MINISTÈRE DE LA JUSTICE

Commission de l'Informatique, des Réseaux et de la Communication Electronique

Cadre de cohérence technique (CCT)

Juin 2005

Référence : COMIRCE/SD/02-893

Version : V 6.11

Ce document a été élaboré et actualisé par la COMIRCE avec les contributions des directions

Version d'origine : V6.5 de novembre 2002

COMIRCE

13, place Vendôme
75042 Paris cedex 01
Téléphone : 01 44 77 70 84
Télécopie : 01 44 77 70 83

AVERTISSEMENT

Le cadre de cohérence technique du ministère de la justice tient compte des recommandations du cadre commun d'interopérabilité publié par l'ADAE[1] (ex-ATICA) dont la circulaire du 4 décembre 2002 confirme et étend sa couverture de mise en oeuvre. Les recommandations qui le constituent sont à prendre en considération lors de la préparation de tout projet technique apportant des modifications aux systèmes d'information 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 cadre commun d'interopérabilité publié par l'ADAE et le présent cadre de cohérence technique devront être référencés dans les cahiers des charges.

* *
*

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 cadre commun d'interopérabilité, une actualisation au minimum annuelle est envisagée. C'est pourquoi :

toute difficulté rencontrée lors de la mise en oeuvre du cadre de cohérence technique devra être signalée à la COMIRCE.

* *
*

Rappel des termes des circulaires du 21 janvier et du 4 décembre 2002

Les prescriptions suivantes devront être respectées :

a. le cadre commun d'interopérabilité devra être référencé en annexe des cahiers des clauses techniques particulières relatives aux projets déjà mentionnés ;

b. s'il s'agit d'une application à caractère interministériel ou accessible à des personnes tierces à l'administration, une attestation de conformité, établie par chaque ministère ou en ayant recours à un organisme spécialisé, devra être adressée au secrétaire général du Gouvernement, préalablement à la mise en oeuvre de cette application ; ou, à défaut, d'indiquer les raisons pour lesquelles il a paru nécessaire de s'en écarter, ainsi que le calendrier envisagé pour assurer la mise en conformité ;

c. pour le fonctionnement de telles applications, il sera nécessaire de veiller tout particulièrement à ce que ne soient utilisés d'autres formats de documents que ceux référencés dans le cadre commun : c'est une condition nécessaire pour assurer la pérennité des documents informatisés et garantir la possibilité d'un accès aux informations qu'ils contiennent.

d. mise en œuvre des recommandations contenues dans les référentiels qui accompagnent les services opérationnels pour l'interopérabilité ; évaluation de conformité par audits périodiques, à la charge des services, avec résultats communiqués au secrétaire général du Gouvernement ;

e. prendre ses dispositions afin que, dans les meilleurs délais, l'ensemble des référentiels de données et des composants logiciels librement réutilisables dont la nature présente un intérêt général soient répertoriés. Les ministères adresseront périodiquement ces deux listes à l'ADAE, qui les publiera ;

f. l'utilisation du répertoire de schémas XML de l'administration doit être conforme aux modalités énoncées dans le référentiel. La méthode de conception retenue doit privilégier l'utilisation de schémas existant par rapport au développement de nouveaux schémas, sauf dérogation expressément accordée par le secrétariat général du Gouvernement ;

g. une consultation systématique du service de ressources numériques doit être envisagée à l'occasion de tout projet d'échanges entre les ministères ou avec des tiers, afin de privilégier la réutilisation de modèles, de référentiels de données et de composants logiciels existants.

Le cadre commun d'interopérabilité peut être consulté en ligne sur le site de l'ADAE (www.adae.pm.gouv.fr).

[1] Agence pour le Développement de l'Administration Electronique

SOMMAIRE

1. Les lignes directrices du cadre de cohérence

1.1 Les besoins et le périmètre

Le Système d'Information 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.

La partie informatisée du Système d'Information 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 interadministratif et à l'intergouvernemental...), l'objectif principal recherché par le ministère de la justice est de disposer d'un système d'information adapté (aux besoins du moment) et adaptable (rapidement et à coûts réduits).

Dans ce contexte, **le cadre de cohérence technique du Système d'Information** (ou CCT) a une quadruple vocation :

- 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 « cadre commun d'interopérabilité des systèmes d'information des administrations » de l'ADAE[2] ;
- 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 communications, bases de données locales, gestion d'habilitation,...).

Le cadre de cohérence est un des résultats majeurs du travail des architectes du Système d'Information, 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 Système d'Information ces qualités de cohérence et d'évolutivité.

Il s'agit à ce stade de recommandations, sauf dans le cas des interfaces avec les services interministériels opérationnels, le respect des standards étant dans ce cas considéré comme acquis.

Ce cadre de cohérence doit être **partagé, visible et évolutif**.

Partagé : le cadre sera d'autant mieux adapté qu'il répondra aux besoins des administrations et des usagers y compris les partenaires extérieurs, d'une part, qu'il sera à l'état de l'art, d'autre part. C'est pourquoi des procédures *d'appels à commentaires* dans le cadre de la COMIRCE paraissent adaptées à son élaboration.

[2] Agence pour le Développement de l'Administration Electronique

Visible : la visibilité du cadre apparaît comme une condition de son respect par les maîtrises d'ouvrage et d'œuvre des projets. La publication du cadre apparaît donc nécessaire, sa mise en ligne sur le site intranet de la Comirce et à terme sur ADER y contribuera.

Evolutif : les choix faits correspondent à l'état de l'art, dont on sait qu'il est évolutif. Une actualisation au minimum annuelle du cadre est envisagée. Ces choix doivent être complétés et enrichis à partir de référentiels inter-administrations (ceux en particulier mis en ligne par l'ADAE), de projets innovants opérationnels (conçus en centrale ou en initiative locale).

1.2 Les bénéficiaires du cadre de cohérence technique

1.2.1 Les acteurs

Les différents acteurs de l'informatique du Ministère de la Justice ont des rôles et des demandes différentes par rapport au cadre de cohérence technique :

- **Les maîtres d'ouvrage** : Ils sont les clients des concepteurs et développeurs des applications et services.

  Ils contribuent à la cohérence technique de la partie informatisée du système d'information en réclamant dans leurs cahiers des charges l'utilisation de produits conformes aux recommandations préconisées par le cadre de cohérence. Ils obtiennent ainsi des solutions :

  - construites à partir d'éléments validés dont la pérennité est garantie par les architectes du Système d'Information ;
  - s'intégrant facilement dans l'informatique du ministère 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 finals** : Ils sont les bénéficiaires des services et des applications mis à leur disposition et sont clients des administrateurs.

  Ils sont soumis aux à l'utilisation de solutions préconisées par le cadre de cohérence technique 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 services ;
  - faciliter une meilleure réactivité des administrateurs et des supports (help) 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 cadre de cohérence technique des produits :
  - testés et validés : qui ont obtenu le « label » du Ministère ;
  - sur lesquels 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** : Architectes d'application, ils trouvent dans les modèles du cadre de cohérence technique, la classification des services techniques de l'infrastructure logicielle utilisable.

  Exploitants, ils recherchent dans le cadre de cohérence technique les services et les outils préconisés pour soutenir leurs activités.

1.2.2 Les applications

Les applications doivent se conformer au cadre de cohérence technique.

L'adoption du cadre de cohérence sera d'autant plus facile qu'il sera de qualité, maintenu à jour et mis en ligne sur l'intranet : ***nul ne pourra l'ignorer***.

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

Les applications d'initiative locale doivent se conformer au cadre de cohérence technique ; ne peuvent en déroger que celles dont la non-conformité n'a pas d'impact sur des infrastructures partagées ou sur les activités de structures informatiques mutualisées. 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.

Une application qui n'est pas conforme au cadre de cohérence doit satisfaire au minimum les propriétés suivantes :

- elle doit fonctionner sur des postes de travail dédiés afin de ne pas risquer de perturber les systèmes de communication et les applications conformes au cadre de cohérence ;
- elle ne pourra utiliser une infrastructure mutualisée (RPVJ, serveur local de ressources, serveur de sauvegarde, …) qu'à la seule condition d'avoir fait l'objet d'un rapport d'expertise technique favorable d'une structure nationale (SDI/ATI) ou régionale (SDI/CPR).

Dans le cadre d'une mutualisation des expériences, la description d'application à contexte innovant est remontée à la Comirce et à la SDI. Si une application utilise un composant logiciel ou technique non référencé mais concernant un segment du système d'information n'ayant pas été identifié au CCT, une déclaration est également nécessaire et peut aboutir à une évolution du CCT.

1.3 Les propriétés recherchées

Les propriétés recherchées pour les systèmes d'information et de communication à travers le respect du cadre de cohérence technique sont principalement les suivantes :

- **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,
- **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 oeuvre 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.

Ces propriétés traduisent des grands principes, ou règles de l'art, concernant :

- L'ergonomie de l'interaction avec la machine
- La conformité aux normes des standards et référentiels.
- La modularité des composants du Système d'Information

Partage de la ressource poste de travail

Tous les services (messagerie, intranet, partage de ressources, …), toutes les applications métiers, les suites bureautiques et collecticiels 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.

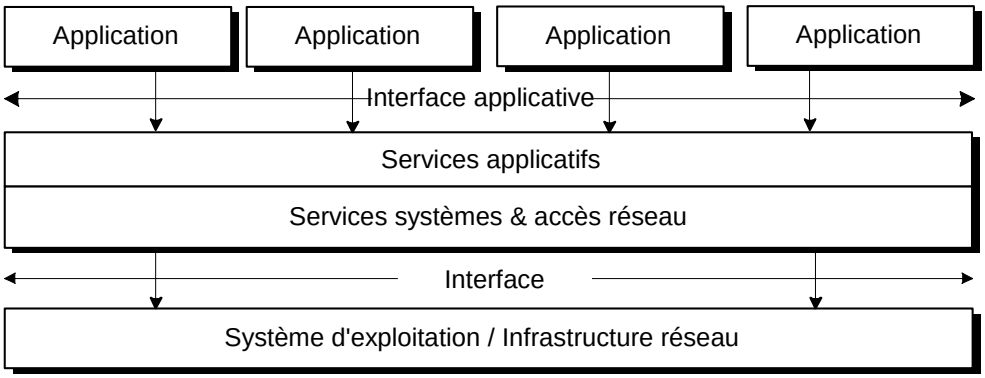
Cela requiert pour les développeurs de s'affranchir de paramètres spécifiques de configuration du poste de travail ou tout au moins de les publier et de vérifier leur compatibilité avec l'environnement standard des futurs utilisateurs.

Principe de non-adhérence

Afin de limiter les dépendances, les interactions entre les différents composants du logiciel utilisent des interfaces standardisées.

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

Illustration du principe de non-adhérence



Homogénéité des interfaces homme / machine

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, ce qui a également pour effet de réduire les phases d'apprentissage. Les coûts de conception, de développement et de maintenance sont également réduits en raison d'une meilleure homogénéité des applications.

Caractère industriel des applications

La conception, la réalisation, la mise en oeuvre 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 modules.

Ainsi, les infrastructures et les applications informatiques se présentent comme la mise en oeuvre d'un ensemble de grandes générations 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 mieux maîtriser les coûts.

Principe de continuité

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

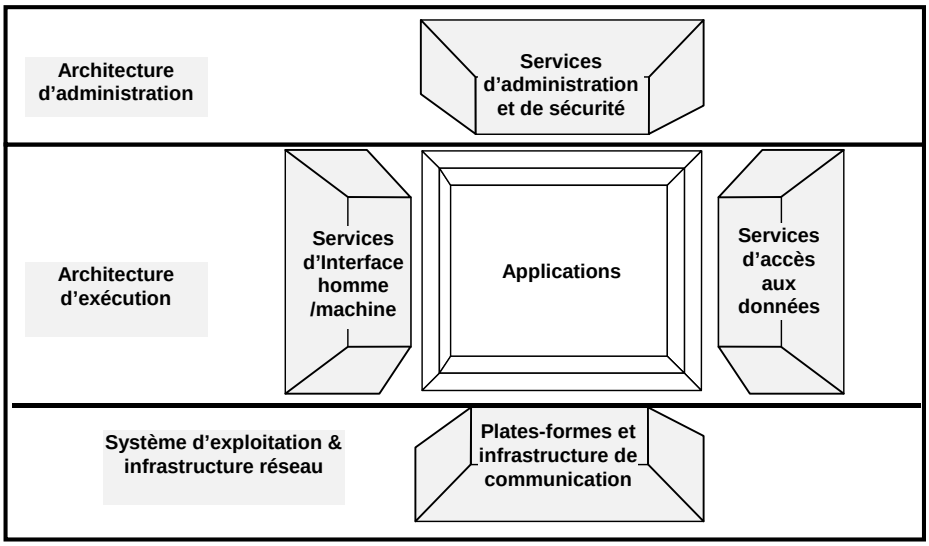
Ces dispositions permettent d'éviter une nouvelle saisie des données et de satisfaire aux exigences de la fonction de conservation des informations. Pour les investissements du parc, cela permettra de réduire les coûts en optimisant les transitions (plans de migration) tout en assurant une continuité de service.

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.

1.4 Les services applicatifs

Dans le cadre de cohérence technique, la composante technique des applications est vue comme un assemblage, statique ou dynamique, de services élémentaires qui séparent ces applications des caractéristiques propres aux matériels et aux logiciels de base.

