données ne fonctionnent qu'avec l'un des systèmes d'exploitation.

CCT83	Il est RECOMMANDÉ d'utiliser Linux en cas de forts besoins de sécurité ou de disponibilité.

Il est à noter que Linux CentOS est généralement dédié aux produits commerciaux packagés (appliances) nécessitant cette contrainte. Le **système d'exploitation privilégié pour l'hébergement est Red Hat Enterprise Linux.**

L'utilisation de Windows 2012 Server (et plus) est envisageable si l'application n'est pas compatible avec Linux.

Dans le cas où le système à choisir n'est pas contraint par l'application, on prendra en compte les critères d'exploitation, et notamment la possibilité d'intégrer le système d'exploitation dans les architectures existantes, ainsi que les compétences et les besoins de formation des agents d'exploitation.

Pour une même application, on choisira un seul système d'exploitation du serveur. On ne cherchera pas à installer certaines configurations sous Windows Server et d'autres sous Linux, ce qui aurait pour effet d'accroître les coûts d'intégration, de qualification, de télédiffusion, d'exploitation et d'administration.

CCT84	Il est RECOMMANDÉ d'utiliser Linux pour les bases de données PostgreSQL.

Matériel

Description

L'objectif de ce thème est de définir les matériels susceptibles de supporter les serveurs de différents types ainsi que les contraintes qui les accompagnent et les sécurités à mettre en place.

Les serveurs supportés sont de type serveurs matériels banalisés **x86** (Intel, AMD) ces plates-formes multi-constructeurs supportent différents systèmes d'exploitation : Windows, Linux, … ;

Produits / composants

Le détail de ces configurations est publié sur la GED interne accessible uniquement aux agents du ministère de la Justice cf. URL référencée en [R07].

CCT85	Il est OBLIGATOIRE de passer par les marchés nationaux pour l'acquisition des serveurs sous risque de ne pas être maintenu par le Service National de Maintenance (SNM).

Sécurité

CCT86	Il est OBLIGATOIRE de sécuriser les serveurs, aussi bien au niveau matériel que logiciel, en suivant les recommandations : - mise à jour de sécurité des systèmes d'exploitation - antivirus selon le cas

5.1.3. Serveurs locaux de ressources

Description

Le serveur local de ressources (SLR) doit être l'élément fédérateur pour les utilisateurs du réseau local. A ce titre il permet, en fonction des opportunités, le partage d'équipements spécialisés (sauvegarde, télécopie, modem, imprimantes couleur ou haut débit, ...).

Les serveurs locaux de ressources fournissent les services suivants :

- fonctions techniques au sein du réseau local : services de partage de fichiers, d'inventaire, d'anti-virus,
- partage de périphériques : sauvegarde, imprimantes, scanner, télécopie, …

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Stockage	Linux CentOS avec Samba	3.6.x 4.2.x		

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

CCT87	Il est RECOMMANDÉ de limiter le nombre de SLR au profit de solutions mutualisées.

CCT88	Il est OBLIGATOIRE que le serveur local de ressources soit banalisé et indépendant des applications.

Remarques / points complémentaires

Le serveur local de ressources, pour des raisons de performance, est en général implanté au niveau de la plus forte concentration d'accès ; il est exploité (c'est-à-dire administré, supervisé, sauvegardé) à ce niveau.

5.1.4. Imprimantes

Description

Ce paragraphe concerne la gestion des files d'attente d'imprimante et le partage d'imprimantes pour des postes de travail.

Le principal intérêt d'un serveur d'impression, outre sa capacité à gérer des fichiers de très gros volume, est qu'il permet d'éviter d'installer les pilotes d'imprimantes sur tous les postes de travail.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
File d'impression	CUPS pour les serveurs linux	2.0.x	Intégré à Windows Server	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

Remarques / Points complémentaires

CCT89	Il est RECOMMANDÉ d'utiliser le format PDF (Portable Document Format) lors de l'envoi d'un demande d'impression à une file d'impression (économie de bande passante).

CCT90	Il est OBLIGATOIRE de passer par les marchés nationaux pour l'acquisition des imprimantes, sous risque de ne pas être maintenu par le SNM.

5.1.5. Autres équipements

D'autres équipements sont susceptibles d'être branchés sur le RPVJ :

- badgeuse
- serveurs de biométrie
- scanner
- photocopieur / numériseur

Dans tous les cas, il convient d'être particulièrement vigilant sur les problématiques de sécurité qui peuvent y être associées.

CCT91	Il est OBLIGATOIRE de demander un avis au SSIC avant le branchement de tout nouveau type d'équipement sur le RPVJ.

On pourra se référer à la PMDS pour plus de précisions (cf. document référencé [A10]).

5.1.6. Virtualisation des ressources

Description

La virtualisation est un ensemble de techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation avec plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.

La mise en place de la virtualisation a notamment pour intérêts :

- de faciliter l'installation, le déploiement et la migration des machines virtuelles d'une machine physique à une autre ;
- d'économiser sur le matériel par mutualisation (consommation électrique, entretien physique, monitoring, support, compatibilité matérielle, etc.) ;
- de sécuriser et/ou d'isoler un réseau (exemple : cassage des systèmes d'exploitation virtuels, mais pas des systèmes d'exploitation hôtes qui sont invisibles pour l'attaquant) ;
- d'allouer dynamiquement de la puissance de calcul en fonction des besoins de chaque application à un instant donné ;
- de diminuer les risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, ;

La virtualisation apporte un gain en disponibilité (en cas de panne, il est plus aisé de remplacer une machine virtuelle par une autre que de réinstaller un serveur). En cas de panne matérielle du serveur hôte, il est également plus facile de migrer la machine virtuelle sur un autre serveur hôte. Ce type d'approche permet de considérer les infrastructures matérielles comme des consommables (« commodities ») que l'on peut facilement remplacer si nécessaire.

Toutefois, la virtualisation induit une surconsommation de mémoire et de puissance de calcul de l'ordre de 15% (variable selon les technologies).

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Virtualisation de système d'exploitation	KVM	selon distribution linux	VMWare Esx(i)	>=6.0 u3
			Microsoft Hyper-V	2016 LTSB server pour les nouveaux serveurs. 2012R2 (fin support 2023) : migration à planifier

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

CCT92	Il est RECOMMANDÉ que l'application soit supportée sur un serveur virtuel.

Pour les serveurs virtualisés sous Microsoft HyperV 2012R2 (fin de support 2023), il est nécessaire de planifier une migration technique pour migrer vers les versions 2016.

5.1.7. Mutualisation / consolidation des ressources

Description

Cohabitation des applications/ des données sur un serveur

Il est important de prévoir, lors de la conception des applications, qu'elles pourront cohabiter sur un même serveur, on parle alors de mutualisation.

Concernant l'implantation des applications sur les serveurs, les cas suivants sont à prévoir :

- serveur dédié : **mono-instance et mono-application/base,**
- serveur collectif : **mono-instance et multi-applications/bases,**
- serveur mutualisé : **multi-instances et mono-application/base,**
- serveur banalisé : **multi-instances et multi-applications/bases.**

Une instance est par exemple un service, une entité administrative.

Les applications nationales doivent pouvoir être installées, au choix, sur un serveur dédié à une instance ou partagé entre plusieurs instances. Un serveur doit également pouvoir héberger plusieurs applications sur un environnement homogène de bases de données.

Un regroupement ou un éclatement des instances d'applications doit pouvoir être effectué facilement. On veillera à cette fin à conserver une indépendance totale entre les services, même si leurs données cohabitent sur la même machine.

Avantages / inconvénients

La consolidation de services sur un même serveur n'induit pas, contrairement à la virtualisation, de surconsommation de mémoire ou de puissance de calcul, autre que celles des services mis en oeuvre.

L'un des inconvénients majeurs de la consolidation est le couplage qui est induit entre les applications mutualisées, en particulier par rapport à la version du système d'exploitation utilisé.

Mise en oeuvre:

La mutualisation/consolidation est aujourd'hui mise en œuvre au ministère de la Justice mais mériterait d'être développée :

- sur les serveurs de présentation web
- sur les serveurs de présentation Citrix
- sur les serveurs d'application
- sur les serveurs de base de données

CCT93	Il est OBLIGATOIRE de mettre en œuvre les services de présentation sur des serveurs mutualisés.

CCT94	il est RECOMMANDÉ de mettre en œuvre la mutualisation des services en mode multi-instance, afin d'assurer un maximum de découplage entre les services.

En effet, une instance logicielle par application (que ce soit au niveau des serveurs de présentation, applicatif ou de base de données) permet de découpler les applications mutualisées par :

- la possibilité de démarrer/arrêter les services propres à une application indépendamment les uns des autres
- la possibilité d'avoir des versions logicielles différentes pour le même service, d'une application à l'autre

En pratique, cela signifie qu'il n'est pas recommandé de mettre des virtuals hosts multiples dans une seule instance APACHE, ou de déployer plusieurs webapps dans le même conteneur TOMCAT.

Sécurité

La mise en œuvre de la mutualisation peut induire des risques supplémentaires pour une application sensible en cas d'attaque et de prise de main via une des autres applications hébergées sur le même serveur. Ce risque est toutefois à relativiser, en particulier sur les centres de production, dans lesquels le réseau très cloisonné implique par lui même un haut niveau de sécurité.

Afin de minimiser les risques de sécurité liés à la mutualisation, il convient d'utiliser des services distincts pour chaque application hébergée sur un même serveur.

CCT95	Il est RECOMMANDÉ que chaque service applicatif exécuté sur un serveur le soit avec un utilisateur technique propre à l'application. En particulier, les services ne doivent pas être exécutés directement par l'utilisateur root ou par l'administrateur.

5.2. RÉSEAU

CCT96	Il est OBLIGATOIRE pour toute application d'estimer, lors de la phase d'architecture, la bande passante consommée et de la vérifier lors de la recette.

Pour cela, il est indispensable de **sensibiliser les équipes projets à la problématique de consommation de la bande passante.** Il est important de rappeler que quel que soit le débit offert par le réseau, les applications développées pour l'utiliser doivent respecter les consignes de développement. Par exemple, il faut apporter un soin particulier à la richesse des pages envoyées à un navigateur internet.

Il est primordial de sensibiliser les équipes projets dès les phases amont sur les points suivants :

- l'optimisation du poids des pages HTML
- le poids des flux multimédia : images, sons, vidéos ;
- la qualité de service nécessaire pour la téléphonie sur IP.

5.2.1. Réseau local (LAN)

Complément au système de câblage structuré

Certaines situations géographiques ne peuvent pas justifier l'investissement d'une infrastructure de câblage structuré (site classé, faible taux d'occupation, location temporaire...) aussi malgré les limitations actuelles en matière de distance et de bande passante, les technologies du réseau sans fil , ou du Courant Porteur en Ligne (CPL) peuvent apporter une solution complémentaire pour les raccordements d'équipements .

CCT97	Il est OBLIGATOIRE pour la mise en œuvre de solutions sans fil ou CPL de réaliser une étude de sécurité et d'en obtenir une validation conjointe SSIC-FSSI.

CCT98	Il est OBLIGATOIRE pour la mise en œuvre de solutions sans fil ou CPL d'utiliser un protocole conforme à la version de la norme 802.11 qui intègre les niveaux de sécurité renforcée.

Câblage, structuré du réseau local

CCT99	Il est OBLIGATOIRE de se conformer au cahier des clauses techniques de câblage établi par le SSIC.

Dispositifs de connexion et de commutation

Les éléments actifs (Répéteur Ethernet, Commutateur, Pont/routeur) installés sur le câblage constituent le réseau local Ethernet.

CCT100	Il est INTERDIT, pour des raisons de qualité de service, d'utiliser des HUB et les doubleurs sur les prises RJ-45.

L'intérêt des commutateurs est d'offrir le débit maximal (10 Mbits/s, 100 Mbits/s ou 1000 Mbits/) en mode point à point pour chacune des machines ou des sous-réseaux qui lui sont connectés.

- Au niveau des locaux de sous répartition, le raccordement appelé aussi brassage des points d'accès aux éléments actifs de premier niveau permet de construire des segments Ethernet indépendants (groupe de travail indépendant lié à une application). Prioritairement des commutateurs Ethernet niveau 2 y sont installés.