Le schéma ci-dessous illustre cette séparation entre les applications d'une part, les plates-formes et le réseau d'autre part :



Le cadre de cohérence technique reconnaît, actuellement, les classes de services suivantes :

- **services d'interface utilisateur,** qui concernent l'interaction entre les applications et les utilisateurs qui participent à la saisie et à la restitution des données **;**
- **services de gestion des données**, qui gèrent l'accès et la structuration des données ;
- **services de communication**, qui procurent les mécanismes nécessaires à l'échange et au partage d'informations ;
- **services de sécurité**, qui permettent de préserver la confidentialité des informations ;
- **services d'administration**, qui participent à la gestion des systèmes informatiques ;
- **services de développement**, qui fournissent les outils supportant la réalisation des applications.

Les produits retenus par le Ministère pour la mise en oeuvre de ces différents services sont décrits dans les chapitres suivants du cadre de cohérence technique. Ils ont été regroupés en fonction des trois principaux niveaux d'architecture du Système d'Information :

- l'architecture d'exécution,
- l'architecture d'administration,
- l'architecture de développement.

Le chapitre *2 Architectures d'exécution préconisées* donne les principes généraux nécessaires à l'équipement des sites, et indique les architectures d'exécution à prévoir selon les types de sites du ministère.

Le chapitre *3 Architecture d'exécution* traite à la fois l'infrastructure et les services applicatifs directement liés d'une part à l'exécution des applications, et d'autre part à l'implantation et aux déploiements de systèmes de communications.

Le chapitre *4 Architecture d'administration* traite les services applicatifs liés à l'exploitation, à l'administration et à la sécurité des systèmes et des applications.

Le chapitre *5 Architecture de développement* traite les outils et les services utiles au développement des applications et décrit des modèles types d'architectures.

1.5 Les autres référentiels et les liens utiles

Les référentiels et des rapports publiés par l'Agence pour le Développement de l'Administration Electronique (ADAE ex ATICA) :

http://www.adae.pm.gouv.fr

Des informations et consignes de sécurités :

http://intranet.justice.gouv.fr/securite/accueil.htm

Le guide méthodologique de création d'un site Internet :

http://intranet.justice.gouv.fr/site/sicom/index.php

Le déploiement du RPVJ : guides, études, …..

http://intranet.justice.gouv.fr/rpvj

Le site de la COMIRCE :

http://comirce.intranet.justice.gouv.fr/

2. Architectures d'exécution préconisées pour les sites Justice

Après un rappel des définitions et principe de construction des architectures d'exécution, le présent chapitre expose, par type de site du ministère, les architectures à prévoir *en cas de renouvellement ou de création de site* et les préconisations à appliquer.

Les architectures indiquées constituent la cible à rechercher. Les *mesures de transition* éventuellement mentionnées couvrent les cas où les applications ne sont pas (encore) disponibles dans des versions compatibles avec l'architecture spécifiée en cible.

2.1 Définitions et principes généraux pour l'équipement des sites

Le problème général du responsable informatique d'un site confronté à la question du renouvellement des équipements ou de leur évolution se pose en trois étapes

- inventorier les applications nécessaires sur le site,
- sélectionner une architecture d'exécution capable d'accueillir l'ensemble de ces applications,
- déterminer les caractéristiques des équipements, parmi les caractéristiques inventoriées dans le cadre de cohérence technique.

L'inventaire des applications est nécessaire pour vérifier la compatibilité de celles-ci avec l'architecture d'exécution envisagée. Les applications nationales sont conçues pour s'adapter aux architectures d'exécution préconisées. Certaines applications d'initiative locale pourront requérir soit une migration, soit une refonte pour assurer la compatibilité avec l'architecture technique projetée.

Le renouvellement des équipements d'un site peut être l'occasion de modifier en profondeur l'architecture d'exécution. Ceci peut induire la substitution d'un serveur du site par l'accès à un serveur distant sur un site mutualisé. Ceci peut également induire le remplacement de certaines applications incompatibles avec les nouvelles architectures par des versions plus récentes ou par des applications nouvelles. Le responsable informatique prévoira les tâches de migration et de reprise des données éventuellement nécessaires.

L'architecture d'exécution reconnaît trois types de ressources de traitement :

- les **serveurs d'applications** (WINDOWS 2000, LINUX, UNIX (AIX, HP-UX), BULL / GCOS 7) ; qui eux-mêmes peuvent être segmentés en :
  - serveurs d'application, y compris les logiciels génériques (messagerie, groupware, GED, …)
  - serveurs de présentation, dédiés à la gestion des postes clients : serveurs web http ou serveurs de terminaux Citrix Métaframe,
  - serveurs de base de données, dédiés à la gestion des données (ORACLE, SQLBase, …) ;
- les **serveurs locaux de ressources** (NETWARE, WINDOWS 2000, LINUX/SAMBA), permettant notamment le partage de logiciels, de fichiers et de ressources matérielles (imprimantes, télécopie, sauvegarde, …) ;
- les **postes de travail** (PC et imprimantes individuelles).

Un **serveur d'application exécute la partie serveur des applications**. Des traitements s'y déroulent : la partie serveur des applications (procédures cataloguées, triggers, procédures batch,…), la partie serveur des progiciels client-serveur, et certains outils, par exemple les outils d'administration ou de sauvegarde. Il utilise les services d'un serveur de présentation pour la gestion des postes clients, et d'un serveur de base de données pour la gestion des données. Ces deux serveurs peuvent toutefois être confondus avec le serveur d'application.

Un **serveur local de ressources** gère le partage des ressources sur le réseau local, pour le compte des postes de travail. Ces ressources partageables sont :

- des **équipements**, par exemple des imprimantes, des bibliothèques de sauvegarde ou des télécopieurs. Le serveur local de ressources (souvent appelé « serveur bureautique ») auquel ils sont connectés en gère l'accès et le partage. Il est, autant que faire se peut, préférable de partager des équipements plutôt que d'en équiper chaque poste de travail ;

- de **l'espace disque**, ce qui évite de dupliquer certains fichiers sur chaque poste de travail, par exemple les outils bureautiques. Le serveur local de ressources se comporte alors comme une extension du disque du poste de travail, sur lequel les outils continuent à être exécutés localement ;
- certains **fichiers de données**, non organisés en bases de données, mais partageables entre plusieurs occurrences d'une même application s'exécutant sur des postes du même réseau local.

Le **poste de travail** permet l'accès de l'usager aux ressources et applications du système d'information.

La partie *3 Architecture d'exécution* décrit les préconisations admises pour chacun des éléments physiques définis ci-dessus.

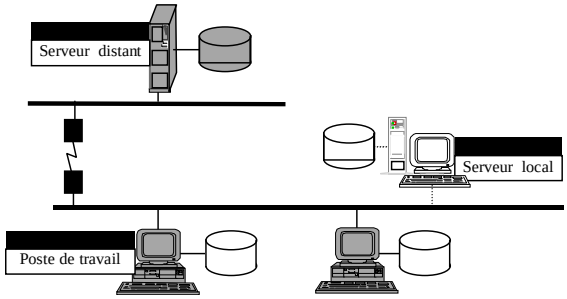
2.1.1 Types de répartition des données et des traitements

L'architecture d'une application est composée d'éléments physiques dont les combinaisons applicables dans le cadre du Ministère sont décrites ci-dessous sous forme de **quatre types d'architecture physique**, définis en fonction des types d'équipements devant être déployés aux trois niveaux d'hébergement principaux (niveau local, régional ou national).

Machines au Niveau d'exploitation ➔ machines au Niveau d'utilisation ⬇	aucun serveur d'application	Serveur d'application en local	Serveur d'application distant régional ou national
Poste de travail	4) Local de type monoposte (possible)	3) C/S « Client lourd » (possible) **1) C/ S « Client léger » (Recommandé)**	**1) C/ S « Client léger » (Recommandé)** **2) C/S « Client distant »** (Citrix) **(préconisé pour migration sur le RPVJ de l'existant)**

Nota : C/S est une abréviation de « client-serveur »

1. Architecture physique de type « C/S client léger » : RECOMMANDÉ

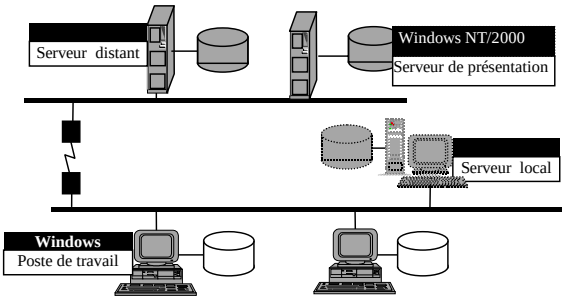


Application client-serveur : Client léger, le serveur est local ou distant.

- 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.

Une application peut avoir à accéder en modification, au sein d'une même transaction, à plus d'un serveur d'application. Il est alors nécessaire d'utiliser un moniteur transactionnel ou un commit à deux phases afin de ne pas risquer d'introduire des incohérences entre les deux bases de données.

2. *Architecture physique de type « C/S client lourd, serveur distant » :* ***PRÉCONISÉ POUR MIGRATION SUR LE RPVJ DE L'EXISTANT***

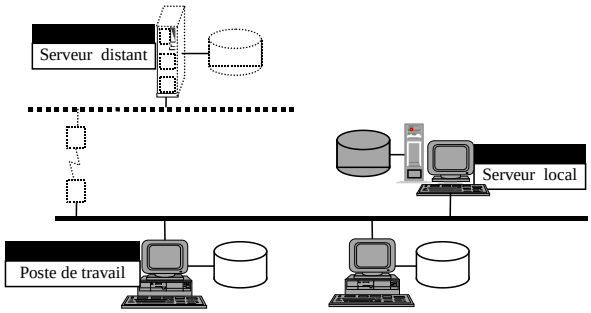


Combinaison des architectures de type « C/S client lourd » avec mise en œuvre d'un « serveur d'application distant ».
L'objectif de cette répartition est une solution de transition pour améliorer les performances de communication par rapport à une architecture de type « C/S standard », elle permet à une **application (compatible Windows NT/2000)** développée initialement pour une exploitation locale de fonctionner correctement en s'adossant au RPVJ. Ici, les données accédées fréquemment peuvent être sur le serveur local en lecture.

Les bases de données sont stockées sur des serveurs distants, les traitements s'exécutent aussi sur des serveurs distants mixtes ou dédiés sous Windows 2000/NT avec la couche « Metaframe » de Citrix.

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

3. *Architecture physique de type « C/S Client lourd » :* ***POSSIBLE***



Application client-serveur en local.

Les données sont stockées sur un serveur connecté au réseau local.

L'application s'exécute pour sa partie serveur sur le serveur local, et pour sa partie cliente sur le poste de travail :

la présentation est gérée par le poste de travail,

la gestion des données est réalisée par le serveur,

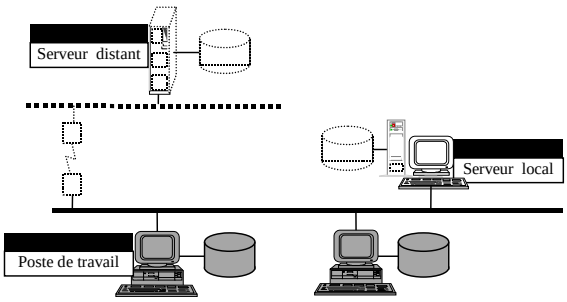
les traitements sont réalisés pour partie par le serveur et pour partie par le client.

Les programmes sont stockés pour la partie serveur sur le serveur local, et pour la partie client sur un disque du poste de travail.

Le disque du poste de travail est soit local, soit géré par un serveur de fichier. Dans ce cas, une copie unique de la partie cliente des programmes peut être partagée par plusieurs postes de travail. Le serveur de fichier n'est pas nécessairement la même machine que le serveur de l'application.

Performances Attention : les capacités de traitement des serveurs de réseau local sont limitées. De plus, la gestion de l'évolution d'un grand nombre de « petits » serveurs locaux coûte extrêmement cher.

4. Architecture physique de type « Local de type monoposte » : Possible



L'application n'est pas client-serveur. Il s'agit d'une application « micro » :

Les données sont stockées sur le poste de travail.

Les programmes et les paramètres de l'application sont stockés sur le poste de travail.

L'application s'exécute sur le poste de travail.

Le disque du poste de travail est soit local, soit géré par un serveur de fichier. Dans ce cas, une copie unique des programmes peut être partagée par plusieurs postes de travail, mais avec un seul utilisateur à la fois.

Dans cette architecture, les données dites locales peuvent également se trouver sur un disque réseau, qui, s'il est partagé, permettra à plusieurs utilisateurs d'accéder tour à tour à ces données, avec des performances dégradées par la traversée des couches réseau.

Les applications dites « en fichiers partagés X-Base » relèvent de cette architecture. Les fichiers partagés sont hébergés par le serveur local de ressources. Le même fichier peut être ouvert par plusieurs utilisateurs du réseau, mais chaque donnée ne doit être modifiée que par un utilisateur à un instant donné. Contrairement au serveur de bases de données, les mécanismes d'accès du serveur local de ressources ne garantissent pas la cohérence de la base de données si plusieurs utilisateurs tentent simultanément de modifier des données liées entre elles.

2.1.2 Recommandations d'utilisation

1. ***Les serveurs locaux de ressources et les serveurs d'application 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. En conséquence :***

   On évitera si possible d'utiliser une même machine à la fois comme serveur local de ressources et comme serveur d'applications.