- Pour permettre à partir des postes de travail autorisés, d'accéder à des ressources partagées, notamment l'accès au RPVJ ou à des serveurs d'application, ces segments indépendants seront interconnectés par un commutateur Ethernet de niveau 3.

L'architecture et l'exploitation des réseaux locaux sont du ressort du SSIC.

De plus, un cloisonnement est effectué sur les sites possédant un pare-feu.

Ce cloisonnement par VLAN est découpé de la manière suivante :

Type de VLAN	Description
RPVJ4	Dédié aux équipements opérateur mais également aux appliances de priorisation de flux et de filtrage.
Postes de travail et imprimantes	Dédié aux équipements de type poste de travail et imprimantes.
Serveurs internes	Dédié aux serveurs atteignables depuis l'extérieur uniquement pour des fonctions d'administrations par des utilisateurs de type administrateur dûment identifiés.
Serveur externes	Dédié aux serveurs atteignables depuis n'importe quel site distant du Ministère en fonction des règles de filtrage imposées par le RSSI de la direction métier.
Visioconférence	Dédié aux équipements de Visioconférence
VoIP/ToIP	Dédié aux équipements de téléphonie sur IP.
Administration	Dédié aux équipements devant être administrés via une adresse IP (exemple : équipements actifs de réseau).
PSE/PSEM	Dédié aux équipements concernant le dispositif de bracelet électronique.
Équipements internes	Dédié aux équipements exploités par la direction métier qui ne sont uniquement atteignable que pour des fonctions d'administration par des utilisateurs de type administrateur dûment identifiés.
Équipements externes	Dédié aux équipements exploités par la direction métier atteignables depuis n'importe quel site distant du Ministère en fonction des règles de filtrage imposées par le RSSI de la direction métier.

De plus, des conventions d'adressage et de nommage sont définis par un document de normalisation des LAN (cf. Normalisation des vlans et de l'@ ip-rpvj-V2 9)

Raccordement des serveurs au réseau local

Les serveurs dont les besoins de communication sur le réseau local sont importants seront connectés directement à un commutateur Ethernet, via une liaison à 100 Mbits/s voire une liaison à 1000 Mbits/s.

Protocole

Description

Le protocole du réseau local décrit les protocoles de communication de haut niveau nécessaires aux machines pour communiquer entre elles. Le protocole cité ici (TCP/IP) est un protocole dit « de transport » qui vient se placer au-dessus des protocoles réseaux utilisés (CSMA/CD).

CCT101	Il est OBLIGATOIRE d'utiliser le protocole TCP/IP pour les communications entre les machines du ministère.

CCT102	Il est DÉCONSEILLÉ d'utiliser des fonctionnalités spécifiques à l'API Microsoft WINSOCK (Windows Sockets).

CCT103	Il est INTERDIT d'utiliser le protocole NETBIOS en réseau distant. En cas de nécessité absolue, l'utilisation du protocole normalisé NETBIOS over TCP/IP est envisageable.

Sites déconcentrés

La bande passante des sites du ministère de la Justice est dimensionnée selon plusieurs critères:

- L'effectif du site
- Les services mis à la disposition du site (Visioconférence, Téléphonie sur IP...)
- L'hébergement de pôle utilisant des applications spécifiques (CHORUS, PSE/PSEM)

Ces dimensionnements sont réévalués en fonction des déploiements applicatifs ou d'ajout de service sur ces sites.

Sites nationaux

De façon générale, la bande passante allouée aux centres de production nationaux doit permettre la bonne marche des applications dites centralisées. Ce dimensionnement est réévalué en fonction des pré-réquis techniques des futures applications à déployer.

5.2.2. Réseau distant RPVJ (WAN)

Description

Au-delà des applications et des données accessibles sur un poste de travail ou sur un serveur local, l'utilisateur doit pouvoir :

- accéder à des applications hébergées sur des serveurs distants ;
- échanger des informations avec d'autres services du ministère de la Justice ;
- communiquer avec les environnements informatiques des interlocuteurs du ministère de la Justice.

CCT104	Il est OBLIGATOIRE d'utiliser l'infrastructure RPVJ pour les échanges entre sites distants.

Le réseau national de transmission de données du ministère de la Justice est le Réseau Privé Virtuel Justice.

Le RPVJ constitue la solution technique de référence pour tous les besoins de communications informatiques entre services relevant du ministère de la Justice (administration centrale, juridictions, services déconcentrés). Il est également interconnecté aux réseaux des autres administrations de l'Etat via le réseau AdER et aux extranets des ordres professionnels (avocats, avoués, ..).

Le RPVJ offre par ailleurs un service sécurisé d'interconnexion avec Internet, exclusif de toute autre solution d'accès au « réseau des réseaux ».

Le RPVJ est un réseau entièrement basé sur les standards IP. Il fait l'objet d'une infogérance. Cette architecture permet le partage d'une épine dorsale à base de relais de trames (frame relay) ou en ATM. Les points d'accès physiques à cette structure sont obtenus par l'intermédiaire d'une liaison (spécialisée, S/ADSL ou RNIS) entre le site à raccorder et un point d'entrée sur l'épine dorsale.

Pour les besoins de l'informatique nationale, le ministère de la Justice utilise le RPVJ pour toutes transmissions de données.

Pour les besoins d'interconnexion de sites physiques distants, le RPVJ constitue la solution technique pour tout système d'information du ministère.

Le RPVJ se compose d'une part d'un réseau de transport et d'autre part d'une plate-forme de service .

Le réseau de transport :

- assure une connexion des réseaux locaux implantés dans les sites Justice, par des accès permanents et sécurisé, vis-à-vis d'internet et des autres clients de l'opérateur
- assure la connexion des postes individuels (nomades) via un kit de mobilité permettant une multitude de moyens de connexion (RTC, Ethernet, Wifi et 3G) ;
- permet la communication de réseau local à réseau local et/ou de poste individuel à réseau local ;
- met en relation les réseaux locaux et les postes individuels avec la plate-forme de service du RPVJ.

La plate-forme de service RPVJ :

- Elle héberge les équipements techniques qui supportent les services communs du RPVJ (relais de messagerie, serveurs de noms, antivirus …) et offre l'accès à l'Internet. Ainsi, tous les utilisateurs justice partagent, au travers du réseau de transport ce même accès mutualisé et sécurisé à l'Internet.

Le RPVJ se compose de plusieurs VRF (Virtual Routing Forwading) que l'on peut associer à des VPN distincts :

Nom VRF	Description
VRF S0	Regroupe la majeure partie des sites du Ministère de la Justice (environ 95%).
VRF S1	Regroupe la totalité des sites DOM/TOM.

VRF N0	Regroupe les sites dont la gestion du LAN n'est pas assurée par le Secrétariat Générale.
VRF N1	Regroupe les accès nomades.
VRF PARTENAIRE	Regroupe les accès vers les partenaires publics/privés.

Dans chaque VRF, la politique de routage est de type « Any-to-Any », chaque site peut donc communiquer avec les autres.

Le routage inter-VRF est assuré en cœur de réseau via la plate-forme de service mise à disposition par l'opérateur. Un filtrage des flux inter-VRF est effectué afin de garantir un niveau de sécurité suffisant.

Il est à noter qu'une interconnexion existe avec l'opérateur Orange pour les sites de Mayotte de la justice.

Le schéma ci-dessous représente l'architecture de principe du RPVJ :

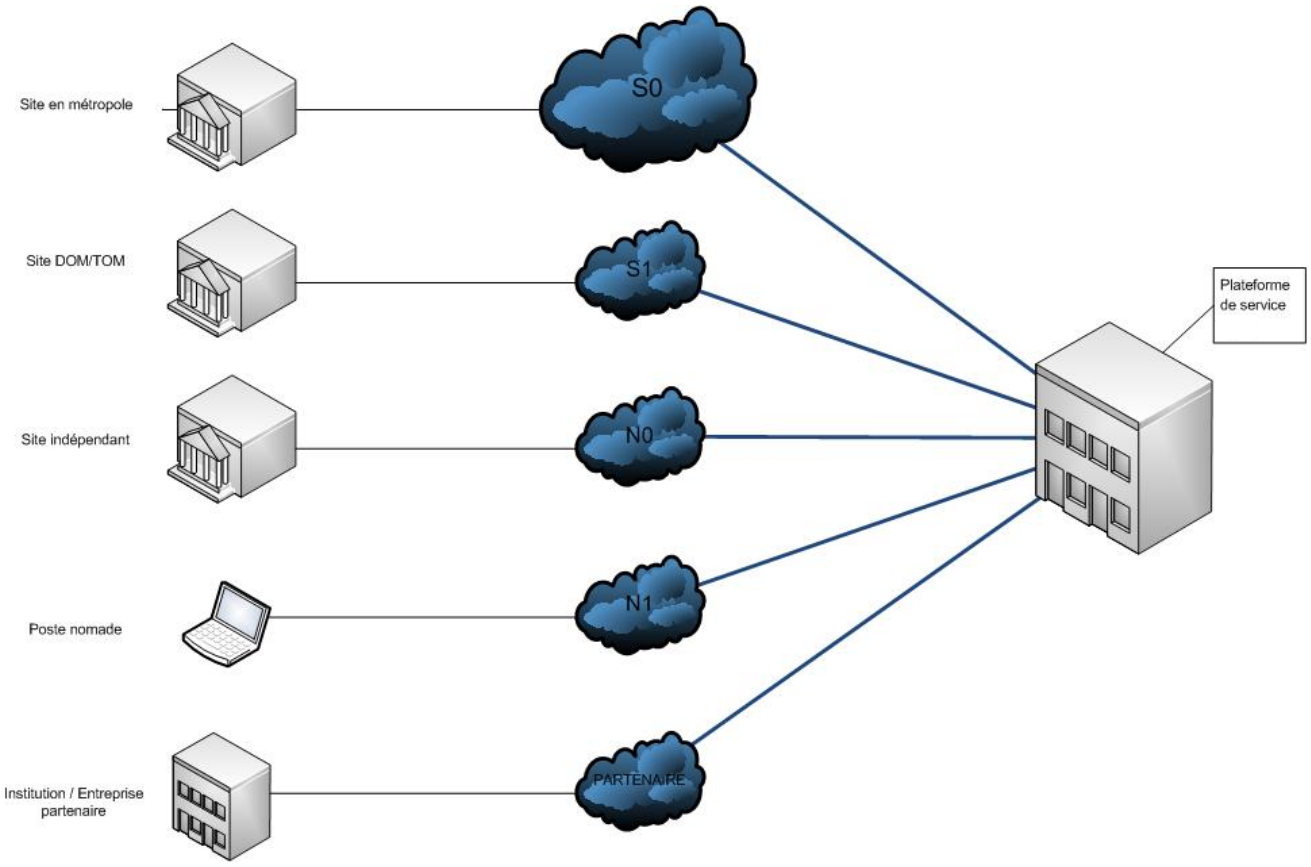

Schéma de principe du RPVJ

Le RPVJ irrigue la totalité des sites du ministère de la Justice (administration centrale, juridictions, services déconcentrés de l'administration pénitentiaire, services déconcentrés de la protection judiciaire de la jeunesse, GIP et établissements publics placés sous tutelle du ministère de la Justice).

Architecture d'accès sécurisé

Accès sécurisé à l'Internet

Connexions « entrantes » depuis l'Internet

Les seules initialisations de connexions admises en provenance d'Internet (connexions « entrantes ») concernent les messages issus du domaine public Internet et destinés à un utilisateur du domaine **justice.gouv.fr** ou **justice.fr**.

Un pare-feu associé à un relais SMTP assure la rupture des flux destinés aux serveurs de messagerie où sont gérées les boîtes aux lettres E-mail.

Un serveur antivirus analyse la totalité des flux SMTP (messages et pièces jointes), HTTP et FTP à l'exception de ceux cryptés. La table des virus connus est mise à jour dès que les virus sont détectés par un laboratoire spécialisé.