Installer un serveur d'application sur une machine qui est déjà serveur local de ressources a pour conséquence de la surcharger, d'en compliquer l'exploitation et les évolutions. Le matériel deviendra plus vite obsolète car, contrairement à celles du serveur local de ressources, les nouvelles versions des logiciels des serveurs d'applications sont généralement plus consommatrices de ressources CPU et mémoire.

Pour les applications, il faut configurer les serveurs en fonction des caractéristiques des sites servis et des prévisions d'évolution, de montée en charge et de mutualisation.

Dans le cadre de la mise en place d'une application, le serveur peut intégrer le recours à des services de partage de ressources propres à cette application. Dans ce cas, le recours à un partage de ressources sur le serveur d'applications pour les seuls utilisateurs de cette application peut s'avérer une solution économiquement viable.

La cohabitation sur le même serveur (on parle alors de « mutualisation ») devra être traitée avec attention, et en aucun cas ce mode de fonctionnement ne saurait être généralisé à l'ensemble des utilisateurs connectés au réseau local d'un site.

La mise en place de serveurs locaux de ressources dédiés à des fonctions techniques dissociées de celles des applications devrait permettre d'aller dans le sens de la dissociation Serveur d'application/Serveur local de ressources, et simplifierait la mise à disposition sur les sites de fonctions de messagerie, de groupware et le partage de ressources de télécommunication.

La séparation entre serveur d'application et serveur local de ressources permet en outre d'envisager de façon systématique la mutualisation des serveurs d'applications.

2. ***On évitera, sauf impérieuse nécessité en relation avec la sécurité, de spécialiser certains postes de travail à certaines applications.***

3. ***Chaque site géographique doit être desservi par un serveur local de ressources***

Voir 3.1.8 Fiche « Serveur local de ressources ». Cette règle ne souffre d'exception que pour les petits sites ne comprenant pas plus de cinq postes de travail co-localisés en réseau non administré. Sur ces postes, les applications sont soit monopostes ***sans fichier partagé***, soit en client serveur avec serveur distant, soit en client léger.

4. ***La mutualisation de serveur de même type sur un site géographique***

Les entités hébergées sur un même site peuvent utiliser le même serveur local de ressources. Cette mutualisation est source d'économies d'exploitation.

De même, sur un même serveur d'applications est possible l'hébergement de plusieurs applications destinées à des établissements différents, du moment que ces applications utilisent un environnement homogène de bases de données : voir 3.1.9 Fiche « Serveur d'applications ou de données ».

Les responsables informatiques de services déconcentrés pourront, en cas de doute, demander à leur CPR une étude particulière de l'architecture de leur site.

2.2 Sites des services judiciaires

2.2.1 Fiche « Cour d'appel »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : les postes sont en Windows 98 jusqu'à la diffusion de toutes les applications en client Windows XP Pro.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Accès à Winpark par client « distant » Citrix Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP. ***Mesure de transition*** **:** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Windows 2000 Server. Hébergement d'applications d'initiative locale **Option :** hébergement des suites bureautiques sur serveur ***Mesure de transition*** **:** Maintien d'un serveur Netware jusqu'à qualification sous Windows 2000 Server des applications nationales ou d'initiative locale
Accès aux applications comptables	Serveur sur site Windows 2000 Server, SQLBase - Application comptable GIBUS - Application régie REGINA ***Mesure de transition*** **:** Maintien d'un serveur Windows NT4 SQLBase
Accès à l'application civile	**Cas 1 : Cour d'appel standard:** WinCI-CA (version fichiers partagés Xbase) hébergé sur serveur local de ressources. **Cas 2 : Cour d'appel d'activité importante :** - Windows 2000 Server, Oracle, WinCI-CA (version Oracle)
Serveur messagerie	Serveur Windows 2000 Server, Microsoft Exchange 2000 Serveur Windows 2000 Server utilisé en contrôleur de domaine au sens de Active Directory Messagerie pour les agents du ressort de la Cour d'appel
Serveur Web applicatif communication partenaire	1ère application d'échange COM-CI : - Windows 2000 Server, Microsoft IIS
Accès RPVJ (gérés par la SDI)	**Accès permanent** : Gold SDSL minimum 160 (débit calibré suivant l'activité du site) voire Gold via LS si justifié
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.2.2 Fiche « Service administratif régional distant ou isolé »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : les postes sont en Windows 98 jusqu'à la diffusion de toutes les applications en client Windows XP Pro.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Accès à Winpark par client « distant » Citrix Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP. ***Mesure de transition*** **:** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Windows 2000 Server. Hébergement d'applications d'initiative locale. **Option :** hébergement des suites bureautiques sur serveur. ***Mesure de transition*** **:** Maintien d'un serveur Netware jusqu'à qualification sous Windows 2000 Server des applications d'initiative locale
Accès aux applications comptables	Windows 2000 Server, SQLBase - Application comptable GIBUS ***Mesure de transition*** **:** Maintien d'un serveur Windows NT4 SQLBase
Accès RPVJ	**Accès permanent** Gold ADSL (débit à calibrer suivant l'activité du site)
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.2.3 Fiche « Tribunal de grande instance »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** **:** maintien de postes spécialisés pour accès à la micro- ou la minipénale et éventuellement à l'application commerciale ALINEA.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP. ***Mesure de transition*** **:** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Windows 2000 Server. Hébergement d'applications d'initiative locale **Option** : hébergement des suites bureautiques sur serveur. ***Mesure de transition*** **:** Maintien du serveur local Netware jusqu'à qualification sous Windows 2000 Server des applications nationales ou d'initiative locale
Accès aux applications comptables	Windows 2000 Server, SQLBase - Application comptable GIBUS - Application régie REGINA - Application aide juridictionnelle AJWin ***Mesure de transition*** **:** Maintien d'un serveur Windows NT4 SQLBase
Accès à l'application civile	**Cas 1 : TGI standard** WinCI-TGI (version fichiers partagés X-Base) sur serveur local de ressources **Cas 2 : TGI d'activité importante** Windows 2000 Server, Oracle, WinCI-TGI (version Oracle).
Accès à l'application pénale nationale	**Cas 1 : TGI de province (Cassiopée)** Accès via client léger à serveur pénal distant ***Mesure de transition*** **:** Maintien du serveur « Micropénale » ou « Minipénale » selon le cas. *Le serveur « Minipénale » doit être en état de fonctionner jusque fin 2006 sans renouvellement de matériel.* **Cas 2 : TGI de région parisienne (NCP) :** Accès via émulateur à serveur pénal régional
Accès à l'application juridiction commerciale	**Serveur sur site, client léger (projet ITACC)** Windows 2000 Server, Oracle, Citrix Client léger (ICA) sous XP Pro **Mesure de transition :** Serveur d'application dédié ALINEA
Serveur Web applicatif communication partenaire	1ère application d'échange COM-CI : - Windows 2000 Server, Microsoft IIS
Accès RPVJ	**Accès permanent** Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.2.4 Fiche « Tribunal d'instance et greffe détaché »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard **banalisé,** type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : les postes sont en Windows 98 jusqu'à la diffusion des applications Minos et X.TI qualifiées pour client Windows XP Pro.
Bureautique multimédia	Traitement de texte *unique* (au terme du schéma directeur) compatible avec toutes les applications en TI La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site. ***Mesure de transition*** **:** Toutes versions de Corel WordPerfect (5 à 8) nécessaires au fonctionnement des applications X.TI.
Applications spécifiques	Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP. ***Mesure de transition*** **:** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Windows 2000 Server. **Option** : hébergement des suites bureautiques sur serveur. ***Mesure de transition*** : maintien du serveur sous Netware hébergeant Minos, X.TI et certains applications d'initiative locale jusqu'à diffusion de Minos refondue et des applications X.TI compatibles Windows 2000 Server.
Accès aux applications	serveur d'application Windows 2000 – SQLBase hébergeant : - applications civiles (X.TI) - future application pénale tribunal de police - application nationale de régie REGINA *Par dérogation, après avis technique SDI, ce serveur d'application peut jouer le rôle de serveur local de ressources* ***Mesure de transition*** : Maintien du serveur d'application local sous Netware – SQLBase hébergeant les applications civiles nationales X.TI.
Accès aux applications spécifiques en Alsace-Moselle	**Tenue du registre du commerce et des sociétés : Projet ITACC** Serveur sur site, Windows 2000 Server, Oracle, Citrix client léger (ICA) sous XP Pro ***Mesure de transition*** **:** Serveur d'application dédié module RCS de l'application ALINEA **Livre Foncier :** accès client léger à l'application AMALFI du GILFAM
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.2.5 Fiche « Tribunal de police » (Paris, Lyon, Marseille)

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : les postes sont en Windows 98 jusqu'à la diffusion de l'application remplaçant Minos.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP. ***Mesure de transition*** **:** Maintien de IPX/SPX en cohabitation tant que le serveur local de ressources l'exige.
Serveur local de ressources	Windows 2000 Server. **Option** : hébergement des suites bureautiques sur serveur. ***Mesure de transition*** : maintien du serveur sous Netware hébergeant Minos jusqu'à diffusion de l'application qui la remplace.
Accès à l'application pénale	Serveur d'application sur site ou accès client léger selon spécification à venir. ***Mesure de transition*** : l'application Minos est hébergée par le serveur local de ressource, ou par un poste dédié, selon organisation du site.
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.2.6 Fiche « Conseil des prud'hommes »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Applications métiers, selon répartition des données et traitements de chaque application (cf. 2.1.1)
Réseau local	TCP/IP.
Accès à l'application juridiction prud'homale	**Cas 1 : serveur local de partage de ressources** Windows 2000 Server, WinGes CPH (version fichiers partagés X-Base) **Option** : hébergement des suites bureautiques sur serveur. **Cas 2 : serveur d'application et de partage de ressources** Windows 2000 Server, Oracle,WinGes CPH (version Oracle) *Par dérogation, après avis technique SDI, le serveur d'application peut jouer le rôle de serveur local de ressources* **Option** : hébergement des suites bureautiques sur serveur.
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades
Télémaintenance	Cf 4.1.4 Services de télémaintenance

2.3 Sites de l'administration pénitentiaire

2.3.1 Fiche « Direction régionale des services pénitentiaires »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : - les postes sont en Windows 98 jusqu'à validation de toutes les applications en client Windows XP Pro
Bureautique multimédia	Privilégier l'homogénéisation du site. OpenOffice.org en cours d'évaluation par l'AP en vue d'un déploiement à partir de 2005 en remplacement de la suite Microsoft Office.
Applications spécifiques	Client GRPP Accès à Winpark par client « distant » Citrix Autres applications : selon répartition des données et traitements de chaque application (cf. 2.1.1).
Réseau local	TCP/IP. ***Mesure de transition*** : Migration en cours des protocoles IPX/SPX vers TCP/IP.
Serveur local de ressources	Linux Hébergement des suites bureautiques sur serveur. ***Mesure de transition*** **:** Migration programmée à partir de 2004 des SLR Netware et Windows 2000 vers des SLR sous Linux. (cible fin 2005)
Serveurs d'application métier	**Serveur d'application GRPP** Windows 2000 Server, SQLBase
Serveur messagerie	Serveur Windows 2000 Server, Microsoft Exchange 2000 Serveur Windows 2000 Server utilisé en contrôleur de domaine au sens de Active Directory Messagerie pour les agents du ressort de la région
Accès RPVJ (gérés par la SDI)	**Accès permanent** Gold SDSL minimum 160 (débit calibré suivant l'activité du site) voire Gold via LS si justifié

2.3.2 Fiche « Etablissement pénitentiaire de milieu fermé »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : - les postes sont en Windows 98 jusqu'à la diffusion de GIDE en client Windows XP Pro à partir de début 2004. - les postes applicatifs GE, OMAP, Comptabilité générale sont maintenus jusqu'à extinction de ces applications
Bureautique multimédia	Word 97 et Excel pour les postes de travail GIDE Privilégier l'homogénéisation du site. OpenOffice.org en cours d'évaluation par l'AP en vue d'un déploiement à partir de 2005 en remplacement de la suite Microsoft Office.
Applications spécifiques	GIDE partie cliente (sur les postes concernés uniquement) Autres applications : selon répartition des données et traitements de chaque application (cf. 2.1.1).
Poste parloir	Poste *dédié* type 5 + GIDE partie cliente
Poste accès FND	Poste standard type 1, 2 ou 3 + lecteur de carte à puce
Réseau local	TCP/IP ***Mesure de transition* :** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Linux Hébergement - des applications locales. - de l'outil checkup d'inventorisation des matériels informatiques - des suites bureautiques.
GIDE	Serveur Linux, Sybase
Accès autres applications	- Applications comptables - Application GTS - Application FND - Application APPI **Cas 1 : serveur d'applications sur site** Serveur Linux (séparé du serveur GIDE) **Cas 2 : serveur distant mutualisé, accès via client léger**
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades

2.3.3 Fiche « Service pénitentiaire d'insertion et de probation »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site.
Système d'exploitation	Tout nouveau poste peut fonctionner sous Windows XP Pro. ***Mesure de transition*** : - les postes sont en Windows 98 jusqu'au remplacement de l'application MOUVE par APPI
Bureautique multimédia	OpenOffice.org en cours d'évaluation par l'AP en vue d'un déploiement à partir de 2005 en remplacement de la suite Microsoft Office. Maintien de Microsoft Excel sur les postes de travail dotés de l'application Cobra
Applications spécifiques	APPI : accès par navigateur (client léger) Autres applications : selon répartition des données et traitements de chaque application (cf. 2.1.1).
Réseau local	TCP/IP. ***Mesure de transition* :** Maintien de IPX/SPX en cohabitation tant qu'un serveur local l'exige.
Serveur local de ressources	Linux Hébergement - des applications locales. - de l'outil checkup d'inventorisation des matériels informatiques - des suites bureautiques. ***Mesure de transition*** : maintien du serveur Netware jusqu'au remplacement de l'application MOUVE par APPI.
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades

2.4 Sites de la protection judiciaire de la jeunesse

2.4.1 Fiche « Direction régionale ou départementale »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail	Poste fixe standard banalisé, type selon organisation du site
Système d'exploitation	Windows XP Pro.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site.
Applications spécifiques	Chargement à partir du serveur local de ressources
Applications particulières	NDL via émulateur
Réseau local	TCP/IP. ***Mesure de transition* :** Maintien de IPX/SPX en cohabitation tant que le serveur local de ressources l'exige.
Serveur local de ressources	Windows 2000 Server ou Linux, le choix du système d'exploitation doit être guidé par l'optimisation des ressources locales tant en homogénéité qu'en compétences. Hébergement des applications métiers PJJ sur serveur. **Option** : hébergement des suites bureautiques sur serveur.
Serveur messagerie (en DR uniquement)	Serveur Windows 2000 Server, Microsoft Exchange 2000 Serveur Windows 2000 Server utilisé en contrôleur de domaine au sens de Active Directory Messagerie pour les agents du ressort de la région
Serveur d'échange partenaires (en DR uniquement)	Windows 2000 Server Microsoft IIS Applications d'échange avec les partenaires
Accès RPVJ (DR gérés par la SDI)	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades

2.4.2 Fiche « Site d'action éducative »

	Elément préconisé:
Champ d'application	**Commentaire**
Poste de travail pédagogique	Poste fixe standard, **sans accès possible au RPVJ** (réseau local distinct)
Système d'exploitation	Windows XP Pro.
Bureautique multimédia	Pas de préconisation particulière, privilégier l'homogénéisation du site.
Applications spécifiques	Logiciels pédagogiques

Poste de travail agent	Poste fixe standard banalisé, type selon organisation du site
Système d'exploitation	Windows XP Pro.
Bureautique multimédia	La dernière version des suites bureautiques compatible avec l'environnement applicatif du site (cf. tableau croisé des compatibilités http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf) (cf.3.3.1) Privilégier l'homogénéisation du site..
Applications spécifiques	Chargement à partir du serveur local de ressources

Réseau local	TCP/IP. ***Mesure de transition* :** Maintien de IPX/SPX en cohabitation tant que le serveur local de ressources l'exige.
Serveur local de ressources	Windows 2000 Server ou Linux, le choix du système d'exploitation doit être guidé par l'optimisation des ressources locales tant en homogénéité qu'en compétences. Hébergement sur serveur des applications GAME, parfois COBRA. **Option** : hébergement des suites bureautiques sur serveur.
Accès RPVJ	**Accès permanent** : Pour les plus petits : ADSL Light (si éligible) à défaut SRL Pour les autres : Gold ADSL (débit à calibrer suivant l'activité du site) Les accès SPI sont à réserver aux postes nomades

3. Architecture d'exécution

3.1 Les composants d'infrastructure

L'architecture d'exécution décrit le système, présent ou futur, en proposant un **squelette** faisant référence à des **composants de base** (poste de travail, serveur,...) et à leur agencement en s'appuyant sur **trois notions de fonction principale** : les fonctions **« utilisation », « exploitation »** et **« administration »**.

- La fonction d'**utilisation** permet aux utilisateurs finals de disposer des services offerts par le système d'information. Le besoin correspondant à cette fonction peut être ainsi résumé : disposer du service souhaité avec la qualité requise (disponibilité, sécurité, support, …). Y contribuent notamment les postes de travail et les serveurs de ressources du réseau local.

- La fonction d'**exploitation** couvre l'ensemble des actions de suivi et de supervision de l'infrastructure du système d'information et des sécurités y afférents (sauvegardes, réorganisation, performances, …) ainsi que la prise en compte de traitements périodiques (archivage, statistique, …).

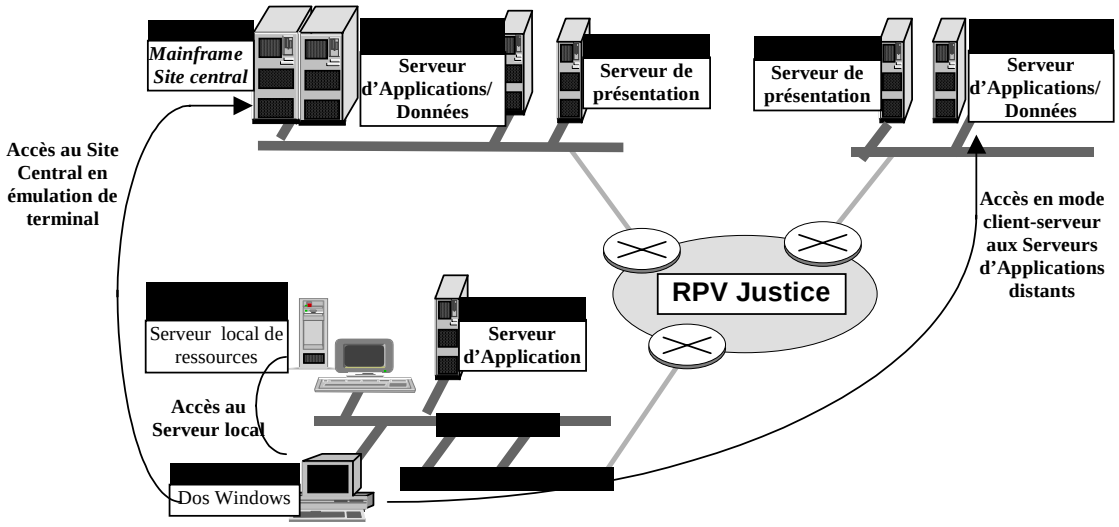
- La fonction d'exploitation est souvent complétée par une fonction d'**administration**, qui couvre des services de télémaintenance, de télésurveillance des composants des systèmes communs de communication et souvent un support de 2ème niveau pour les exploitants.

Pour localiser physiquement ces fonctions, on parlera de **niveau d'hébergement** des ressources informatiques. Le niveau d'hébergement de la fonction exploitation peut être le niveau **local** si les serveurs d'applications se trouvent sur le même site que les utilisateurs, ou le niveau **régional ou national** suivant la localisation où les machines sont regroupées et où se situent les exploitants. La fonction d'administration est en général située au niveau national alors que celle d'utilisation est strictement locale.

Plates-formes

Les composants de base de l'architecture d'exécution, ou plates-formes, sont les suivants :

- Les postes de travail ;
- Les serveurs locaux de ressources (partage de ressources disques et impression, dispositif de sauvegardes) ;
- Les serveurs d'applications/données ;
- Les serveurs de présentation ;
- Le réseau : le réseau distant et les réseaux locaux ;
- *Les ordinateurs centraux de type « mainframe » pour mémoire.*



3.1.1 Fiche « Poste de travail »

	Objectif
Les **postes de travail** sont des PC sous MS Windows 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 standard (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, parloir GIDE, accès restreint en zone publique ou pédagogique, …). 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.	
	configurations préconisées :
champ d'application	**commentaire**
Poste de travail	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.
Configuration type portable	Type 1 : classique Type 2 : milieu de gamme Type 3 : Notebook Type 4 : ultra portable Type 5 : haut de gamme
Configuration type poste fixe	Type 1 : client léger Type 2 : entrée de gamme supportant exclusivement des applications métiers Type 3 : milieu de gamme supportant des suites bureautiques et des outils collaboratifs et/ou des applications métiers Type 4 : haut de gamme pour des fonctions particulières : administration, PAO, PréPAO, GED, … Type 5 : station parloir GIDE Type 6 : type 2 + encombrement réduit Type 7 : type 3 + encombrement réduit Type 8 : type 4 + mini-tour Le détail de ces configurations est publié sur l'Intranet DAGE (Informatique/Marchés) à l'adresse : http://intranet.justice.gouv.fr/dage/sdi/PRI-National.htm
Unité centrale	Voir puissance suivant les modèles types
Mémoire	Selon modèles types : - client léger : configuration mémoire d'entrée de gamme - autres : au moins 4 fois la configuration mémoire d'entrée de gamme

Disque	Selon modèles types : - client léger : configuration disque d'entrée de gamme - autres : au moins 2 fois la configuration mémoire d'entrée de gamme - pour certaines applications : configuration spécifique à prévoir.
connexion réseau	carte Ethernet 10 /100 Mb/s -
Ecran	Ecran 15 pouces SVGA (800*600) au minimum pour les postes bureautiques, 1 Mo de mémoire vidéo Ecran 17 pouces 1280*1000 pour les postes GED, 2 Mo de mémoire vidéo
	Conditions d'application :
Produit	**commentaire**
Configuration	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 centres de prestations régionaux (CPR). La liste des matériels pour lesquels le SNM est compétent est publié sur le site intranet de la DAGE http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SNM2JUIN.htm. Cette liste est nécessairement limitative afin d'assurer une qualité de support correcte : en effet, tant les équipes du ministère de la justice que celles des sous-traitants chargés de la maintenance des postes de travail ne peuvent maintenir de relations techniques et commerciales qu'avec un nombre limité de constructeurs et/ou de fournisseurs. Si cette liste est susceptible d'évoluer dans le temps, les items la constituant ne sont retirés que lorsque les matériels correspondants ont été entièrement retirés du service opérationnel au sein du système d'information justice.
Disque dur	Il est recommandé d'équiper les postes de travail d'un disque dur afin : • de ne pas surcharger le réseau, • de ne pas pénaliser les performances, • de sauvegarder temporairement en local les dernières informations saisies ou consultées.
Sécurité	Il est recommandé de sécuriser au maximum le poste de travail, aussi bien au niveau matériel que logiciel. Suivre les recommandations : http://intranet.justice.gouv.fr/securite/GUIDE/HOME.HTM
Banalisation de l'interface utilisateur	Les applications doivent apparaître pour l'utilisateur comme un des outils accessibles à partir de son bureau électronique. Les applications doivent être conformes aux normes Windows (GUI) en matière d'ergonomie ou navigateur Internet (NUI), notamment pour ce qui concerne son apparence et son comportement, la structure de ses menus, l'aide contextuelle et les touches accélératrices. L'analyse des développements déjà effectués devrait permettre d'élaborer des recommandations minima à respecter.
Banalisation des postes de travail	L'installation des applications doit permettre la banalisation des postes, et l'ouverture requise pour la localisation des exécutables. En particulier: les exécutables et les fichiers de paramétrage propres à chaque utilisateur doivent pouvoir être placés dans des répertoires différents, éventuellement sur des disques différents, locaux ou situés sur un serveur local.

3.1.2 Fiche « Système d'exploitation des postes de travail »

Objectif
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. La fin de support ne signifie en aucun cas l'interdiction d'utilisation mais un objectif raisonnablement ambitieux pour motiver à la migration.

Produits préconisés :	
champ d'application Produit	**commentaire**
Système d'exploitation du poste de travail	Les nouvelles applications métiers sont développées en environnement 32 bits en tenant compte des caractéristiques particulières de ce système d'exploitation (exemple : base de registre).
Windows XP Pro	Système d'exploitation standard pour le poste de travail justice. Le service pack 2 a été validé par la SDI en environnement bureautique. Les applications métiers sont systématiquement validées en environnement Windows XP Pro (applications rentrant en diffusion après le 1/1/2002)
Windows 95, 98, Me	Système d'exploitation possible du poste de travail justice. Les applications métiers sont encore validées en environnement Windows 98 (applications rentrant en diffusion après le 1/1/2002)  Windows 95 n'est plus supporté depuis le 1/01/2004, pas de diffusion de correctif.
Linux	Distribution recommandée : Red Hat dernière version. Les postes de travail sous LINUX sont autorisés à titre expérimental. Le support en interne au ministère n'est pas garanti. **Aucune application ne sera validée dans ce contexte.** La distribution LINUX Red Hat 6.2 présente des faiblesses de gestion des périphériques USB et réseaux. Elle n'est plus recommandée.

Conditions d'application :	
Produit	**commentaire**
Windows XP Pro	Windows XP Pro constitue le système d'exploitation par défaut du poste de travail justice (notamment au regard des supports juridiques génériques d'acquisition de postes de travail mis en œuvre au plan national).
Passage à Windows XP Pro	Tout poste intégrant un accès à une application nationale devra faire l'objet d'une qualification par la Sous-Direction de l'Informatique avant de pouvoir migrer sous **Windows XP**. **Windows XP** requiert 256 Mo de RAM pour avoir des performances correctes.
Partage des ressources de poste à poste	**Il est fortement déconseillé d'utiliser ce mode de partage** Ce mode de partage est commode sur de très petits sites où il peut éviter d'avoir à acquérir un serveur, mais il devient vite impossible à administrer.
Intégration des applications	Cela implique que l'ensemble des logiciels réseau, interfaces... cohabitent en mémoire, que les logiciels s'exécutent obligatoirement sous Windows ou navigateur. Les développeurs d'applications métiers doivent notamment systématiquement vérifier le bon fonctionnement simultané de leur application et des principaux outils de productivité personnelle et collective (suite bureautique, messagerie, navigateur, …).

3.1.3 Fiche « Infrastructure du réseau local »

	Objectif
Tout site, immeuble ou groupe d'immeubles rassemblés sur un « site géographique », doit disposer d'une infrastructure de câblage permettant la mise en œuvre d'un **réseau local**, ensemble d'éléments actifs, qui relie physiquement des ordinateurs et leurs périphériques. Le réseau local permet aux utilisateurs l'échange et le partage d'informations, ainsi que l'accès aux ressources et aux applications sur le site. Le réseau local peut être divisé physiquement (par action sur le câblage) ou logiquement (par action sur les éléments actifs) créant ainsi des segments dédiés à des domaines ciblés comme le segment Pénal, segment Civil, le segment administration, le segment « public » (salle d'audiences, accueil,…), le segment éducatif…. Lorsque historiquement, plusieurs réseaux locaux sont présents sur un site immobilier, ceux-ci doivent être interconnectés de façon à partager les ressources communes, notamment l'accès au réseau distant Réseau Privé Virtuel Justice (RPVJ). L'installation des réseaux locaux et le câblage des immeubles sont nécessairement progressifs dans le temps, il faut donc s'assurer, préalablement au déploiement d'une application, que l'infrastructure réseau composée d'une structure de câblage équipée d'éléments actifs est en place.	

champ d'application	Produits préconisés : commentaire
Câblage structuré des bâtiments	La conception d'un réseau local et sa mise en œuvre dépendent de la structure de câblage du site. Pour cela chaque fois que cela est possible, la mise en place d'un câblage structuré doit être réalisée : • à la construction de nouveaux immeubles • à la réhabilitation de bâtiments • à la mise en place d'applications importantes nécessitant d'importants travaux de câblage • à la mise en place du RPVJ. La conception d'un câblage structuré doit être menée en prenant en compte la topologie des bâtiments ou groupes d'immeubles constituant le site. Toutes les zones d'un bâtiment doivent être câblées, cependant des réflexions sont à mener pour les zones dites sensibles ou publiques mais aussi dans les bâtiments historiques. Toutefois, quelle que soit l'étendue du câblage à effectuer sur un site, il conviendra de respecter les normes liées à la mise en place d'un câblage structuré. Le système de câblage structuré s'appuie sur la Norme ISO 11801 édition 2 ainsi que les normes européennes EN50173 et EN50174. Ces normes couvrent principalement les domaines comme : • la topologie du câblage • les distances • les types de support et leur utilisation • les spécifications des connecteurs • les terminaisons et l'installation Un système de câblage structuré réalisé par un installateur agréé, permet de bénéficier d'une garantie constructeur. Une telle mise en œuvre garantit une souplesse d'installation du réseau local indépendante des applications, permettant de mettre ainsi en place une exploitation de qualité et évolutive du site.

Topologie du câblage structuré

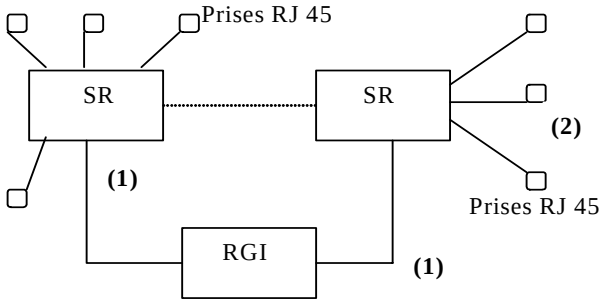
Les points d'accès informatiques ou prises terminales implantés dans chacun des bureaux sont raccordés par des liaisons paires torsadées en étoile depuis un local technique appelé « Local de sous répartition - SR ».
Dans certains cas très particuliers, l'usage de la fibre optique pourrait s'avérer nécessaire.

Les sous-répartiteurs assurant la distribution des zones de bureaux sont concentrés par des liaisons fibres optiques ou paires torsadées au « Répartiteur Général Informatique (RGI) » soit directement soit au travers d'un autre sous-répartiteur.

Topologie du réseau local

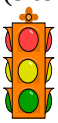
Les sous-répartiteurs accueillent les éléments actifs (concentrateur de terminaux, commutateur, etc..) du réseau local et permettent ainsi de raccorder physiquement et logiquement les équipements informatiques entre eux.

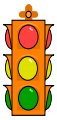
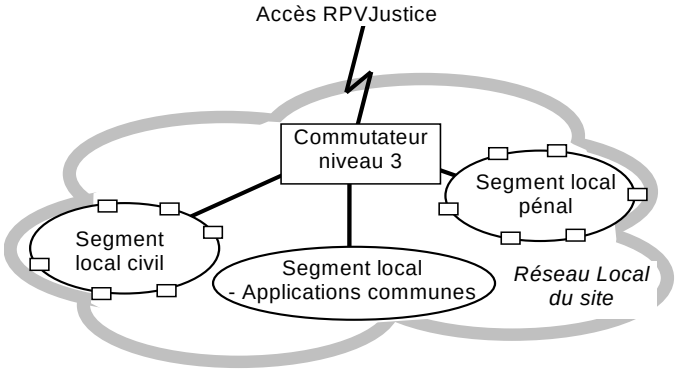
Le Répartiteur Général Informatique accueille les éléments actifs permettant le raccordement et l'interconnexion des différents locaux de sous-répartition.



(1) **artère ou rocade** :
Support cuivre paires torsadées cat 6
Support fibre optique

(2) **réseau capillaire** :
Support cuivre 4 paires torsadées cat 6

Les types de support	Lorsque le site géographique le permet, les interconnexions entre bâtiments sont réalisées principalement en fibre optique multimode qui bénéficie de caractéristiques autorisant des débits élevés > 100 Mégabits et d'un haut degré de sécurité. La fibre optique monomode pourraient être utilisée en cas de nécessité. A l'intérieur d'un même bâtiment, les liaisons entre sous-répartiteurs, ou des sous-répartiteurs vers le répartiteur général informatique, sont de préférence réalisées en fibre optique multimode. Le support préconisé pour la distribution vers les zones de bureaux depuis le sous-répartiteur est la paire torsadée cuivre 100 Ohms FTP de catégorie 6 Classe E. Les installations doivent être effectuées en utilisant la catégorie en vigueur au moment des travaux de câblage, et permettre au minimum des débits à 100 Mbits/s. Les bureaux et les zones câblées sont équipés d'un point d'accès informatique (point terminal de la distribution depuis le SR) composé de prises courant fort et de prises courant faible. Le connecteur de type RJ45 défini par la Norme ISO 8877 est utilisé pour toute distribution en paires torsadées. Dans certains cas très particuliers liés au respect des normes, où l'irrigation entre le sous répartiteur et le bureau sera réalisée en fibre optique, le connecteur sera de type SC.
Protocole de communication	Ethernet 10 baseT , 100 baseT, 1000 baseT avec un protocole conforme à la norme IEEE 802.3 Cette norme, de loin la plus répandue sur le marché, garantit l'interconnexion des équipements même lorsque ceux-ci émanent de fournisseurs différents. Le protocole est basé sur l'émission libre de données sur le réseau, et la réémission en cas de détection de collision après un laps de temps aléatoire (CSMA/CD). Cette norme permet de garantir une vitesse de transmission de 10 Mbits/seconde ou 100 Mbits/seconde ou 1000 Mbits/s sur un support de type paire torsadée (FTP) et normalise le connecteur RJ45 (4 paires) catégorie 6.
Complément au système de câblage structuré	Malgré les limitations actuelles en matière de distance et de bande passante, la technologie du réseau sans fil apporte une solution complémentaire pour les raccordements d'équipements situés dans une zone non adaptée au câblage (site classé).  Chaque mise en œuvre de solution sans fil doit être réalisée avec un protocole conforme à la version de la norme 802.11 qui intègre les niveaux de sécurité renforcée et doit faire l'objet d'une étude et validation conjointe CPR-FSSI.

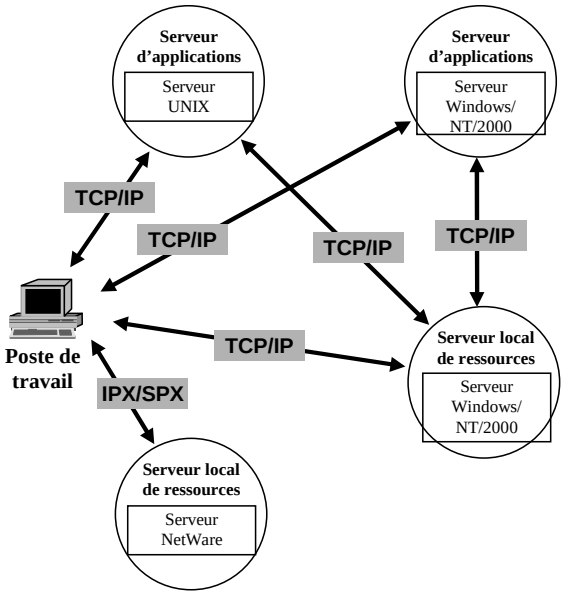
Produit	Conditions d'application : commentaire
Câblage, structuré du réseau local	Se conformer au cahier des clauses techniques de câblage établi par la Sous-Direction de l'Informatique et disponible dans les centres de prestations régionaux, ainsi que sur le site DAGE rubrique informatique, RPVJ et Intranet.
Dispositifs de connexion et de commutation	
Connexion des équipements	Les éléments actifs (Répéteur Ethernet ou HUB, Commutateur, Pont/routeur) installés sur le câblage constituent le réseau local Ethernet. 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 • pour des raisons financières, une alternative commutateur niveau 2 + routeur.  L'interconnexion des segments au niveau d'un bâtiment doit faire l'objet d'une validation technique de la Sous-Direction de l'Informatique (CPR, ATI). Les supports juridiques destinés à l'acquisition d'équipements réseaux au plan national, spécifient, sous forme de configurations types, différents modèles de commutateurs et routeurs adaptés à la topologie des réseaux du Ministère de la Justice. Le schéma logique d'interconnexion sera par exemple le suivant 
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 voir une liaison à 1000 Mbits/s

3.1.4 Fiche « Protocole du réseau local »

	Objectifs :

Le protocole du réseau local décrit les protocoles de communication de haut niveau nécessaires aux machines pour communiquer entre elles. Les protocoles cités ici (TCP/IP ou IPX/SPX) sont des protocoles dits « de transport » qui viennent se placer au-dessus des protocoles réseaux utilisés (CSMA/CD).

	Produits préconisés :
champ d'application	**commentaire**
Protocoles d'échange entre les différentes plates-formes	Le schéma suivant fournit les protocoles préconisés pour les échanges entre les différentes plates-formes :



TCP/IP

TCP/IP est le protocole standard pour les communications entre les machines du Ministère.
TCP/IP doit être utilisé à chaque fois que c'est possible. Cependant, pour des raisons historiques, d'autres protocoles peuvent subsister, tels DSA ou IPX/SPX, pour communiquer avec des machines qui ne supportent pas TCP/IP, comme c'est le cas notamment des serveurs Netware ou des « mainframes » BULL.

TCP (Transmission Control Program) est un protocole permettant l'ouverture de circuits virtuels entre applications.
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).
Ces deux protocoles sont utilisés au-dessus des couches physiques standard Ethernet 802.3.
De nombreux outils accompagnent généralement les implémentations de TCP/IP, regroupés en quatre catégories :

- applications permettant des connexions à distances (rlogin, telnet),
- applications permettant de faire du transfert de fichiers (rcp, ftp),
- applications permettant de réaliser des commandes à distance (rsh),
- d'autres applications plus avancées (messagerie, partage de fichiers, Intranet...).

Protocole d'échange entre les postes de travail et le serveur de réseau local	TCP/IP est le protocole standard pour toutes les communications entre les machines du ministère. IPX/SPX, protocole propriétaire Novell peut être utilisé au Ministère pour gérer les communications entre les postes de travail et les serveurs locaux de ressources fonctionnant encore sous Netware et TwinServer. IPX/SPX inclut des fonctions proches de celles de TCP/IP. C'est le seul protocole fonctionnant correctement pour communiquer avec les serveurs Netware de version < 5.x. ⇒ **Le paramétrage du RPVJ et les équipements de routage ne sont pas prévus pour « router » le protocole IPX/SPX. Celui-ci ne doit donc être utilisé que pour des communications internes à un site.** IPX/SPX doit être remplacer progressivement par TCP/IP lors du remplacement des serveurs fonctionnant sous Netware par des serveurs sous Windows 2000.
Protocole d'échange avec les serveurs d'applications	TCP/IP est le protocole préconisé pour les échanges avec les serveurs d'applications au sein du Ministère. La gestion de ce protocole est incluse dans les systèmes d'exploitation Linux, UNIX et Windows NT/2000. **Pour les postes de travail PC sous Windows, on utilisera exclusivement l'implémentation fournie par Microsoft, qui offre l'interface WINSOCK (Windows Sockets).**

	Conditions d'application :
Produit	**Commentaire**
Cohabitation IPX/SPX et TCP/IP	L'ensemble de l'infrastructure du Système d'Information du Ministère est conçu pour supporter le protocole TCP/IP, notamment le nommage (DNS) et l'adressage des machines ainsi que le paramétrage des routeurs. La mise en oeuvre de TCP/IP au sein des projets devra se conformer à ces règles. La coexistence sur un même réseau local de protocole IPX et TCP/IP est possible, mais pose le problème de la dualité d'accès à des serveurs IP et IPX sur le même poste de travail. L'utilisation du protocole NETBIOS over TCP/IP (normalisé) est la seule autorisée.