CCT105	Il est INTERDIT d'initialiser des connexions en provenance d'Internet (connexions « entrantes » autres que les messages issus du domaine public Internet et destinés à un utilisateur du domaine ***.justice.gouv.fr** ou ***.justice.fr**.

Connexions « sortantes » vers l'Internet

Quel que soit le mode d'accès utilisé, chaque utilisateur du RPVJ peut potentiellement, depuis son navigateur, accéder à l'Internet (serveurs Web, serveurs FTP, …) via l'accès mutualisé entre tous les sites du ministère. Cet accès bénéficie d'une sécurité de trois ordres :

1. les adresses internes au RPVJ sont masquées à l'égard d'Internet ;
2. un service anti-virus est appliqué aux flux HTTP et FTP issus de l'Internet. La table des virus connus est mise à jour dès que les virus sont détectés par un laboratoire spécialisé.
3. les connexions « entrantes » sont interdites (seuls les messages en provenance de l'Internet sont admis par le pare-feu).
4. Filtrage des sites web par liste noire et en fonction de leur contenu

Accès vers et depuis les Extranets

L'interconnexion du RPVJ avec d'autres réseaux Intranet (Extranets) est traitée via une liaison centralisée. Cette liaison est raccordée côté plate-forme justice à un serveur « pare-feu » auquel est associée une plate-forme « DMZ EXTRANET ». Seuls les serveurs présents dans cette zone sont directement accessibles par les utilisateurs des extranets.

Un relais SMTP

Les messages en provenance des domaines d'un extranet ne sont acceptés que s'ils proviennent du relais SMTP de l'extranet considéré. Les seuls domaines visés acceptés sont : ***.justice.fr** et ***.justice.gouv.fr**.

Les messages sont redirigés ensuite vers le relais « Central » justice interne. Ce relais « Central » se charge enfin d'orienter les messages vers les serveurs de messagerie hébergeant la boîte à lettres de l'utilisateur Justice.

Un relais HTTP

Ce relais est le seul serveur HTTP accessible depuis l'extranet considéré. Il se charge de relayer les demandes vers les véritables serveurs Web visés. Il gère donc une table de correspondance entre les noms externes et des noms internes.

A ce jour, la plate-forme gère l'interconnexion avec AdER (interconnexion avec les autres ministères) et avec les autres extranet partenaires.

5.2.3. Pare-feu

Une partie, et à terme, l'ensemble des sites déconcentrés du ministère de la Justice est pourvu d'un pare-feu permettant de cloisonner l'ensemble des flux. La politique de filtrage de chaque direction métier (DSJ, DAP, DPJJ) est piloté par chaque RSSI. Il lui revient la tâche de définir quels sont les flux à autoriser ou à bloquer ; il en fait alors part à SSIC/SDIDE/TOP/IVD, qui est garant, par le biais de son infogérant, de l'intégrité et de la conformité des règles présentes sur les pare-feux.

CCT106	Il est OBLIGATOIRE de faire une demande d'ouverture auprès de la SSIC/SDIDE/TOP/IVD. lorsqu'une application utilise un port non standard. Par défaut, seuls les protocoles et les ports réellement utilisés par les applications du ministère sont autorisés par le dispositif de sécurité du RPVJ.

5.2.4. Mobilité (nomadisme et télétravail)

Description

Pour rejoindre les ressources de son réseau, le ministère de la Justice offre la possibilité à ses utilisateurs nomades la possibilité de se connecter via une solution sécurisée par VPN.

Cette solution se matérialise par l'installation sur un poste fixe ou nomade (obligatoirement fourni par le Ministère) d'un kit de connexion personnalisé ainsi que d'une surcouche VPN avec technologie IPsec pour le chiffrement des données.

Connexion au RPVJ des postes nomades

La connexion des postes nomades est possible à partir d'une prise téléphonique du réseau téléphonique commuté (RTC) public, d'une prise Ethernet hors-RPVJ, d'une connexion Wifi ou d'une connexion 3g.

Pour préserver la confidentialité des données justice, une connexion via un kit de connexion fourni par l'opérateur est prévue. Celui-ci intègre une solution embarquée d'encapsulation VPN/IPsec.

Poste nomade

CCT107	Il est OBLIGATOIRE de respecter les recommandations de sécurisation des postes de travail mobiles décrites dans le document intitulé « Politique ministérielle de défense et de sécurité » (cf. document [A10]).

Journalisation

Une journalisation des accès et tentatives d'accès est effectuée par le prestataire de réseau distant. Toute anomalie est signalée selon sa gravité.

Ressources accessibles

Les ressources RPVJ accessibles depuis les postes nomades sont :

- la messagerie électronique ministérielle,
- l'intranet ministériel,
- les applications web HTTP et HTTPS,
- internet, selon les mêmes restrictions que les postes fixes connectés sur les LAN des sites.

Tout accès à une application à travers un accès nomade donne lieu à une authentification manuelle de l'utilisateur.

Les opérations sur les applications métiers effectuées via accès nomade sont tracées.

Suivi de l'usage

Les accès nomades au RPVJ sont accordés après avis des directeurs et sous-directeurs au niveau central, des chefs de cour et des directeurs de services régionaux au niveau déconcentré. Les analyses du trafic nomade (avec indication des anomalies, du nombre d'appel, de la durée totale de ceux-ci) sont envoyées tous les six mois aux directeurs concernés, pour contrôle.

5.3. SERVICES TECHNIQUES

Ce chapitre présente les services techniques existant au Ministère et devant être utilisés par les applicatifs.

5.3.1. DNS / Résolution de nom

Le protocole DNS permet de référencer des machines (ou tout équipement portant une adresse IP) par un nom « parlant » plutôt que par son adresse IP.

Un service national de Résolution de Nom existe sur le RPVJ. Il est composé de multiples serveurs répartis sur le territoire répliquant une base centrale.

CCT108	Il est OBLIGATOIRE d'utiliser des noms de domaine plutôt que des adresses IP pour rendre accessibles les applications aux utilisateurs.

Ceci permet en particulier d'éviter les opérations de déploiement en cas de changement d'adresse IP des serveurs.

CCT109	Il est OBLIGATOIRE que les applications nationales intranet utilisent un nom de domaine finissant par intranet.justice.gouv.fr.

5.3.2. NTP / serveur de temps

Le protocole NTP permet aux différents équipements d'un système d'information de synchroniser leurs horloges sur un serveur de temps central.

CCT110	Il est OBLIGATOIRE que tout serveur synchronise son horloge sur le serveur NTP du Ministère, ou sur un de ses relais officiels.

5.3.3. Annuaires de ressources

Description

Les services d'annuaire sont destinés à fournir des informations sur des ressources : techniques, logicielles, humaines ... Ces informations peuvent être utilisées par les applications constituant le système d'information justice, par exemple :

- pour adresser (atteindre) un utilisateur, une personne physique, un service ou un équipement,
- pour vérifier l'authentification d'un utilisateur,
- pour associer des droits d'accès ou d'action à un utilisateur,
- ...

Dans le contexte technique du ministère de la Justice, le besoin identifié couvre essentiellement :

- des besoins en termes d'identification/authentification d'utilisateurs et de droits associés (la cible potentielle est constituée par toutes les applications métiers, même si la mise en œuvre ne se fait que nécessairement très progressivement),
- des besoins en termes d'annuaire des agents du Ministère, des juridictions et des services déconcentrés (organigramme, téléphone, messagerie, ...).

Active Directory

Les recommandations particulières concernant la mise en œuvre d'Active Directory et notamment les normes de nommage, sont publiées sur le site intranet de la SDIDE.

CCT111	Il est RECOMMANDÉ, afin de pouvoir exploiter les applications dans de bonnes conditions de disponibilité et de sécurité, qu'un domaine enfant comporte au moins 2 contrôleurs de domaine (DC).

Annuaire Ministériel LDAP

CCT112	Il est OBLIGATOIRE d'utiliser LDAP v3 (RFCs 2251 à 2255) pour couvrir les besoins liés à l'identification/authentification des utilisateurs, notamment dans le cadre des applications sensibles, nécessitant par exemple une sécurité forte.

Le produit libre « 389 Directory Server » est utilisé pour l'infrastructure nationale de serveurs d'annuaire sur les sites de production.

On pourra également se reporter aux chapitres 3.10.4 Habilitations et profils et 4.2.2 Annuaire ministériel

5.3.4. Plateformes d'échanges

Description

Les plateformes d'échanges permettent de découpler les échanges de données entre les sous-systèmes d'un SI ou avec l'extérieur.

Ils peuvent prendre en charge des échanges :

- d'application à application
- d'utilisateur à application
- d'application à utilisateur

D'un point de vue technique, on peut distinguer trois types de services applicatifs de communication entre applications:

- le mode transfert de fichiers,
- le mode orienté message (MOM),
- le mode web service entre serveurs d'applications.

Une plateforme d'échange peut prendre en charge :

- le routage des données
- la garantie du bon acheminement des données
- une transformation de protocole de communication entre les applications source et destination

Le mode Transfert de fichiers

Les conditions de sa mise en œuvre sont à étudier au coup par coup entre l'émetteur et le destinataire pour ce qui concerne, l'enveloppe (type et format du fichier), la syntaxe du contenu, la périodicité et le mode d'activation des transferts.

Le transfert de fichier ne constitue pas à lui seul, un élément suffisant pour établir une communication exhaustive ; c'est pourquoi, bien souvent, il sera associé à un moniteur de transfert de fichier.

CCT113	Il est OBLIGATOIRE d'utiliser le format XML pour tout fichier échangé entre deux applications.

Le mode Messagerie

Par définition la Messagerie au sens MOM permet l'émission et la réception de messages entre applications, que ce soit dans le cadre d'une infrastructure locale ou étendue. L'échange doit pouvoir s'effectuer entre des équipements hétérogènes.

Le principe de ce type de mécanisme est celui du caractère ASYNCHRONE de la mise en relation de l'émetteur et du récepteur : un applicatif en mode messagerie demande un service à un serveur, mais ne se met pas en attente du résultat.

Le mode Services Web

Le mode web-service permet de répondre à des besoins d'échanges synchrones entre des applications potentiellement très hétérogènes. Le développement de ces interfaces peut être réalisé dans différents langages de programmation conformes au CCT.

CCT114	Il est OBLIGATOIRE de mettre en oeuvre tout échange inter-applicatif de données synchrone sous forme de web-service.

Échanges de données informatisés

EDI (acronyme anglais pour Electronic Data Interchange) est un transfert électronique de données structurées entre applications informatiques, au travers d'un réseau de télécommunication.

CCT115	Il est DÉCONSEILLÉ d'utiliser les technologies EDI.

Mise en œuvre au ministère de la Justice

Au niveau National, **le projet PFE (Plate-Forme d'Échange)** vise à prendre en charge tous les échanges inter-applicatifs internes ou avec l'extérieur du Ministère d'application à application.

Son objectif est de centraliser les échanges de données métier des applications, en servant d'intermédiaire unique pour tous les partenaires. Ainsi, quand une application veut émettre et/ou recevoir des informations avec un partenaire, la PFE est son seul interlocuteur. Ceci est valable aussi bien pour les entités externes, que pour celles appartenant au ministère. De cette manière, la PFE simplifie l'architecture du réseau justice en évitant la mise en place d'interconnexions spécifiques à chaque création d'un nouveau flux de données.

Il met en œuvre :

- le mode transfert de fichiers,
- le mode service web entre serveurs d'applications.

Pour plus de détail sur les possibilités de la PFE cf. document référencé [R06]

CCT116	Il est OBLIGATOIRE d'utiliser la PFE pour mettre en œuvre tout échange de données entre 2 applications.

CCT117	Il est INTERDIT de mettre des règles de transformations métiers dans la PFE.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
EAI / ESB/GATEWAY	Apache ServiceMix	5.5.x/6.x	Axway Synchrony (PFE)	
	WSO2	2.x		
MOM	ActiveMQ		Axway Synchrony	
Transfert de fichiers	SFTP avec filezilla		AXWAY CFT	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

5.3.5. Archivage

Description

Le système d'archivage permet la conservation dans un temps défini des données à valeur probante et/ou présentant un intérêt historique.