3.1.5 Fiche « réseau distant »

	Objectif

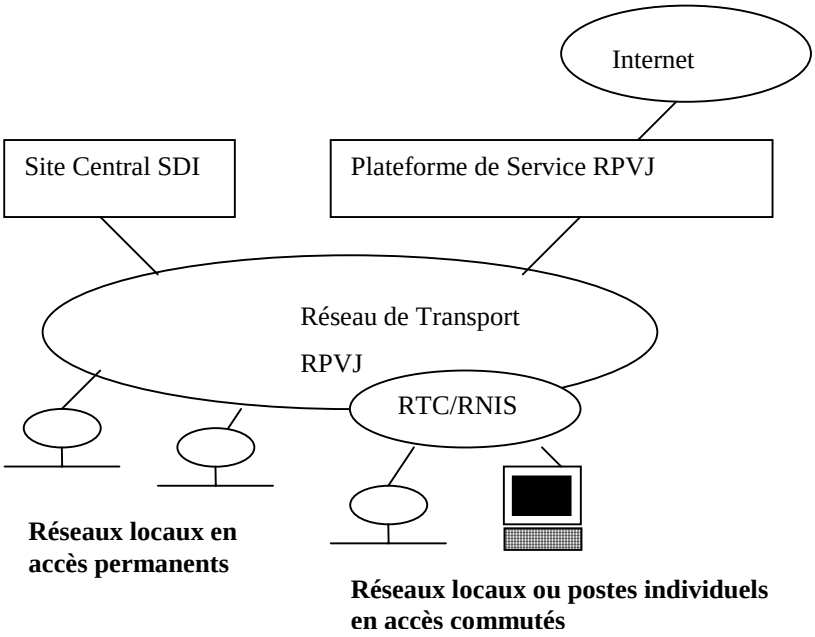
Au-delà des applications et des données accessibles sur son poste de travail ou sur un serveur local, l'utilisateur doit pouvoir :

- Accéder à des applications hébergées sur des serveurs distants
- Echanger des informations avec d'autres services du Ministère de la Justice
- Communiquer avec les environnements informatiques des interlocuteurs du Ministère de la Justice.

Les supports de télécommunication sur lesquels sont développées les interfaces applicatifs et les échanges de messages doivent respecter à un certain nombre de recommandations :

- Utiliser l'infrastructure du RPVJ
- Ne retenir que les protocoles de communication normalisés ou standards de fait. Le recours à un protocole « propriétaire » s'avère cependant parfois nécessaire pour tenir compte de l'existant.
- Retenir l'architecture adéquate en fonction de l'analyse des flux (volume, débit, temps de réponse...).

	Produits préconisés :
champ d'application	**commentaire**
Infrastructure de communication – Types de Liaisons	
Informatique nationale et interconnexion de sites	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. A la date d'actualisation de la présente fiche, le RPVJ est basé sur l'offre Global Intranet de France Télécom [le marché couvre la période 2004 – 2007]. 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. L'utilisation d'un tel réseau permet de partager les investissements nécessaires sur l'épine dorsale – garantie de qualité de service en phase d'explosion de la consommation de bande passante – avec les autres clients de l'offre tout en garantissant un excellent niveau de sécurité au travers de l'utilisation de « tunnels IP » virtuels. Pour les besoins de l'informatique nationale, le ministère de la justice s'est fixé comme objectif d'utiliser le RPVJ pour les transmissions de données. Pour les besoins d'interconnexion de sites physiques distants, le RPVJ constitue une solution technique suffisante pour tout système d'information local travaillant en mode client léger (web ou Citrix) ou asynchrone (messagerie). Les centres de prestations régionaux (CPR) doivent être sollicités par les services déconcentrés et les juridictions à qualifier leurs besoins afin de déterminer si le RPVJ, solution à examiner en priorité, est suffisante.



Le RPVJ se compose d'une part d'un réseau de transport (dénommé Equant IP VPN dans l'offre France Télécom Transpac) et d'autre part d'une plate-forme de service (localisée chez France Télécom/Transpac à Nanterre).

Le réseau de transport :

- Assure la connexion des réseaux locaux implantés dans les sites Justice, soit par des accès permanents, soit par des accès commutés RNIS.
- Assure la connexion des postes individuels (nomades) généralement par des accès du réseau téléphonique commuté traditionnel (le RTC) ou éventuellement par le RNIS.
- 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 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.

Une telle architecture évite aux sites de multiplier les accès (une même connexion donne accès à l'intranet et à l'Internet) ; elle permet en outre le regroupement et la mutualisation des moyens nécessaires à la sécurité et à sa gestion.

Parmi les sites connectés au RPVJ par un accès permanent, le site central joue un rôle particulier. En effet il héberge des serveurs qui participent au service offert par le RPVJ. Il s'agit en particulier du serveur de messagerie centrale, de l'annuaire Justice, de serveurs WEB et FTP de l'intranet et d'autres fonctions techniques (comme le pont de messagerie, le serveur DNS, l'antivirus SMTP …).

Besoins locaux

Si des besoins géographiquement proches nécessitent :

- soit la constitution d'un réseau local étendu incluant un site urbain permettant de mutualiser l'accès distant au RPVJ,
- soit le routage d'un protocole autre que IP,
- soit la mise en relation d'application client serveur lourd nécessitant une bande passante importante,

le recours à la location de liaisons point à point peut s'avérer nécessaire.

	Sur ce segment de marché, la concurrence est ouverte entre les principaux opérateurs du marché ou autres fournisseurs locaux. Services déconcentrés et juridictions doivent se rapprocher des CPR pour les aider à préparer les consultations nécessaires.
Protocoles du réseau distant	
Protocole IP	Le protocole TCP/IP est le protocole retenu comme standard pour les communications entre les sites du Ministère. Ce protocole est routé sur chaque site par l'équipement loué avec l'accès RPVJ auprès de l'opérateur en charge de l'externalisation de ce réseau.
Protocole CHAP	Les liaisons entre les sites du Ministère qui utilisent, à titre transitoire, des lignes commutées, RNIS ou RTC, doivent être sécurisées de façon à éviter les intrusions. Le protocole à utiliser est le service d'authentification CHAP (Challenge Hash Authentication Protocol) de la ressource appelante.
Protocole 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.
	Conditions d'application :
Produit	**commentaire**
Informatique nationale et interconnexion de sites	Le RPVJ est destiné à irriguer 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 de communication	L'architecture de communication, constituée d'un ensemble cohérent de postes de travail, de serveurs et de dispositifs techniques de réseau doit être la plus homogène possible entre les services, la plus stable possible dans le temps, la plus indépendante possible des domaines d'applications. Le Réseau Privé Virtuel Justice propose des différents modes de connexions à choisir en fonction des besoins. Tous permettent une connectivité « any to any » vers n'importe quel autre accès du RPVJ. • Des accès permanents à facturation forfaitaire, avec ou sans possibilité de prioriser des flux pour garantir un temps de transit constant, • Des accès commutés via RNIS ou RTC, facturation à la durée de communication • L'accès IPSEC (tunnel crypté via Internet) pour les TOM uniquement. Pour plus de détail voir le guide RPVJ accessible à partir de : http://intranet.justice.gouv.fr/rpvj On trouvera ci-après un tableau listant les principaux critères à utiliser dans la sélection du type d'accès le plus approprié. Le site contient aussi les éléments de tarification et des informations complémentaires. Pour les liaisons DOM/TOM, seul un sous-ensemble des modes de connexion est disponible. Les gestionnaires sont invités à consulter le guide du RPVJ et à contacter le bureau ATI qui pourra les conseiller utilement dans leurs choix et les guider au cours de la mise en place.

Critères	Type d'accès conseillé
• Quelques postes connectés par un réseau local. • Le nombre d'utilisateurs se connectant aux services RPVJ est théoriquement illimité, mais la bande passante disponible (64 Kb/s) limite le nombre de connexions simultanées. • La durée de connexion ne dépasse pas **1 heure par jour**. • Le site n'est pas éligible ADSL (offre IP-VPN-ADSL-Light non disponible sur ce site). • La fonction de Call-back est intégrée pour ces accès permettant des accès épisodiques aux serveurs hébergés sur ce site (télémaintenance). • La CoS est configurée au niveau du point de concentration unique secouru.	**IP-VPN-SRL**
• Un poste isolé ou nomade. • Les utilisateurs ont toujours l'initiative de la connexion. • La durée de connexion est faible (**moins de 1 heure par jour**).	**IP-VPN-SPI**
ACCÈS PERMANENT (préconisé)	
• Quelques postes connectés par un réseau local. • Le nombre d'utilisateurs se connectant aux services RPVJ **ne dépasse pas 5 personnes**. • Le site peut comporter un serveur qui nécessite d'être accédé depuis le RPVJ mais ce n'est pas le besoin dominant (télémaintenance). • La CoS est configurée au niveau du point de concentration unique secouru. • La zone géographique où se trouve le site est couverte par le déploiement ADSL de France Télécom. • Facturation forfaitaire pour l'accès ADSL et pour l'abonnement à la ligne RTC dédiée.	**IP-VPN-ADSL-Light** *(accès permanent, sans bande passante garantie* ***sans priorisation des flux)***
• Plusieurs classes de débit sont disponibles, à choisir en fonction du nombre d'utilisateurs et de postes connectés au réseau local. Les débits sont asymétriques. • Les utilisateurs accèdent à des applications métiers à travers le RPVJ, ce type d'accès supportant la définition de classes de services (CoS) • Le site peut comporter un serveur qui nécessite d'être accédé épisodiquement depuis le RPVJ, mais ce n'est pas le besoin dominant. • La zone géographique où se trouve le site est couverte par le déploiement ADSL de France Télécom et la classe de débit souhaitée est disponible pour ce site.	**IP-VPN-ADSL-Gold** *(accès permanent, à debit symétrique, avec bande passante garantie et priorisation des flux)*
• Plusieurs classes de débit sont disponibles, à choisir en fonction du nombre d'utilisateurs et de postes connectés au réseau local. • Les utilisateurs accèdent à des applications métiers à travers le RPVJ, ce type d'accès supportant la définition de classes de services (CoS). • Les débits sont symétriques (le débit montant est égal au débit descendant). Cette symétrie permet d'héberger sur le site un ou plusieurs serveurs accédés depuis le RPVJ de façon fréquente. • La zone géographique où se trouve le site est couverte par le déploiement SDSL de France Télécom et la classe de débit souhaitée est disponible pour ce site.et durables avec un ou plusieurs autres sites du RPVJ.	**IP-VPN-SDSL-Gold** *(accès permanent, à debit symétrique, avec bande passante garantie et priorisation des flux*

• Plusieurs classes de débit sont disponibles, à choisir en fonction du nombre d'utilisateurs et de postes connectés au réseau local. • Les utilisateurs accèdent à des applications métiers à travers le RPVJ, ce type d'accès supportant la définition de classes de services (CoS). • Et/ou le site comporte un serveur qui nécessite d'être accédé depuis le RPVJ de façon fréquente. • Et/ou le site est concerné par des échanges transverses intenses et durables avec un ou plusieurs autres sites du RPVJ. • Le site n'est pas éligible ADSL/SDSL (offres IP-VPN-ADSL-Gold et IP-VPN-SDSL-Gold non disponibles sur ce site) ou la classe de débit souhaitée n'est pas disponible dans les autres types d'accès. • Dans le cas de IP-VPN-LL-Gold Haut débit (supérieur à 2 Mbps), la mise en place de cet accès haut débit nécessite le déploiement de fibre optique et, par conséquent, des travaux de génie civil, de mise en place de répartiteurs optiques.	**IP-VPN-LL-Gold**

L'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 (cf. note ci-dessous). La table des virus connus est mise à jour dès que les virus sont détectés par un laboratoire spécialisé.

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 :

- Les adresses internes au RPVJ sont masquées à l'égard d'Internet
- 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.
- Les connexions « entrantes » sont interdites (seuls les messages en provenance de l'Internet sont admis par le pare-feu).

L'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

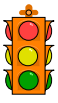
Les messages sont redirigés ensuite vers le relais « Central » justice interne. Ce relais « Central » se charge enfin d'orienter les messages vers les serveurs de messagerie hébergeant la boîte à lettres de l'utilisateur Justice.

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 Extranets Avoués et Avocats.

Dans l'avenir, d'autres interconnexions pourront être envisagées : huissiers de justice, notaires, experts judiciaires et autres.



NB : Par défaut, seuls les protocoles réellement utilisés sont autorisés par le dispositif de sécurité du RPVJ. Toute utilisation d'un port non standard doit faire l'objet d'une demande d'ouverture auprès de DAGE/SDI/ATI.

Besoins locaux	***Dans le cadre d'interconnexions de réseaux locaux via liaison RNIS, il faut impérativement s'assurer que les équipements d'interconnexion (routeurs) supportent le protocole CHAP.***  ***Si une étude s'avère nécessaire pour mettre en place une liaison afin de répondre à des besoins locaux, celle-ci doit être soumise à la validation des CPR(s), notamment si cette liaison n'est pas point à point.***

3.1.6 Fiche « Connexion au RPVJ des postes nomades »

La connexion de postes nomades est possible à partir d'une prise téléphonique du réseau téléphonique commuté (RTC) public.

Pour préserver la confidentialité des données justice, plusieurs niveaux de protection sont prévus.

	Elément préconisé:
Champ d'application	**Commentaire**
Poste nomade	Poste portable selon besoin et utilisation, voir support juridique des postes portables.
Sécurité d'accès au poste	Les recommandations de sécurisation des postes sont obligatoires. Voir http://intranet.justice.gouv.fr/securite/DOCS/DIR-7.pdf
Fonctionnement en site / hors site	L'utilisateur nomade situé sur son site justice s'identifie et se raccorde à son réseau local de manière classique, à travers une interface d'accès au réseau local. En situation de nomade, l'interface d'accès est inactive. Le système d'exploitation du poste nomade détecte alors que l'identification et le raccordement à un serveur local de ressources n'est pas possible. Il demande l'ouverture d'une session en autonome. L'utilisateur doit émettre la même authentification (mot de passe ou clé physique) que sur son site justice.
Réseau d'accès	Le réseau physique d'accès est le réseau téléphonique commuté public (RTC), accessible à partir d'un point d'accès individuel analogique d'un opérateur de réseau et de service téléphonique ouvert au public.
Sécurisation de l'accès réseau	Un accès GI-SPI est obligatoire. Le mot de passe de cet accès est passé manuellement par l'utilisateur. Il doit être renouvelé tous les six mois.
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 selon ce mode sont : • la messagerie électronique ministérielle, • l'intranet ministériel. 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 total de ceux-ci) sont envoyées tous les six mois aux directeurs concernés, pour contrôle.

3.1.7 Fiche « Serveurs »

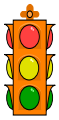
	Objectif
L'objectif de ce thème est de définir les matériels susceptibles de supporter les serveurs de différents types ainsi que les contraintes qui les accompagnent et les sécurités à mettre en place. Les définitions et principes d'usage des serveurs sont donnés en 2.1 Définitions et principes généraux pour l'équipement des sites. Deux grands types de serveurs matériels : ➢ serveurs matériels banalisés INTEL, ces plates-formes multi-constructeurs supportent différent système d'exploitation : Netware, Windows, Linux, … ; ➢ serveurs propriétaires : le constructeur lie de façon très étroite et incontournable la plate-forme matérielle et le système d'exploitation de base.	

	Produits préconisés :
champ d'application	**commentaire**
Serveurs banalisés Intel	Les supports juridiques destinés à l'acquisition de serveur au plan national spécifient, sous forme de configurations types, différents modèles de serveur adaptés essentiellement au volume des traitements à supporter (nombre d'utilisateurs, volume des bases, nombre de ressources) et aux performances attendues (temps de réponse, niveau de sécurité, …) pour couvrir les différents types de missions. 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.
Configuration type	Type 1 : Serveur pour petit site (- de 20 postes) et application non critique Type 2 : Serveur pour petit site (- de 20 postes) et application critique Type 3 :Serveur pour site moyen (- de 35 postes) comprenant une base de données Type 4 : Serveur pour site important et/ou application critique Type 5 : Serveur de traitement pour application de type client léger Type 6 : Serveur pour site important comprenant plusieurs bases de données Type 7 : Serveur haute disponibilité (cluster) Type 8 : Serveur centralisé de sauvegarde Type 9 : Serveur pour fermes de serveurs Le détail de ces configurations est publié sur l'Intranet DAGE (Informatique/Marchés) à l'adresse : http://intranet.justice.gouv.fr/dage/sdi/PRI-National.htm
Unité centrale	Voir puissance suivant les modèles types
Mémoire	Selon modèle type, configuration particulière à prévoir selon usage.
Disque	Selon modèle type, configuration particulière à prévoir selon usage.
connexion réseau	Carte Ethernet 10 /100 Mbits -

Serveurs propriétaires	Les supports juridiques sont spécifiques et réservés aux acquisitions par l'administration centrale. Serveurs d'une capacité en générale supérieure aux configurations Intel, leur acquisition est justifiée par le contexte applicatif ou technique.
Bull/DPS7	Mainframes sous système d'exploitation GCOS7 Ce matériel reste supporté jusqu'à la migration/ré-écriture des applications qui les supportent (NCP, Sigma/Thémis, NCJ, GAP).
Serveurs de production sous UNIX	Serveur-mainframe sous le système d'exploitation AIX ou HP-UX. Serveur réservé au support d'application et de base de données nationale demandant une forte puissance informatique. Le premier doit être favorisé.

	Conditions d'application :
Produit	**commentaire**
Configuration	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 centres de prestations régionaux (CPR). La liste des matériels pour lesquels le SNM intervient est publiée sur le site intranet de la DAGE http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SNM2JUIN.htm. Cette liste est nécessairement limitative afin d'assurer une qualité de support correcte : en effet, tant les équipes du ministère de la justice que celles des sous-traitants chargés de la maintenance des postes de travail ne peuvent maintenir de relations techniques et commerciales qu'avec un nombre limité de constructeurs et/ou de fournisseurs. Si cette liste est susceptible d'évoluer dans le temps, les items la constituant ne sont retirés que lorsque les matériels correspondants ont été entièrement retirés du service opérationnel au sein du système d'information justice.
Sécurité	Il est recommandé de sécuriser au maximum les serveurs, aussi bien au niveau matériel que logiciel. Suivre les recommandations : http://intranet.justice.gouv.fr/securite/GUIDE/HOME.HTM Une directive particulière pour la protection des salles serveurs : http://intranet.justice.gouv.fr/securite/DOCS/Dir-6.PDF

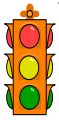
3.1.8 Fiche « Serveur local de ressources »

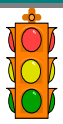
	Objectif
Le serveur local de ressources doit être l'élément fédérateur pour les utilisateurs du réseau local. A ce titre il permet, en fonction des opportunités, le partage d'équipements spécialisés (sauvegarde, télécopie, modem, imprimantes couleur ou haut débit...). Le serveur local de ressources doit également être l'environnement de prédilection pour le partage de fichiers entre utilisateurs et le stockage d'informations personnalisées dans un espace réservé. La mutualisation de l'espace de stockage réservé aux utilisateurs au niveau du serveur de réseau local est d'ailleurs une des fonctions premières souhaitées. Ceci autant pour des raisons économiques que de sécurité (sauvegardes, confidentialité...). Dans ce même ordre d'idées, l'installation des logiciels bureautiques sur le serveur de réseau local et leur accès par les utilisateurs à partir des postes de travail peut faire partie des objectifs recherchés. Une telle solution permet en effet de limiter l'effort de migration lors de changement de versions.	
	Produits préconisés :
champ d'application	**commentaire**
Système d'exploitation du serveur local de ressources	
Windows 2000 Server	Windows 2000 de la société Microsoft, remplacera progressivement Netware et Windows NT. Windows 2000 possède les avantages : • de disposer d'un bon crédit en terme de pérennité, • d'être largement supporté par la quasi-totalité des éditeurs du marché, • d'offrir des possibilités multiprocesseurs, • d'être un système fiable et convivial (apprécié des utilisateurs). Ce système d'exploitation est recommandé pour tous les serveurs locaux de ressources mis en œuvre à partir du 01/07/2001.  ***Nécessite l'obtention d'une CAL (licence d'accès client) pour chaque poste client susceptible d'y accéder.***
Linux - Samba	Samba (logiciel libre) permet d'étendre les possibilités des serveurs Linux pour qu'ils gèrent des ressources partagées, accessibles depuis des postes de travail. Le support technique peut être assuré par la SDI dans le cadre de ses marchés.
Windows NT 4.0	Quelques serveurs ont été installés avec ce système. Fin de commercialisation par Microsoft le 1/10/2001. Il n'est plus supporté sur notre environnement depuis 01/01/2003. **Plan de migration à prévoir**
Netware 3.20	NetWare 3, de la société Novell, est le gestionnaire de réseau local largement implanté dans les années 90 au Ministère. Ce système présente des qualités marquées, notamment en ce qui concerne la stabilité. Toutefois, les doutes persistants sur la pérennité de son éditeur (Novell) et l'état du marché ont conduit le ministère à modifier ses préconisations. Ce système n'est plus supporté depuis le 01/01/2004. **Plan de migration à prévoir**
Netware 4.x et 5.x	Ces systèmes ont été installés par certains services (y compris la SDI) dans la droite ligne de la préconisation antérieure. Netware 4 n'est plus supporté par la SDI depuis le 01/01/2004, et Netware 5 ne le sera plus au 01/01/2005 (date susceptible d'être modifié au vu des parcs).

Equipement du réseau local	***Tout réseau local devrait posséder au moins un serveur local de ressources.*** Pour que le réseau local fonctionne, il faut qu'il soit équipé d'au moins un **serveur en local** remplissant les fonctions de serveur d'accueil (sous Windows NT/2000, on parle de contrôleur de domaine, documentation sur l'intranet). Le serveur d'accueil est nécessaire notamment lors de la connexion des postes de travail, pour leur fournir les données d'identification et d'authentification de l'utilisateur, et leur restituer son environnement de travail.
Rôle du serveur local de ressources	***Le serveur local est banalisé - donc indépendant des applications -*** Les serveurs locaux de ressources fournissent les services suivants : • fonctions techniques au sein du réseau local Services d'accueil, de partage de fichiers, d'inventaire, d'anti-virus • Partage de périphériques Sauvegarde, imprimantes, scanner, télécopie, ….
Partage de ressources par un serveur d'applications	Le recours au partage de ressources intégré dans le serveur d'applications doit être expressément réservé aux besoins de l'application concernée.
	Conditions d'application :
Produit	**commentaire**
Serveurs Netware	Le passage à une version 4.x ou 5.x ne doit pas être privilégié. L'alternative Windows 2000 doit être étudiée. Se reporter à la Fiche « Protocole du réseau local » (3.1.4) pour une information sur la connectivité des serveurs de réseau local.
Exploitation du serveur local de ressources	***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*** Les sauvegardes sont sous la responsabilité des administrateurs. Les supports changés quotidiennement, doivent être impérativement stockés dans un coffre ignifuge ou externalisés.
Gestion des télécopies	Pas de produit particulièrement référencé

3.1.9 Fiche « Serveur d'applications ou de données »

Objectif
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.

Produits préconisés :	
champ d'application	**commentaire**
Système d'exploitation	
Linux	**Linux est le système d'exploitation à préférer pour les serveurs d'application du ministère.** La version à utiliser est Linux Red Hat 7.3 au minimum. Linux est un système d'exploitation largement répandu sur plate-forme à base de microprocesseur Intel et compatibles et profite par ailleurs d'une constante augmentation de puissance et de popularité, notamment auprès des éditeurs.
Microsoft Windows 2000 Server	Windows 2000 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. Le système Windows 2000 Server peut être retenu comme serveur d'application ou de données lorsque cela présente un intérêt économique, et lorsque les applications s'y prêtent. Les critères de choix entre Windows et Linux sont indiqués dans les conditions d'application qui suivent.  ***Nécessite l'obtention d'une CAL (licence d'accès client) pour chaque poste client susceptible d'y accéder.***
Microsoft Windows NT 4	Ce système n'a guère été utilisé au plan national que pour l'application GIBUS. ***Son utilisation n'est plus recommandée pour les nouveaux développements.***
UNIX SCO Open Server 5	***UNIX SCO Open Server 5 n'est plus recommandé pour les nouveaux développements.*** La migration vers Linux est engagée.
Unix de production : AIX, HP-UX	Ces systèmes UNIX constituent des choix possibles pour les applications de portée nationale ou départementale (cf. section 4) demandant une forte puissance informatique. Le premier doit être favorisé, sans que les applications fonctionnant sous le deuxième dussent faire l'objet de plans de migration.
BULL GCOS 7	Ce système propriétaire de la société Bull est inhérent aux applications transactionnelles développées sur « mainframe » Bull. Ce système n'est désormais retenu que pour les grandes applications en service à ce jour : NCP (nouvelle chaîne pénale), NCJ (casier judiciaire), SIGMA/THEMIS (comptabilité budgétaire)...
Netware	**Ce système d'exploitation de la société Novell ne doit pas être utilisé comme serveur d'application.** Seule dérogation pour assurer la continuité d'applications C/S construites avec un SGBD/R (« Network Load Module » ou NLM). Les applications nationales sous le SGBD/R **SQLBase** sont dans ce cas.

Produit	Conditions d'application : commentaire
Windows NT/2000 Server	 ***Les recommandations particulières concernant la mise en œuvre d'Active Directory[3], et notamment les normes de nommage, sont publiées sur le site intranet de la SDI.***
Rôle du serveur d'application	Les serveurs d'applications hébergent les applications et plus souvent les données associées nationales ou locales, certaines applications d'initiative locale, ainsi que des outils: • *d'administration* Habilitations, en plus de ce qui est géré au niveau applicatif ou au niveau serveur local de ressources, Télédistribution : machine servant à piloter le processus de télédistribution, Gestion de parc : machine contenant la base de données d'inventaire du parc, et pilotant le processus d'inventaire pour une région, ou une direction, Supervision de système : par exemple machine serveur ISM. • *de fonctions techniques* Messagerie, Groupware, GED, Vidéotex, Web, • *de services d'accès à certains périphériques d'exploitation de masse* Serveur de sauvegarde : pilotage du robot de sauvegarde, et sauvegarde de l'ensemble des serveurs du site. Serveur d'impression pour les impressions de masse • *de fonctions de communication de masse* Serveur de transfert de fichiers pour réaliser les transferts de masse entre les sites.
Rôle du serveur de données	Les serveurs de données hébergent des bases relatives à des applications nationales ou celles de portée départementale. Sa mise en place ne se justifie souvent qu'en cas de mutualisation des serveurs d'application ou pour des bases de données volumineuses.
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.