Le terme de « données » utilisé dans ce cadre est à comprendre dans son acception la plus large, il désigne aussi bien des données non-structurées, semi-structurées ou structurées, brutes ou agrégées, et cela, quels

que soient la nature, le format, le métier ou le sujet sur lesquels portent ces données, tel que défini par le code du patrimoine dans son article L211-1.

La conservation de ces données est assurée grâce à un dispositif organisationnel, fonctionnel et matériel qui autorise leur accès et leur restitution et ce, indépendamment des évolutions matérielles ou logicielles des applicatifs.

La conservation diffère de la sauvegarde informatique (backup) dans le sens où les données et documents devant être conservés ont été au préalable sélectionnés, contextualisés et décrits et que le dispositif de conservation est à même de garantir dans le temps long la valeur probante et la lisibilité de l'information.

Les données à pérenniser proviennent potentiellement de l'ensemble des systèmes producteurs de données ou de documents du ministère.

Cette mission d'archivage repose sur le ministère de la Justice durant la **D**urée d'**U**tilité **A**dministrative (**DUA**) des données et documents générés par ses services.

A échéance de cette DUA, en fonction du sort final à appliquer, les données ou documents sont soit :

- éliminés selon les processus en vigueur ;
- conservés définitivement par les **A**rchives **N**ationales (**AN**), rattachées au ministère de la Culture en charge de la conservation des archives historiques définitives pour les données produites en centrale, ou par les services d'**A**rchives **D**épartementaux (**AD**) pour les données produites par les juridictions et services déconcentrés de la justice.

La politique d'archivage

Les délais de conservation et les sorts finaux doivent être déterminés par accord entre les services producteurs et le **D**épartement des **A**rchives, de la **D**ocumentation et du **P**atrimoine (**DADP**), au regard des circulaires publiées par le **S**ervice **I**nterministériel des **A**rchives de **F**rance (**SIAF**) et des besoins du métier.

CCT118●	Il est OBLIGATOIRE de procéder à un pré-cadrage avec le DADP afin d'analyser le besoin portant sur le cycle de vie, le caractère personnel et la valeur patrimoniale des données générées.

Si le pré-cadrage indique une nécessité de versement des données au DADP, il est nécessaire de réaliser un cadrage afin de définir les exigences et de rédiger un contrat de service à appliquer.

CCT119●	Si le pré-cadrage le préconise, il est OBLIGATOIRE de procéder à un cadrage afin de définir un contrat de service et un contrat de versement des données générées ou gérées par le système.

Le versement des données

Les données doivent être versées par le système producteur conformément aux spécifications définies dans le contrat de versement.

En fonction du besoin lié à la valeur probante du document, le système pourra verser les données ou documents :

- à échéance de la **D**urée d'**U**tilité **C**ourante (**DUC** - durée pendant laquelle les données sont accédées de manière régulière, également dites « en stockage de production »)
- dès leur création. Dans ce cas les données sont à la fois versées au système d'archivage et stockées dans le système de production. Le système d'archivage assure dans ce cas la valeur probante et la lisibilité des informations durant l'ensemble du cycle de vie du document.

Le versement des données doit être réalisé avec leurs métadonnées métier, leurs métadonnées archivistiques et leurs données techniques liées via la PFE selon le protocole définit dans le contrat de versement.

Toute donnée versée dans le système d'archivage ne peut plus être modifiée, ni supprimée. Seule une nouvelle version de la donnée peut être archivée.

CCT120●	Il est INTERDIT de modifier une donnée archivée dans le système d'archivage.

Des procédures de vérification des versements par le DADP et par le système d'archivage permettent de s'assurer de l'intégrité des données transférées.

Formats

CCT121●	Il est RECOMMANDÉ d'utiliser un format pérenne* selon le type de donnée. Par exemple, le format PDF/A (Portable Document Format) de l'éditeur Adobe et normalisé par l'ISO (norme ISO 19005), pour la conservation des documents non structurés et semi-structurés.

* Un format pérenne est un format ouvert : les données sont interopérables, les spécifications techniques sont publiques, sans restriction d'accès ni de mise en œuvre.

CCT122●	Il est OBLIGATOIRE d'utiliser le format XML, pour les données à pérenniser et la transmission des méta données du document.

La modification des métadonnées

Les documents archivés ne peuvent plus être modifiés. Seules les métadonnées peuvent être modifiées ou ajoutées en fonction du contexte et si le contrat de service ou le contrat de versement l'autorisent et que la demande est justifiée.

La consultation des archives

La recherche et la consultation des archives ne peuvent pas être exécutées depuis un système automatisé. Pour des raisons de sécurité des archives et afin d'assurer la traçabilité de leur accès, seules des personnes ayant un accès nominatif direct au système d'archivage peuvent consulter les archives en fonction de leurs attributions.

CCT123●	Il est INTERDIT de consulter ou de rechercher des archives depuis un système autre que le système d'archivage.

L'élimination des données

Une fois la Durée d'Utilité Courante (DUC) ou la Durée d'Utilité Administrative (DUA) expirées, les données ne sont plus accessibles car elles sont éliminées ou transmises aux Archives Nationales (AN) ou aux services d'Archives Départementaux (AD).

Seuls les bordereaux relatifs à ces actions restent consultables.

5.3.6. Système de Stockage objet

Le Stockage Objet permet de gérer de très grands volumes de données non structurées. Il s'agit notamment de données rarement modifiées contrairement aux données dites transactionnelles constamment modifiées, comme celles contenues dans les bases de données.

Le principe d'un système de stockage objet est :

- une représentation classique de fichiers dans une arborescence de répertoires,
- et un niveau complémentaire : les métadonnées.

Chaque fichier est donc associé à des métadonnées et forme l'objet. Les métadonnées correspondent principalement à de l'information complémentaire à la donnée source.

Une photo, par exemple, accompagnée d'un descriptif est un objet:

- L'image est la donnée,
- La description précisant le contenu de la photo est la métadonnée.

Un objet est donc composé de :

- La donnée,
- Un identifiant unique (correspond au chemin d'accès de la donnée).
  L'utilisateur dispose donc **d'une base de référence unique** quel que soit l'endroit où se trouve son objet.
- Des métadonnées,
  Il s'agit des informations liées au contexte de l'objet comme le type de données (vidéo, fichier, etc...), sa structure, etc... Ces métadonnées permettent de faire le lien entre plusieurs objets qui comportent ces mêmes métadonnées.

Les avantages de ce système de stockage sont:

- Le coût :
  En comparaison les traditionnels systèmes de stockage NAS/SAN ne sont pas toujours adaptés d'un point de vue financier pour gérer de très grands volumes de données.
- Communication Client ↔ Système Stockage simplifié
  Généralement via des API de type RESTful (PUT/DELETE/POST/GET, etc..)
- Une scalabilité aisée :
  Pour le client intégrant ce système de stockage, cela est transparent (par le biais de la communication avec le système au travers d'APIs RESTful). Pour l'administration du système, il

suffit de gérer l'évolution, la capacité de stockage du système et d'ajouter des serveurs au fur et à mesure des besoins. Ces serveurs sont alors pris en compte de manière automatique sans remise en cause du système.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel/matériel	Version
Système de Stockage objet			Hitachi Content Platform (HCP)	8.1.x (08/2019)

Remarques :

Les profils types des projets susceptibles d'utiliser cette solution sont ceux réalisant du stockage de documents sans aspects GED avancés.

Les modalités d'utilisation du produit sont référencées en [R03].

5.4. SERVICES DE SÉCURITÉ

D'après l'article 2 de la Recommandation Interministérielle n° 901 du 2 mars 1994 : « est dénommé **sécurité d'un système d'information** l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer :

- la **confidentialité**, c'est-à-dire le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service;
- la **disponibilité**, qui est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances;
- **l'intégrité** du système et de l'information qui garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination. »

Afin d'assurer ces qualités de sécurité, les systèmes informatiques doivent être conçus et élaborés en intégrant différents services :

- **l'habilitation (ou contrôle d'accès) :** limiter à certains utilisateurs l'accès à certaines ressources (lecture, écriture, création, effacement, …).
- **l'authentification :** permettre de s'assurer que le demandeur identifié d'un service (fichier, programme, fonction, …) est bien celui qu'il prétend être.
- **la confidentialité :** permettre de rendre impossible à certains utilisateurs l'accès à certaines données (en lecture notamment).

- **la non-répudiation** : permettre à l'émetteur d'une information d'avoir la preuve de sa réception, ou, pour un destinataire, d'avoir la preuve de son émission.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Annuaire LDAP	389 Directory Server	1.4.x	Micosoft Active Directory	2012
Infrastructure de gestion des clés	EJBCA Community (de PrimeKey)	6.5.0.5		
Web SSO / reverse proxy	LemonLDAP::NG	1.4 (actuellement en production)		
Reverse proxy/LoadBalancer	Haproxy	1.8.x		
	NGINX	1.14.x		
Pare-feu			Projet PRIAM	
Antivirus			Projet PRIAM	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

5.4.1. Infrastructure de gestion des clés

Le rôle d'une IGC est de gérer des clés cryptographiques au profit d'une communauté d'utilisateurs qui les utilisent pour sécuriser des applications ou protéger le transport de données entre les serveurs ou/et les postes.

Un opérateur de certification a été sélectionné pour réaliser l'opération cryptographique pour le compte du ministère de la Justice. Il est chargé de la fourniture des cartes à puce, de la génération des certificats, de la personnalisation graphique des cartes, du stockage des certificats sur cartes à puce, et de la diffusion de ces cartes vers leurs destinataires.

Le Ministère possède une IGC « autosignée » pour tous les certificats serveurs et certains certificats clients.

Pour les sites publics sécurisés, le Ministère utilise des certificats signés par une autorité privée.

5.4.2. Fédération d'identité

La fédération d'identité vise à permettre à des sous-systèmes utilisant des référentiels d'identité différents de pouvoir partager un identifiant commun pour une identité sans pour autant permettre aux sous-systèmes d'effectuer des rapprochements de données.

A ce jour, le ministère de la Justice a mis en place un SSO ministériel basé sur l'annuaire LDAP du Ministère (389 Directory Server) et sur la solution libre LemonLDAP::NG afin de disposer d'un portail unique de connexion à ses applications.

Les nouvelles applications développées utilisent cette architecture, tandis que des études seront menées sur les applications déjà en exploitation afin d'y être intégrées.

Cette architecture supporte les systèmes à authentification forte.

L'authentification forte à base de certificats se base sur la mise en œuvre de l'IGC du Ministère.

Les accès au SI Justice par d'autres Ministères ou des partenaires sont réalisés par délégation d'authentification : les utilisateurs sont authentifiés sur le portail SSO de leur administration d'origine, auquel l'application « Justice » fait confiance.

L'interface entre le ministère de la Justice et les fournisseurs de service externes repose sur une infrastructure de fédération d'identité conforme au standard SAML V2.0. Cette infrastructure permet aux fournisseurs de service de réaliser la délégation d'authentification. Les demandes d'authentification et les informations d'identification des utilisateurs authentifiés étant échangées sous la forme d'assertions SAML au format XML.

5.4.3. Habilitation et gestion des profils

La gestion des profils et des rôles est réalisée dans l'application Pages Blanches.

cf. chapitre 3.10.4 Habilitations et profils

5.4.4. Chiffrement (canal, messages et stockage)

Chiffrement du canal

Il permet de se protéger des attaques sur les flux de communication.

CCT124	Il est RECOMMANDÉ d'utiliser le protocole HTTPS pour toute application intranet.

CCT125	Il est OBLIGATOIRE d'utiliser le protocole HTTPS pour protéger la phase d'authentification de toute application intranet.

Le chiffrement du canal n'est pas nécessairement mis en place de bout-en-bout. En effet, il n'est pas possible de mener des analyses de flux pour détecter des intrusions sur des flux chiffrés.

CCT126	Il est DÉCONSEILLÉ de chiffrer les flux à l'intérieur du centre de production.

Chiffrement des messages

Il permet de protéger les données envoyées sur un canal non protégé. Ceci peut être utile dans le cas d'envoi de données en utilisant un protocole non sécurisé (par exemple CFT).

Chiffrement du stockage

Il est destiné à se protéger des personnes ayant un accès à la base de données ou à ses sauvegardes. Un chiffrement des disques ou partitions, qui est transparent pour l'application, ne permet de se protéger que des vols de sauvegardes.

Un chiffrement plus efficace consiste à chiffrer les données sensibles dans la base de données. Ce dispositif peut être mis en place en faisant opérer les fonctions de chiffrement/déchiffrement par le serveur d'application, qui détient la clé.

Ce type de dispositif sous entend une segmentation organisationnelle dans l'accès aux serveurs : les administrateurs ayant accès aux clés de chiffrement ne doivent pas être les mêmes que les administrateurs de base de données.

De plus, ce type de chiffrement « en base » a des impacts non négligeables sur l'application, en particulier par rapport aux performances de recherche sur les données chiffrées.

5.4.5. Garantie de l'intégrité de l'information

La garantie de l'intégrité de l'information ne peut être efficace que par la mise en place de moyens cryptographiques basés sur la signature électronique des données, opérée par le système.

Dans le cadre d'échanges inter-applicatifs, la mise en place de solutions de garantie de l'intégrité de l'information doit notamment porter sur les deux critères suivants :

- l'authentification de l'expéditeur et du destinataire des données et la confirmation du non-interception du flux par un élément tiers, par la mise en place d'une solution de contrôle, par exemple en chiffrant les flux ou en contrôlant les adresses IP de l'expéditeur et du destinataire, cette liste n'étant pas exhaustive ;
- le contrôle de l'intégrité des données (complétude et absence de corruption de la source en cours de transfert), par la mise en place d'une solution de contrôle de l'empreinte de ces données.

CCT127	Il est RECOMMANDÉ de mettre en place des solutions garantissant l'intégrité de l'information dans le cadre d'échanges inter-applicatifs.

5.4.6. Signature et vérification de signature électronique

Dans le cadre du socle de confiance du ministère de la Justice, deux projets traitent de la signature électronique :

- Scorpion : coffre-fort électronique offrant un service de cachet serveur et un service de vérification de signature,
- Signa : services de signature et de vérification de signature électronique conforme eIDAS développé au sein du Ministère à partir du projet européen open source sd-dss. La mise à disponibilité de la solution signa est programmé pour fin 2018.

5.4.7. Service d'Horodatage

Un service d'horodatage permet d'attester qu'un objet numérique existe à un instant donné.

L'horodatage électronique consiste à apposer sur tous types de données numériques une heure et une date pouvant faire juridiquement foi sous la forme d'un jeton d'horodatage. Ce jeton d'horodatage garantit que les données horodatées existent à partir de la date et de l'heure certifiées, et qu'elles n'ont pas été modifiées depuis.

Au sein du Ministère, un service d'horodatage est disponible par le biais du projet Scorpion.

5.4.8. Coffre-fort numérique

Au sein du Ministère, le projet Scorpion met à disposition un Coffre-Fort Numérique (CFN) conforme à la norme NF Z42-020 offrant tous les niveaux de sécurité nécessaires à la conservation d'objets numériques dans des conditions de nature à en garantir leur intégrité dans le temps.

5.4.9. Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer les logiciels malveillants (dont les virus ne sont qu'un exemple).

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
PC (Windows 7/Windows 10) - protection virale			Projet PRIAM TrendMicro OfficeScan	 10.5 (win7) 12.0.5309 (win10)
PC (Windows 7/Windows 10) - décontamination virale			Projet PRIAM TrendMicro OfficeScan	 10.5 (win7) 12.0.5309 (win10)
Serveur Windows 2008/2012			Sophos	5.5.0
Serveur UNIX/Linux			Sophos	5.5.0
Serveurs de messagerie Exchange (Microsoft)			ScanMail (TrendMicro)	11

6. EXPLOITATION

Ce chapitre définit les outils et règles associés mis en oeuvre par les équipes d'exploitation afin d'assurer le bon fonctionnement des systèmes.

6.1. ADMINISTRATION

6.1.1. Sauvegardes

Description

La sauvegarde consiste à garder une copie consistante des différentes données vivantes d'une application. Les outils peuvent également être utilisé pour reconstruire complètement un serveur (disaster recovery).

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Sauvegarde de données (centre de production)			Tina	4.4
			Rman (oracle)	
Sauvegarde des données (windows)			Veritas Backup Exec	15

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

La sauvegarde des bases PostgreSQL s'effectue par dump de la base et peut être effectuée base ouverte et l'application opérationnelle.

La sauvegarde des bases Oracle transactionnelle s'effectue avec son utilitaire RMAN, base ouverte et application opérationnelle.

La sauvegarde des bases Oracle d'infocentre s'effectue par dump, base ouverte et application opérationnelle.

Les sauvegardes sont conçues dans l'optique de privilégier une restauration rapide et fiable. Les modes de sauvegarde/restauration sont le résultat d'une réflexion dans le cadre de chaque application en fonction de paramètres tels que la durée de perte de saisie acceptée. Les supports de sauvegarde doivent être impérativement stockés dans un coffre ignifuge ou externalisés.

CCT128	Il est RECOMMANDÉ de réaliser régulièrement des sauvegardes totales. Pour la base de données ces sauvegardes peuvent être réalisées « base ouverte ».

Les procédures de sauvegarde devront être modifiables afin de les aménager ou d'utiliser une solution transversale.

Les sauvegardes sont sous la responsabilité des administrateurs. Les supports changés quotidiennement, doivent être impérativement stockés dans un coffre ignifuge ou externalisés.

6.1.2. Gestion des logs

Description

Les outils de gestion des logs permettent de centraliser les journaux des serveurs et disposent de fonctionnalités facilitant la recherche.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Gestion de logs	Syslog-ng	Version disponible les distribs		

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.1.3. Création d'images / gestion de partitions

Description

Les logiciels de création d'images permettent d'obtenir une copie conforme d'un disque dur. Les outils de gestions de partitions permettent de retailler en fonction du besoin les partitions sur un disque.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Création d'images / gestion de partitions	Clonezilla		Ghost	

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

CCT129	Il est RECOMMANDÉ d'utiliser LVM (logical volume manager) ou une couche d'abstraction équivalente sur les partitions des serveurs UNIX ou LINUX.

6.1.4. Ordonnancement

Description

Les logiciels d'ordonnancement permettent de planifier l'exécution de batch sur différents serveurs (systèmes d'exploitation multiples), les tâches pouvant dépendre l'un de l'autre.

CCT130	Il est OBLIGATOIRE d'utiliser les logiciels d'ordonnancement en vigueur en centre de production pour planifier l'exécution des batchs.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Ordonnancement mono serveur			planificateur de tâches windows	
Ordonnancement multi-serveur			VTom (Abyss)	5.6

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.1.5. Télédistribution

Description

Les logiciels de télédistribution permettent de déployer automatiquement de nouveaux logiciels, leurs mises à jour ou de nouvelles configurations sur des postes de travail ou des serveurs.

Selon la cible (logiciel Microsoft, poste de travail, serveur windows, serveur linux), les solutions utilisées à ce jour au ministère de la Justice sont différentes.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Télédistribution des correctifs Microsoft poste de travail et serveur			WSUS (correctifs système)	2012
Télédistribution autres logiciels	OCS Inventory *(**)*	2.1.x	GPO d'Active Directory	
			LANDESK	
			SCCM	6.1.5

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

*(**) - en cours de qualification*

6.1.6. Prise de contrôle à distance

Description

Compte tenu de la nature de ces produits, ceux-ci ne doivent être utilisés que dans le cadre de la maintenance des postes de travail et des serveurs. Ils doivent être installés, configurés et utilisés (pour ce qui est de leur fonctionnalité de prise de contrôle à distance) par les équipes informatiques compétentes en respectant les règles de sécurité (filtrage sur les firewall ou les routeurs, activation/désactivation à chaque intervention, prise de contrôle sur l'initiative de l'utilisateur, contrôle téléphonique au cours de l'intervention ...).

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Prise de main à distance			Terminal server SCCM	6.1.5
	ssh			

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.1.7. Gestion de parc

Description

Les logiciels de gestion de parc permettent d'avoir une vision d'ensemble de la configuration logicielle et matérielle du parc de poste de travail et/ou de serveur.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Gestion de parc	GLPI	0.85.x	EasyVista	2016
Inventaire du parc	OCS Inventory	2.1.x		

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.1.8. Gestion des incidents

Description

Les outils de gestion des incidents permettent d'enregistrer et d'opérer le suivi des incidents survenant sur le SI (incident applicatif, incident matériel) à travers plusieurs niveaux de support.

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Gestion des incidents applicatifs	Mantis	2.4.x		
			Jira	7.8.x
Gestion des incidents matériel			Application GSI (logiciel EasyVista)	2016

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.1.9. Mise à jour des applications

Les fichiers permettant d'installer les applications dans les centres de production doivent respecter une certaine norme de paquetage. Cette norme est définie dans le document [A09].

6.2. EXPLOITABILITÉ

Les règles suivantes permettent d'améliorer l'exploitabilité des applications :

Indépendance vis à vis des évolutions

Le déploiement d'une version d'une application nationale est nécessairement progressif, nécessitant donc la cohabitation avec les versions précédentes de cette même application. Les applications doivent pouvoir s'interfacer avec leur version précédente, en particulier lors des échanges inter sites.

CCT131	Il est RECOMMANDÉ, dans la mesure du possible, que les applications puissent s'interfacer avec leur version précédente, en particulier lors des échanges inter sites.

Placer toutes les données persistantes dans la base de données de l'application

Ce point est important pour ne pas trop compliquer les procédures d'administration et d'exploitation, notamment lors d'une reprise ou d'un redéploiement de l'application.

CCT132	Il est RECOMMANDÉ de placer toutes les données persistantes dans la base de données de l'application.

Indépendance vis à vis des adaptations locales

Il faut veiller à ce que les adaptations locales ne risquent pas d'introduire d'incohérence par rapport aux paramètres nationaux.

Réciproquement, les adaptations locales ne doivent pas être impactées lors de la diffusion d'une nouvelle version de l'application ou d'une mise à jour des tables nationales.

Interface avec la supervision de système

Pour permettre une supervision à distance, les applications doivent tenir à jour un fichier journal (log), compatible avec l'environnement de supervision de système.

CCT133	Il est OBLIGATOIRE que les applications tiennent à jour un fichier journal (log) compatible avec l'environnement de supervision de système.

Sécurité et Gestion des habilitations

Il est nécessaire, pour ne pas introduire de faille dans le système de sécurité, de prendre quelques mesures techniques au sein des applications pour éviter par exemple qu'elles n'emploient des comptes de niveau administrateur (i.e. root sous UNIX) ou qu'elles ne stockent des mots de passe en clair.

Gestion des modes dégradés et des reprises

Afin de faciliter la reprise, éventuellement sur une autre machine ou un autre site, les applications ne doivent pas conserver d'information relative à leur implantation physique à un moment donné (numéro de machine, adresse IP, ...).

6.3. SUPERVISION

6.3.1. Supervision technique

Description

La supervision technique des systèmes consiste à garder une trace de l'activité des systèmes de façon à faciliter le diagnostique en cas d'anomalie. La plupart des systèmes de supervision permettent de faire des notifications automatiques en cas d'alerte.

La supervision technique peut inclure des tests matériels et des tests logiciels.

Ces outils sont utilisés de manière réactive (réaction au plus vite en cas d'incident) et préventive (mise en place d'un plan d'action en cas de dépassement d'un seuil d'alerte non critique, avant que les utilisateurs en subissent les conséquences).

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Supervision	Centreon	18.10.x		

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

6.3.2. Supervision applicative

Description

La supervision applicative permet principalement de mesurer la performance des applications de façon à connaître le ressenti utilisateur. Ces outils sont utiles :

- pour la gestion des incidents : les équipes techniques peuvent être alertées d'un ralentissement, pas uniquement pendant les heures de travail des utilisateurs
- de façon préventive : ils permettent d'avoir un suivi des performances sur le long terme. On peut ainsi connaître l'effet sur les temps de réponses d'une augmentation du nombre d'utilisateurs, par exemple.

Produits / composants

A ce jour, la supervision applicative n'est pas mise en œuvre de manière systématique au sein du Ministère. Néanmoins pour certaines applications web, l'outil JMeter (ordonnancé par VTOM) est utilisé pour répondre à ce besoin.

6.4. CAPACITY PLANNING

Description

Le « capacity planning » est l'élaboration des tendances d'utilisation d'une application ou d'un système, en vue de prévoir un besoin de mise à niveau. Le principe est de deviner à quel moment le système sera saturer en fonction des remontées de sondes actuelles et passées.

Produits / composants

Aucun produit dédié n'est préconisé dans ce CCT. L'utilisation conjointe de la supervision technique et applicative permet d'avoir un premier niveau de visibilité sur les saturations futures d'un système.

6.5. HÉBERGEMENT (SERVICES DÉCONCENTRÉS)

Description

Ce chapitre détaille les modalités d'hébergement des sites et applications webs des services déconcentrés.

Produits / composants

Les services déconcentrés ont le choix entre deux modes d'hébergement :

- national (sur *,justice.gouv.fr)
- local.

Hébergement sur le site national :

En cas d'externalisation de la réalisation du site, il convient de fixer les contraintes techniques au prestataire sous la forme d'une annexe au CCTP sachant que les serveurs qui supportent actuellement le dispositif ont les caractéristiques suivantes :

- Serveur sous Linux Red Hat ; serveur HTTP : Apache intègrant la gestion de Perl, PHP ainsi que l'interface CGI
- L'URL du site pourra être normalisée (ex : www.<typejuridication>.justice.fr/<ville>).

Hébergement régional local :

La plupart des fournisseurs d'accès proposent un service d'hébergement de pages Web ou de serveur.

CCT134	Il est RECOMMANDÉ de faire héberger tout site web à destination du grand public par la Chancellerie.

6.6. SUPPORT/TÉLÉMAINTENANCE

Le support est une activité essentielle dans le cadre de l'amélioration permanente de la qualité du système d'information justice et dans sa perception par l'utilisateur.

Cette activité nécessite dans certains cas la possibilité pour un technicien d'accéder au serveur ou au poste de travail sur lequel son intervention est requise. Or, les coûts et délais associés à des interventions physiques posent problème dans un contexte de très fort éclatement géographique et d'absence fréquente de compétence technique sur place.

La télémaintenance constitue donc un facteur de progrès, sous la réserve expresse d'être mise en place dans des conditions techniques compatibles avec le maintien d'un niveau adéquat de sécurité, en application des directives du fonctionnaire de sécurité des systèmes d'information.

Utilisation du RPVJ

Le RPVJ constitue le réseau national de transmission de données du ministère de la Justice. Il constitue donc le réseau de référence pour l'ensemble des opérations de télémaintenance, en particulier lorsque ces opérations sont conduites à partir de ressources internes.

Du côté site télémaintenu, l'accès RPVJ doit être impérativement un accès permanent au minimum de type ADSL (ou à la rigueur SRL si le site n'est pas éligible à l'ADSL).

Le RPVJ ne peut toutefois pas être utilisé lorsque les équipes chargées des opérations de télémaintenance sont physiquement localisées dans des locaux ne relevant pas du ministère de la Justice.

Sécurisation des opérations de télémaintenance

Les opérations de télémaintenance réalisées sur des systèmes d'information reliés ou non au RPVJ par les équipes internes au Ministère comme par les prestataires externes doivent être sécurisées de telle sorte à :

- identifier et authentifier l'équipe opérant, voire l'agent opérant,
- chiffrer les échanges en cas d'accès à des informations très sensibles,
- restreindre les possibilités d'accès à une liste limitative de machines, en rapport avec l'équipe,
- pourvoir faire l'objet d'un contrôle a posteriori par l'administration.

CCT135	Il est OBLIGATOIRE de définir le périmètre des opérations de télémaintenance laissées aux prestataires en précisant leurs obligations en termes d'engagement de service, de protection des données et de confidentialité.

CCT136	Il est OBLIGATOIRE que les serveurs en télémaintenance soient correctement paramétrés pour ne pas autoriser de rebond sur le RPVJ. Un audit de sécurité doit systématiquement valider la procédure.

Portail d'accès sécurisé internet/RPVJ

CCT137	Il est OBLIGATOIRE d'utiliser, pour tout accès au RPVJ depuis Internet, un portail sécurisé de type extranet, avec un accès restreint après authentification.

Connexion directe RTC ou RNIS

CCT138	Il est INTERDIT que les équipements télé-maintenus en RTC ou RNIS soient inter-connectés, directement ou indirectement, au RPVJ. Ce type de solution doit progressivement migrer vers l'utilisation du portail sécurisé.

7. DESCRIPTION DES ENVIRONNEMENTS

Ce chapitre vise à décrire les différents environnements techniques utilisés au ministère de la Justice.

Les environnements sont décrits dans le cadre de référence de la méthodologie transverse de la démarche de tests du Ministère de la Justice (cf. document référencé [R09]).

8. CADRE DE DÉVELOPPEMENT

8.1. RÈGLES DE MISE EN ŒUVRE

Une bonne répartition des données et des traitements au sein de l'architecture des applications se traduit par une moindre charge du réseau, des serveurs et des postes de travail. L'exploitation de l'application est également plus simple lorsque la problématique de l'exploitant a été prise en compte dans les choix de répartition.

Aujourd'hui, les problématiques les plus critiques pour le ministère de la Justice sont incontestablement :

- le coût et la rareté des ressources réseaux,
- le coût et la rareté des ressources humaines d'exploitation des serveurs.

Dans ce contexte, les équipes de développement se doivent de privilégier ces deux problématiques dans leurs arbitrages internes.

8.2. RÈGLES GÉNÉRALES DE CONCEPTION DE L'ARCHITECTURE DE L'APPLICATION

Élaborer une architecture technique par couches (organisationnelle, logique, physique)

Toute solution de répartition données/traitements doit être étayée par la traduction de besoins des utilisateurs finaux et des exploitants.

Tenir compte des impacts en matière de déploiement, mise en œuvre, migration, formation

Les comparaisons de solutions d'architecture concernant la localisation des données, de leurs accès et des traitements doivent faire apparaître les impacts en matière de déploiement, administration, sécurité, production, exploitation, migration, formation.

Les traitements par lots (batch) sont toujours à prendre en compte dans l'évaluation de la solution technique : moyens de surveillance et d'exploitation, plages d'exploitation, quantification des serveurs. Toutefois, dans le cadre de nouveaux développements, ces traitements doivent, chaque fois que cela est techniquement possible à un coût raisonnable, pouvoir s'effectuer « base ouverte » : le système d'information justice doit rester, à terme, permanent.

Ne pas chercher à synchroniser plus de deux niveaux organisationnels en synchrone ou différé court

Il est souvent difficile de synchroniser de manière fiable et simple des bases de données distantes, surtout si des informations y sont redondantes.

On privilégiera les solutions de type « échanges asynchrones par lot » pour réaliser les échanges de données entre applications, de préférence à des solutions débouchant sur un besoin de synchronisation fort entre serveurs, ou entre applications.

On recherchera des solutions robustes, préservant notamment l'intégrité des données, si plusieurs bases de données doivent être mises à jour au sein d'une même transaction (moniteur transactionnel ou commit à deux phases).

CCT139	Il est OBLIGATOIRE pour les applications de s'appuyer sur le socle technique des postes de travail défini dans le présent document (cf. chapitre 4.1 Socles des applications)

CCT140	Il est OBLIGATOIRE pour les applications de s'appuyer, autant que possible, sur les services mutualisés disponibles dans le système d'information Justice définis dans le présent document (cf. chapitre 4.2 Services applicatifs)

8.3. ARCHITECTURES « CLIENT LÉGER » ET « CLIENT RICHE »

Le client léger résulte d'une architecture logicielle où les traitements sont exécutés le plus possible sur le serveur, et où le poste client ne se charge que de la présentation des informations et des traitements de surface.

Les applications nationales privilégieront une architecture logicielle à base de « client léger » ou de « client riche ».

CCT141	Il est OBLIGATOIRE de développer les applications « client léger » ou « client riche » qui doivent se conformer au standard HTML5 défini par le W3C et pouvoir fonctionner à minima avec Microsoft Internet Explorer, Microsoft Edge et Mozilla Firefox. Elles n'utiliseront donc aucune des fonctions spécifiques à l'un ou l'autre des navigateurs.

Les « clients riches » permettent :

- d'obtenir une IHM réactive offrant un confort d'utilisation et une réactivité proche des applications « client lourd »
- de limiter les échanges entre le navigateur de l'usager et les frontaux Web dans la mesure où :
  - l'IHM est téléchargée la première fois puis mise en cache dans le navigateur
  - seules les données sont échangées.

CCT142	Il est RECOMMANDÉ, pour les IHM « client léger » et « client riche » AJAX de réaliser les contrôles de surface en Javascript au niveau du Navigateur (sous réserve de respecter les contraintes d'accessibilité).

CCT143	Il est OBLIGATOIRE que tous les contrôles réalisés (en JavaScript) sur le client soient vérifiés sur le serveur lors des appels de services.

Il est préférable d'avoir une approche de conception Web qui vise à l'élaboration de sites offrant une expérience de lecture et de navigation optimales pour l'utilisateur quelle que soit sa gamme d'appareil (téléphones mobiles, tablettes, liseuses, écrans d'ordinateur, ...).

Une expérience utilisateur réussie implique un minimum de redimensionnement (zoom), de recadrage, et de défilements multidirectionnels de pages.

Pour répondre à un ce type de besoin, on pourra utiliser des techniques de type « responsive design » ou « adaptive design » par exemple.

CCT144	Il est RECOMMANDÉ de concevoir une application web ayant des IHM et une ergonomie capables de s'adapter aux différents supports utilisateurs (pc, tablette, smartphone, etc..).

CCT145	Il est OBLIGATOIRE, dans une optique de montée en charge, de positionner des verrous fonctionnels, s'ils sont utiles, au niveau de la base de données, plutôt qu'au niveau des serveurs d'applications.

CCT146	Il est OBLIGATOIRE, que toute utilisation de Javascript soit compatible au minimum avec Microsoft Internet Explorer, Microsoft Edge et Mozilla Firefox.

CCT147	Il est INTERDIT de développer des applications web nécessitant l'utilisation de plug-ins.

8.4. OUTILS DE CONCEPTION D'APPLICATION

Description

Les outils de conception d'application sont les suivants **:**

- les outils de conception : ces outils permettent la spécification fonctionnelle et la conception technique des applications ;
- les langages et outils de développement : ces services permettent le développement des applications de production ou d'infocentre ;
- les bibliothèques : ces services assurent le regroupement, le classement et la gestion des différentes briques logicielles utilisées ;
- les services de documentation : ils permettent la création et la maintenance (automatique ou manuelle) de la documentation des développements d'applications tout au long de leur cycle de vie ;
- les outils de tests : ces services regroupent l'outillage logiciel utilisé lors des tests unitaires, d'intégration, de non-régression ou de montée en charge ;
- les services de gestion des versions des composants logiciels : ces services permettent le suivi des versions des différents modules.

CCT148	Il est OBLIGATOIRE, pour modéliser les applications, que les outils de conception et de modélisation s'appuient sur UML (Unified Modeling Language).

CCT149	Il est OBLIGATOIRE de créer toute nouvelle application dans le référentiel d'urbanisation du ministère de la Justice (MEGA/URBI)

CCT150	Il est OBLIGATOIRE de renseigner le code ministériel (trigramme) de toute application dans le référentiel d'urbanisation du ministère de la Justice (MEGA/URBI)

Le code ministériel de l'application (trigramme) est notamment utilisé pour nommer de manière homogène des serveurs physiques et/ou virtuels du ministère afin de garantir l'unicité de nom.

CCT151	Il est RECOMMANDÉ de procéder à une analyse fonctionnelle et applicative avant de procéder à la conception technique. Le résultat de l'analyse fonctionnelle doit être reportée dans le référentiel d'urbanisation du ministère de la Justice (MEGA/URBI)

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	**Version**	**Logiciel**	**Version**
Outil de modélisation de processus / cartographie			MEGA Hopex	V2R1
Outil de modélisation	PolarSys Capella Papyrus Modelio	1.1.2 4.0.0 3.7.1	Sparx Enterprise Architect	14.x
Outils de développement Java	Eclipse	Photon		
Gestion de version	Git	2.x		
	Subversion	1.9.x		
Tests unitaires	JUnit	5		
Automatisation des tests Web	Selenium	3.6		
Gestion des campagnes de tests	Squash TM	1.19.x		
Gestion des anomalies	Mantis	2.4.x		
			Jira	7.8.x
Intégration continue	Maven	3.5.x		
Qualimétrie	SonarQube	6.x 6.7.x(LTS)	CAST AIP	8.2.x +
Métrologie	NetData (linux) wmi-exporter (win)	1.13.0 0.7.0		
	Prometheus	2.8.x		
Tests de charge	JMeter	3.3+		

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

8.4.1. Génération de code

Les outils de génération de code permettent, à partir d'un modèle, de générer tout ou partie du code source de l'application cible. Selon la méthode ou les produits utilisés, les modèles comprennent des schémas UML complétés par d'autres type de modélisation (pour les règles de gestion, par exemple).

Ce type d'approche (MDA : model driven architecture) est souvent mise en avant comme une source d 'économie importante.

Toutefois, son utilisation induit un certain nombre de difficultés qu'il ne faut pas négliger :

- la conformité du modèle aux normes (UML ...)
- la portabilité du modèle : un modèle utilisé par un générateur de code ne sera pas ré-utilisable avec un autre
- les coûts de licence du générateur de code, souvent assez élevés
- la maintenabilité du code sans générateur : le code généré automatiquement est bien souvent in-maintenable sans l'outil
- la pérennité du générateur de code : l'éditeur du générateur peut à tout moment cesser de maintenir telle version de JAVA ou PHP

En conséquence, l'utilisation de générateurs de code doit se faire avec la plus grande prudence.

CCT152	Il est OBLIGATOIRE, avant toute mise en œuvre d'outils ou de mécanismes de génération de code d'obtenir la validation formelle de la SSIC/SDIDE/ETD/APT.

CCT153	Il est INTERDIT de faire réaliser une application à partir d'un générateur de code sans que le Ministère en ai acquis les droits d'usage, lui permettant de maintenir le logiciel.

8.5. PERFORMANCE DES APPLICATIONS

Le développement des applications doit être fait en prenant en compte les aspects performance et montée en charge. Dans le contexte actuel où de nombreuses couches d'abstraction facilitent les développements et masquent la complexité, il est d'autant plus important de porter une attention particulière à l'implémentation physique des traitements et des données.

A ce titre, on portera donc une attention particulière que la bonne utilisation des index et l'adéquation du schéma de base de données au besoin.

Afin de vérifier les performances, des tests de montée en charge sont à effectuer avant toute mise en production. Un modèle de rapport de tests de montée en charge, ainsi qu'un appui méthodologique est fourni par le bureau SSIC/SDIDE/ETD/APT.

CCT154	Il est OBLIGATOIRE de mener des tests de montée en charge sur toute application nationale avant sa mise en production.

Ces tests de montée en charge doivent en particulier:

- Les campagnes de tests de performance doivent être intégrées à la phase de cadrage du projet.
- être représentatifs de l'activité en pic de l'application
- être effectué avec l'outillage préconisé par le Ministère, afin de faciliter la réutilisation des scénarios
- être effectué sur une base de données chargée

Avant la mise en production initiale, les tests de performance sont effectués sur l'environnement de production et sur l'environnement de préproduction. Ceci permet de déterminer un ratio entre ces 2 environnements. Pour les mises en production suivantes, les tests de performance sont réalisés uniquement sur l'environnement de preproduction.

8.6. QUALITÉ DU CODE

Qu'il s'agisse de développement ou de maintenance, l'évaluation de la qualité de la prestation passe par celle du code source de l'application. Celui-ci est mesuré grâce aux critères de conformité à la norme ISO 25023 (ou équivalent) et des bonnes pratiques techniques (normes ou usages du marché).

Le Ministère se réserve la possibilité d'effectuer ou de faire effectuer tous les contrôles et audits qu'il estime nécessaires concernant la qualité du code et sa conformité aux normes et standards en vigueur.

CCT155	Il est RECOMMANDÉ pour tout projet de mettre en place un système de contrôle de qualité de code

Produits / composants

Solution	Open source		Propriétaire (*)	
	Logiciel	Version	Logiciel	Version
Qualimétrie	SonarQube (pmd, findbugs, checkstyle)	6.x 6.7.x(LTS)	Cast AIP	8.2.x +

(*) : cf . CCT14 - Il est OBLIGATOIRE de justifier le choix de produit propriétaire par une analyse de la valeur démontrant son avantage par rapport à une solution open source.

8.7. MATRICE D'EXPRESSION DE BESOINS SÉCURITÉ

La matrice suivante permet à la maîtrise d'ouvrage à déterminer le niveau de sensibilité des informations et à définir leurs besoins de sécurité afin de formaliser son expression de besoins en termes de sécurité et de disponibilité de l'application ou du service. (cf. PMDS document [A10])

	Confidentialité	Authentification	Intégrité	Traçabilité	Disponibilité
0	**Faible ou nul**	**Faible**	**Faible**	**Faible ou nul**	**Faible**
	L'élément essentiel peut être rendu public.	Les personnes accédant à l'élément essentiel n'ont pas besoin de prouver leur identité	L'élément essentiel peut ne pas être intègre.	Aucun besoin de traçabilité.	L'élément essentiel peut être indisponible pour une longue période.
1	**Restreint**	**Authentification simple**	**Intégrité vérifiable**	**Besoin pour information**	**Disponibilité sous quelques jours**
	L'accès à l'élément essentiel est restreint aux personnels ou processus internes autorisés de par leur fonction ou de par leur appartenance à une entité organisationnelle.	Les personnes accédant à l'élément essentiel doivent donner une preuve* de leur identité	Besoin de détection du caractère intègre ou non-intègre de l'élément essentiel, sans correction nécessaire.	Besoin de traçabilité pour information, avec enregistrement éventuel d'une trace (non nécessairement détaillée).	L'élément essentiel doit être disponible sous quelques jours.
2	**Confidentiel**		**Intégrité corrigible**	**Besoin de traçabilité systématique**	**Disponibilité dans la journée**
	L'accès à l'élément essentiel est restreint aux personnels ou processus internes autorisés par leur fonction ou par leur appartenance à une entité organisationnelle et qui par ailleurs ont le besoin d'en connaître.		Besoin de détection du caractère intègre ou non intègre de l'élément essentiel avec correction requise si besoin.	Besoin de traçabilité pour information, avec enregistrement systématique d'une trace détaillée (ex : besoin commercial ou de facturation).	L'élément essentiel doit être disponible dans la journée aux personnes qui ont le besoin d'en disposer.
3	**Secret**	**Forte**	**Intégrité totale**	**Traçabilité légale**	**Disponibilité sans délai**
	Accès strictement restreint aux seuls personnels nommément désignés par la loi ou un règlement.	Les personnes accédant à l'élément essentiel doivent donner au moins deux preuves* de leur identité	L'intégrité de l'élément essentiel doit être totale aussi bien pendant sa période d'utilisation qu'ultérieurement (ex: archivage légal ou opérationnel).	Besoin légal de traçabilité avec enregistrement systématique de trace comme élément de preuve indiscutable.	L'élément essentiel doit être disponible sans délai aux personnes qui ont le besoin d'en disposer.

* Une preuve peut-être « ce qu'on sait » (mot de passe ...), « ce qu'on possède » (certificat électronique, token, passeport...), « ce qu'on est » (biométrie...), « ce qu'on sait faire » (signature ...)

9. ANNEXES

9.1. GLOSSAIRE

Terme	Description / définition
Active Directory	Service d'annuaire de Microsoft
Agilité	
AJAX	Asynchrone Javascript And XML
AOS	Architecture Orientée Services. Cf. SOA.
AOP	Aspect Oriented Programing. Cf. POA
ARCHIMED	ARCHItecture Mutualisée d'EDitique
Bande passante	La bande passante représente le débit des réseaux et se mesure en kilobits (Kb) par seconde, en mégabits (Mb) par seconde ou en gigabits (Gb) par seconde.
Batch	On appelle traitements batch les traitements par lot qui s'exécutent en tâche de fond, par opposition aux traitements intéractifs.
BAPT	Bureau des Architectures et des Projets Transverses
CCT	Cadre de Cohérence Technique
Chaîne fonctionnelle SSI	Groupe d'agents ayant collectivement la responsabilité de la sécurité du système d'information du Ministère et tenus au devoir de discrétion professionnelle, voire de secret professionnel selon leur rôle individuel : • Administrateur système et réseau ; • Correspondants de sécurité des systèmes d'information ; • Responsable de la sécurité des systèmes d'information (RSSI) ; • Autorité qualifiée de sécurité des systèmes d'information(AQSSI) ; • Fonctionnaire de la Sécurité des Systèmes d'Informations (FSSI)
CHAP	Challenge Hash Authentication Protocol
Client	Dans une architecture client-serveur, le client est celui qui est à l'initiative des requêtes faites au serveur.
Client « léger »	On parle de client léger lorsque le client ne prend en charge que la présentation des données transmises par le serveur. Mis à part quelques contrôles de surface, toute l'intelligence métier se trouve sur le serveur.
Client « lourd »	Par opposition au client léger, le client lourd prend en charge une bonne partie (voire toute) l'intelligence « métier » de l'application; le serveur pouvant être limité au stockage des données.
Client « riche »	Un client riche est un client léger doté de fonctionnalités ergonomiques avancées.
Cluster	*Cluster* (grappe) : plusieurs systèmes sont interconnectés soit pour augmenter la puissance de calcul (on parle alors de cluster de performance), soit pour offrir une tolérance de pannes accrue par la redondance des composants unitaires (on parle alors de cluster de haute disponibilité). Dans les deux cas, pour bénéficier de l'architecture en grappe, il faut que les applications aient été conçues en conséquence ou que le système d'exploitation, le compilateur et les logiciels sous-jacents (bases de données, middlewares, etc.) prennent en charge les fonctions adéquates de parallélisation des traitements ou de reprise sur incident.
Contention de ressources	Concept général dans les communications et l'informatique. Se produit lorsque des utilisateurs/applications essayent d'accéder à une même ressource au même moment.
CSS	Cascading Style Sheets : un langage de feuille de style qui permet aux auteurs et aux lecteurs de lier du style (ex. les polices de caractères, l'espacement et un signal auditif) aux documents structurés (ex. documents HTML et applications XML). En séparant la présentation du style du contenu des documents, CSS simplifie l'édition pour le Web et la maintenance d'un site.
DINSIC	Direction Interministérielle du Numérique et du Système d'Information et de la Communication de l'État (placée sous l'autorité du ministre chargée du numérique).
DITP	Direction Interministérielle de la Transformation Publique (placée sous l'autorité du ministre de l'Action et des Comptes publics, chargée de la réforme de l'État).
DNS	Les serveurs de noms de domaines (*Domain Name Servers* en anglais), sont en charge d'établir en un temps très court, la correspondance entre le nom de domaine (forme textuelle) et l'adresse IP (Internet Protocol) numérique du serveur qui supporte le service recherché.

EBIOS	La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) développée par la DCSSI permet de traiter les risques SSI. Elle est compatible avec les normes ISO 13335 (GMITS), ISO 15408 (critères communs) et ISO 17799. Contrairement aux approches d'analyse des risques par scénarios, EBIOS permet d'identifier les éléments de risques (entités et vulnérabilités, méthodes d'attaques et éléments menaçants, éléments essentiels et besoins de sécurité...) et vise l'exhaustivité de l'analyse.
Équilibrage de charge	L'équilibrage de charge (*Load Balancing*, en anglais, aussi appelé répartition de charge) consiste à distribuer une tâche à un ensemble de machines ou de périphériques afin de répartir la charge globale vers les différents équipements et de s'assurer de la disponibilité des équipements, en n'envoyant des données qu'aux équipements en mesure de répondre, voire à ceux offrant le meilleur temps de réponse. Ce mécanisme s'appuie généralement sur un équipement matériel, appelé répartiteur de charge.
Groupware	Logiciel de groupe de travail
EJB	Enterprise Java Beans
ETD	Département de la SDIDE : ÉTudes et Développements
ETL	Extract Transform Load : outil permettant le chargement et la transformation de données dans une base de données.
Framework	Un framework est un ensemble de bibliothèques permettant le développement rapide d'applications. Il fournit suffisamment de briques logicielles pour pouvoir produire une application aboutie. Ces composants sont organisés pour être utilisés en interaction les uns avec les autres. Ils sont en principe spécialisés pour un type d'application. Les principaux avantages de ces frameworks sont la réutilisation de leur code, la standardisation du cycle de vie du logiciel (spécification, développement, maintenance, évolution), ils permettent de formaliser une architecture adaptée au besoin de l'entreprise.
FSSI	Fonctionnaire de la Sécurité des Systèmes d'Informations
Goulet d'étranglement	Un goulet d'étranglement est un point d'un système limitant les performances globales, et pouvant avoir un effet sur les temps de traitement et de réponse. Les goulets d'étranglement peuvent être matériels et/ou logiciels.
GPL	General public Licence : type de licence de logiciel libre
HTML	Hyper Text Markup Language : un standard de description de documents incluant des balises hypertextes. **La version 5** de HTML est « recommandée ». La version 5.1 peut être considérée d'ores et déjà « en observation ».
HFDS	Haut-Fonctionnaire de Défense et de Sécurité
IHM	Interface Homme Machine
Interopérabilité	On entend par interopérabilité la capacité à rendre compatibles deux systèmes quelconques. L'interopérabilité nécessite que les informations nécessaires à sa mise en œuvre soient disponibles sous la forme de standards ouverts.
IoC	Inversion Of Control. Il s'agit d'un Design Pattern de programmation objet dans lequel le framework prend en charge l'exécution principale du programme ; il coordonne et contrôle l'activité de l'application.
IP	IP (Internet Protocole) est un protocole prenant en compte l'adressage des machines dans le réseau (mise en forme des données et routage des paquets).
Java EE	Java Enterprise Edition
LAD	Lecture automatique de documents
LAMP	Linux Apache MySQL PHP
Libre	Un logiciel libre est un logiciel dont la licence dite libre donne à chacun (et sans contrepartie) le droit d'utiliser, d'étudier, de modifier, de dupliquer, et de diffuser (donner et vendre) le dit logiciel. La notion de logiciel libre ne doit se confondre ni avec celle de logiciel gratuit (freewares ou gratuiciels), ni avec celle de sharewares, ni avec celle de domaine public.
Linux	Linux ou GNU/Linux est un système d'exploitation Open source compatible POSIX.

Logiciel libre	Un logiciel libre est un logiciel dont la licence dite libre donne à chacun le droit d'utiliser, d'étudier, de modifier, de dupliquer, de donner et de vendre le dit logiciel sans contrepartie. La notion de logiciel libre ne doit se confondre ni avec celle de logiciel gratuit (freewares ou graticiels), ni avec celle de sharewares, ni avec celle de domaine public. De même, les libertés définies par un logiciel libre sont bien plus étendues que le simple accès au code-source, ce qu'on appelle souvent logiciel Open Source ou « à sources ouvertes ». Toutefois, la notion formelle de logiciel Open Source telle qu'elle est définie par l'Open Source Initiative est reconnue comme techniquement comparable au logiciel libre.
NAS	*Network Attached Storage* : système de stockage connectable directement sur le réseau local et utilisable, en principe, par tous les serveurs et postes de travail de ce même réseau. Un serveur NAS n'est autre qu'un serveur de fichiers. Le terme de NAS est remis au goût du jour par l'arrivée des systèmes de stockage de type SAN. L'administration de ces serveurs se fait généralement au travers d'une interface Web.
ODS	Operational Data Store : base de données de travail dans laquelle sont stockées les données d'alimentation d'un infocentre.
Open Source	La désignation Open Source (source ouverte en français) s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire la possibilité de libre redistribution, d'accès au code source, et de travaux dérivés. On qualifie souvent un logiciel libre d'Open Source, car les licences compatibles Open Source englobent les licences libres selon la définition de la FSF (Free Software Foundation). Le terme Open Source est en concurrence avec le terme Free Software recommandé par la FSF. Le terme Freeware (graticiel) désigne des logiciels gratuits qui ne sont ni nécessairement ouverts, ni libres.
Ouvert	Voir « open source »
Pérennité	On parle de pérennité d'un logiciel libre pour désigner la faculté de la communauté ou de la société qui le publie à en garantir la maintenance dans la durée.
Point de contention	Cf. SPOC
PMDS	Politique Ministérielle de Défense et de Sécurité. Elle intègre la PSSI, et fait foi au sein du ministère de la justice concernant les aspects sécurité
PPP	Le protocole PPP (Point to Point Protocol) est un protocole « standard » d'Internet pour les réseaux Télécom. Il permet d'accéder à un réseau IP à partir d'un équipement distant, par exemple un poste de travail équipé d'un modem.
POA	Programmation orientée aspects : est un paradigme de programmation qui permet de séparer les considérations techniques (*aspect* en anglais) des descriptions métier dans une application.
RAD	Reconnaissance automatique de documents
RDA	Rich Desktop Application
RIA	Rich Internet Application
RPO	*Recovery Point Objective* : précise la perte maximale de données admissible.
RTO	*Recovery Time Objective* : précise le temps/délai maximal de rétablissement des ressources après un sinistre.
SAML	Security Assertion Markup Language est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. SAML est un standard supporté par un grand nombre de solutions de SSO pour les problèmes de gestion d'identité.
SAN	*Storage Area Network* : réseau dédié au stockage, le SAN permet la mutualisation des systèmes de stockage et de sauvegarde tout en ne souffrant pas des limitations de bande passante occasionnées par l'utilisation du réseau local desservant les postes de travail ou les serveurs (cas typique du NAS).
SCORPION	Services de COnservation Référencés Probants pour l'Intégrité des Objets Numériques du ministère de la Justice.
SDIDE	Sous-Direction de l'Ingénierie des Développements et de l'Exploitation
Service	Un service s'exécute automatiquement en tâche de fond et répond aux requêtes des clients. Il est en général installé sur un serveur.
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique. Depuis le décret du 20/11/2017, laisse place à la DITP et la DINSIC.
SI	Cf. système d'information
SILL	Socle Interministériel de Logiciels Libres. Il regroupe l'ensemble des logiciels libres préconisé au sein des ministères. Il est géré par les correspondants ministériels, dans le cadre de l'instance de mutualisation sur les logiciels libres, sous le contrôle de la DINSIC.

SLR	Serveur Local de Ressources
SOA	*Service-Oriented Architecture.* Lancée par Gartner Group, la notion de SOA (pour Architecture Orientée Services) définit un modèle d'interaction applicative mettant en œuvre des connexions en couplage lâche entre divers composants logiciels. Un service désigne une action exécutée par un composant « fournisseur » à l'attention d'un composant « consommateur », basé éventuellement sur un autre système.
SNM-I	Service National de Maintenance Informatique
SNM-R	Service National de Maintenance Réseau
SPOC	*Single Point Of Contention* : littéralement « point individuel de contention ». Consiste dans un système à identifier, pour les différents composants (matériels et/ou logiciels), l'existence de points constituant un goulet d'étranglement. Ce composant est alors considéré comme un SPOC pour le système.
SPOF	*Single Point Of Failure* : littéralement « point individuel de défaillance ». Consiste dans un système à identifier, pour les différents composants (matériels et/ou logiciels), l'existence de points de défaillance pouvant générer un dysfonctionnement du système de par l'impossibilité de redonder ce composant ou de par le choix de ne pas le redonder. Ce composant est alors considéré comme un SPOF pour le système.
Système d'Information	Selon la définition restreinte donnée par Joël de Rosnay, « *Un système est un ensemble d'éléments en interaction dynamique, organisés en fonction d'un but* ». Le système d'information n'échappe pas à cette définition. Il est un ensemble dont les éléments sont les constituantes de toute organisation (entreprise, administration, association, groupement, …). Ces éléments sont de plusieurs natures : organisationnelle, informationnelle, métier, technique, technologique. Tous ces éléments forment un tout (plus ou moins cohérent) et participent à la réussite de l'organisation dans son objectif.
SSIC	Service des Systèmes d'Information et de Communication
TCP	TCP (Transmission Control Program) est un protocole permettant l'ouverture de circuits virtuels entre applications.
Travail collaboratif	Une application de travail collaboratif est un ensemble d'outils, de méthodes et de procédures par lesquels un groupe de personnes peut travailler en commun en partageant informations et documents. On peut distinguer deux catégories de fonctions répondant à cette définition :une première catégorie de services fonctionnant sur un mode asynchrone : la messagerie, l'agenda partagé, la gestion des tâches, le partage de documents, la liste de diffusion, les forums, la gestion des formulaires et des processus, • une seconde catégorie de services fonctionnant sur un mode synchrone : la messagerie instantanée, le chat, la vidéoconférence. Une application de travail collaboratif est toujours structurée autour d'un annuaire où sont inscrits les utilisateurs dont les autorisations d'accès sont fonction des droits attribués à chacun.
Urbanisme fonctionnel	L'urbanisme fonctionnel a pour vocation de définir une vision stable du Système d'Information, au croisement du métier et de la technique. Aussi bien les processus d'une entreprise que son informatique, c'est-à-dire, aussi bien la façon dont elle structure la réalisation de son métier, que la façon dont elle automatise son métier, sont en perpétuel changement. Le découpage en domaines fonctionnel (ou zones fonctionnelles) permet, en liaison avec les processus, et avec l'informatique, de disposer d'un socle capable d'analyses d'impacts à tous les niveaux.
VPN	*Virtual Private Network*, réseau privé virtuel (RPV) : Le principe du RPV consiste à créer un réseau privé au sein d'un réseau public. Cette démarche existe depuis longtemps : les opérateurs s'en servent pour gérer les lignes privées de leurs clients au sein des mêmes « tuyaux ». Aujourd'hui, on parle surtout de réseaux privés virtuels sur Internet. Les RPV mettent en œuvre des mécanismes de contrôle d'accès (authentification des utilisateurs) et assurent la confidentialité des données (cryptographie). Le terme de réseau privé virtuel s'applique aussi au réseau téléphonique: les opérateurs font ainsi transiter sur le réseau public des services évolués de téléphonie jusque-là cantonnés au réseau privé de l'entreprise appel en numérotant uniquement l'extension, renvoi d'appel, conversation à plusieurs, etc. Cette technologie s'étend aussi aux mobiles.

Windows Server	Windows Server est un système multi-tâches, multi-utilisateurs qui dans ses fonctionnalités peut se comparer au système UNIX/Linux. Il présente l'avantage que certains logiciels soient moins chers que leur équivalent fonctionnant sous UNIX, et plus rarement, Linux. Par ailleurs, la quasi-totalité des éditeurs proposent des versions de leurs produits pouvant tourner sur serveur Windows.
XML	Extensible Markup Language : un langage qui permet de structurer l'information en l'encadrant par des balises. Ces balises peuvent être définies par le concepteur d'une application, elles décrivent les informations qui seront échangées à travers internet. Standards soutenus par W3C.
XSL	Extensible Stylesheet Language : un langage pour exprimer les feuilles de style en ce qu'il fournit un vocabulaire pour spécifier la sémantique du formatage. Une feuille de style est appliquée aux données d'un contenu structuré en XML pour fournir une présentation prévisible.

9.2. RÉFÉRENTIELS ET LIENS UTILES

9.2.1. Référentiels

- Référentiels et rapports publiés par la SGMAP : https://references.modernisation.gouv.fr

9.2.2. Contacts

Pour toute information complémentaire, question, remarque concernant le contenu de ce document, vous pouvez contacter le bureau BAPT (SG/SSIC/SDIDE/ETD/APT) qui centralise les demandes et coordonne la mise à jour du CCT.