[3] le service d'annuaire de Microsoft

Indépendance des entités administratives	L'indépendance fonctionnelle des services ou des entités administratives doit être respectée. Ces services doivent rester propriétaires de leurs données, même si les serveurs sont partagés, installés sur des sites distants, ou télé-exploités. Ainsi, il est conseillé de créer une instance de base de données par application et par service. On veillera dans ce cas à ne pas faire de confusion entre les notions de base de données, de fichier et de table.
Choix entre LINUX et Windows NT/2000	Les critères de choix entre Linux et Windows 2000 pour les serveurs d'application 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. 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 2000 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. Par ailleurs il convient d'ajouter que dans tous les cas : • Linux peut être à préférer en cas de forts besoins de sécurité ou de disponibilité bien que des configurations à haute disponibilité soient proposées par les constructeurs sur des environnements W2000 à des coûts très élevés. • Linux est à préférer pour les serveurs d'applications destinés à être mutualisés, l'administration étant plus aisée dans cet environnement. • Windows 2000 Server est plutôt utilisé pour les petits serveurs spécialisés : serveurs GED, de messagerie, de groupware, serveurs Intranet.
Exploitation du serveur d'application/ données	Les sauvegardes sont sous la responsabilité des administrateurs. Les supports changés quotidiennement, doivent être impérativement stockés dans un coffre ignifuge ou externalisés.

3.2 Les services applicatifs

3.2.1 Règles générales

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

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.

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.

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 cadre de cohérence technique 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 en dehors 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.

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.

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. Une application ne peut donc pas accéder directement à une 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.

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.

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

3.2.2 Les services applicatifs du cadre de cohérence technique

3.2.2.1 Classification des services

Le tableau suivant dresse une typologie des services applicatifs transverses disponibles au-dessus des services d'infrastructure décrits plus haut :

Sécurité	**Applications de production ou d'infocentre Bureautique communicante et Intranet, Archivage, GED, Workflow, Knowledge, Internet et communication avec l'extérieur,...**			
Services d'administration	**Services de gestion des données**	**Services de communications**	**Services d'interface utilisateur**	**Services de développement**
○ Installation et changements ○ Gestion des opérations et des ressources ○ Comptabilité / Facturation ○ Gestion de la sécurité ○ Gestion des performances ○ Gestion des incidents ○ Annuaire	○ Base de données ○ Fichiers ○ Extraction / Injection ○ Tri ○ Conversions ○ Interfaces d'archivage	○ Echanges synchrones entre applications ○ Messagerie inter-applications ○ Transfert de fichiers ○ Services d'impression ○ Accès aux bases de données à distance ○ Accès aux fichiers à distance ○ Accès conversationnel ○ Soumission de travaux à distance	○ Interface graphique ○ (Interface caractère) ○ Accès aux données ○ Aide en ligne ○ Présentation des impressions	○ Langages de développement ○ Bibliothèques ○ Documentation ○ Outils de tests ○ Gestion des versions des composants logiciels
	Système d'exploitation — Plate-forme / Infrastructure réseau (se reporter au Chapitre 3.1)			

3.2.2.2 Opportunités technologiques

Les solutions disponibles pour bâtir une application sont de plus en plus diverses. Par exemple, une application de diffusion de documents pourra s'appuyer :

- sur un développement spécifique en architecture client-serveur, client léger ;
- sur des outils de travail collaboratif (type groupware) ;
- sur un outil de GED (Gestion Electronique de Documents) ;
- sur un serveur web Intranet.

Au-delà des choix de produits, les choix technologiques ont un impact de plus en plus déterminant sur les caractéristiques des applications : coût des licences, performances, possibilités de télédiffusion, gestion de la sécurité,...

Dans ce contexte, les technologies liées au WEB voient leur champ d'application s'étendre. Elles peuvent être appliquées à un nombre sans cesse grandissant d'applications, et elles sont séduisantes par la réduction des coûts de développement et surtout de déploiement qu'elles entraînent.

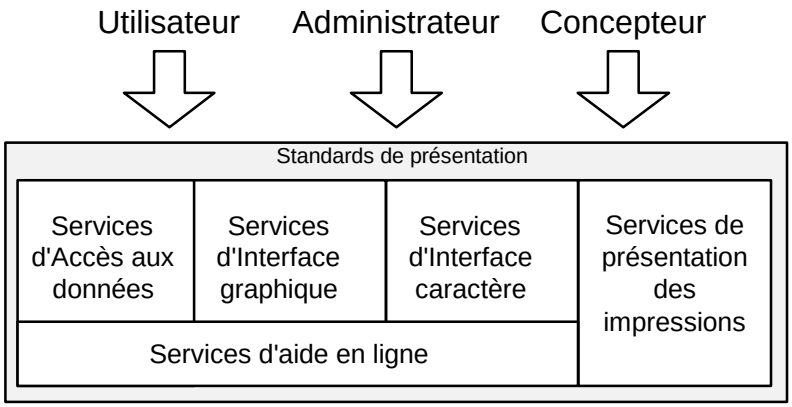
3.2.2.3 Organisation des fiches

La plupart des services mentionnés en 3.2.2.1 sont détaillés dans les fiches suivantes. Certaines applications génériques (bureautique multimédia et GED) sont également décrites.

Lorsqu'un service ne figure pas, cela signifie qu'aucun outil n'est aujourd'hui qualifié. La mise en oeuvre dans tel ou tel développement peut être l'occasion de le retenir, il est donc souhaitable d'en informer soit la Sous-Direction de l'Informatique soit les directions maîtrises d'ouvrage.

3.2.3 Services d'interface utilisateur

Objectif



Le schéma retenu pour ces services met en évidence leur rôle fédérateur par rapport aux environnements des différents acteurs (Utilisateurs, Administrateurs, Concepteurs d'applications).

Ces services s'appuient sur les différents standards de présentation qui unifient l'interface des applications, notamment au travers des guides de style, pour offrir l'utilisation la plus transparente possible des différents types de postes de travail. Ces standards peuvent être ceux d'organismes de normalisation, ceux du marché, ou ceux définis par la SDI.

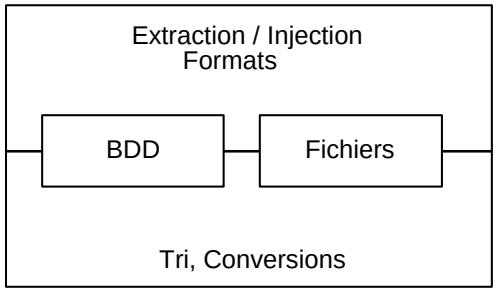
	Produits préconisés :
champ d'application	**commentaire**
les services d'interface graphique de base	Ces services fournissent, aux applications, les mécanismes de construction et de gestion des interfaces graphiques Plate-forme UNIX : • VT340 : interface graphique couleur. • X11 Motif : pour les applications fonctionnant sur stations de travail. • KDE ou Gnome pour PC sous Linux Plate-forme PC : • WINDOWS 98, avec évolution vers WINDOWS XP • X11 Motif : en émulation pour accéder aux applications fonctionnant sur stations de travail UNIX, ou aux outils résidant sur les serveurs UNIX. • Navigateur : pour les applications reposant sur les technologies web (interface graphique hypertexte de type HTML) - **Internet Explorer de Microsoft recommandé** - **Navigateur à base Mozilla 1.6 et au delà.** ⇒ ***Pour garantir leur compatibilité sur nos environnements mais aussi ceux de nos partenaires, les applications Internet devront se conformer au standard HTML4 défini par le W3C et pouvoir fonctionner avec Internet Explorer et tous les navigateurs à base Mozilla 1.6 et au delà. Elles n'utiliseront donc aucune des fonctions spécifiques à l'un ou l'autre des navigateurs.***
Guide d'ergonomie pour les applications WEB	Les développements pour navigateur s'efforceront de respecter les recommandations de la chartre graphique du gouvernement et sa déclinaison ministérielle

Standard Internet de présentation des données	Les principaux standards sont : • HTML (Hyper Text Markup Language) : un standard de description de documents incluant des balises hypertextes. • 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. • 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. • XHTML (eXtensible Hypertext Markup Language) : une reformulation du HTML 4.0 en XML, en quelque sorte une passerelle pour favoriser le passage du HTML au XML. ***Pour complément d'information :*** Site ADAE (voir liens utiles § 1.5)
Les services d'accès aux données	Ils regroupent les outils d'interrogation et de présentation des données**.** **SQL** (Structured Query Language) est un langage d'interrogation et de manipulation de tous les SGBDR actuels (Oracle, Sybase, MS Access et tous les autres). Elle est également mise en œuvre de manière plus conviviale à travers le langage **QBE** (Query By Example) que l'on retrouve seulement sur certains SGBD (Access par exemple). Pour générer des états, l'outil recommandé est le générateur associé à l'outil de développement. Pour les requêtes non prévisibles, on aura recours à un produit plus sophistiqué de type Business Objects, en ayant conscience qu'il faut mettre en place une architecture de publication appropriée. ➢ La partie serveur de **Business Objects** fonctionne sous UNIX ou sous Windows NT/2000. La partie client fonctionne en environnement Windows ou navigateur. Lorsque le coût d'un outil d'infocentre tel que Business Objects est jugé trop élevé, on peut également s'interfacer avec un tableur classique. Business objects, comme la plupart des outils de cette catégorie, offre une interface de type WEB, qui sera préférée à la solution classique lorsqu'elle s'avère utilisable. L'outil client est alors un navigateur WEB standard. ➢ Dans le cadre de l'environnement **SQLBase**, le logiciel **QUEST** (GUPTA, ex CENTURA SOFTWARE) permet d'établir des requêtes à la demande, sans obligatoirement définir de vue utilisateur de la base de données.

les services de présentation des impressions	Ils correspondent aux différents outils permettant à l'utilisateur de mettre en forme ses données en vue de l'impression. Le format standard recommandé à moyen terme pour la présentation des impressions à la demande est le format PDF (Portable Document Format), format propriétaire introduit par Adobe. Grâce au logiciel distribué gratuitement par Adobe, Acrobat Reader, il peut être lu sur plusieurs plates-formes (Windows, Mac OS, UNIX et LINUX), il s'exécute à partir d'un navigateur WEB standard.
Les services de prise de contrôle à distance	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, ...). Par ailleurs, ces outils sont très consommateurs en ressources réseau et il est recommandé, dans la mesure du possible, de ne les utiliser qu'en réseau local. **PcAnywhere** (Symantec) est un produit qui permet d'administrer un serveur distant et de prendre le contrôle d'un poste de travail. Il donne des niveaux de sécurité multiples pour assurer que les sessions de système hôte et élève soient sécurisées. Des mots de passe obligatoires empêchent les usagers non autorisés d'accéder à un hôte PcAnywhere, et les options d'authentification incluent maintenant FTP, HTTP, HTTPS, les domaines génériques LDAP, ADS, NDS, Novell Bindery, et NT. **Terminal Server** (Microsoft), intégré à Windows 2000 Server pour deux accès concurrents, il permet la prise en main à distance sur un serveur Windows 2000 à partir d'une station sous OS Microsoft. Il ne permet pas de transfert de fichier, ni de prise de main à distance sur les postes utilisateurs. **NetMeeting** (Microsoft) est gratuit et offre outre la visioconférence point à point, le contrôle à distance sur le réseau TCP/IP (Internet, RPVJ, résau local) de tout poste de travail équipé de NetMeeting. **LANDESK Management suite** (Intel) est implanté par la Sous-Direction de l'Informatique pour l'administration des serveurs des applications XTI. Il offre un niveau de fonctionnalité analogue à PcAnywhere. A titre expérimental, **TightVNC** (OpenSource) pour les postes de travail uniquement, en respectant bien les consignes de configurations minimum (voir site DAGE/SDI/ATI)

3.2.4 Services de gestion des données

	Objectif
Les services de cette classe aident les applications à utiliser les données des systèmes informatiques.	



Un système de gestion de base de données (SGBD) est un logiciel qui offre l'ensemble des services nécessaires à l'utilisation d'une base de données (stockage, modification, accès aux données...) d'une façon organisée, efficace et fiable.

Dans le domaine des systèmes ouverts, les SGBD relationnels sont caractérisés par l'interface SQL (Structured Query Language) qui est normalisée et assure l'accès transparent aux données et la portabilité des applications entre les SGBD-R.

Actuellement la plate-forme Netware avec un SGBD-R s'appuyant sur les NLM est une composante de l'architecture du ministère.

	Produits préconisés :
champ d'application	**Commentaire**
les services de bases de données	Ces services fournissent les interfaces permettant aux applications d'accéder aux bases de données. Ils comprennent également les mécanismes de définition et de structuration des bases (langages de définition de bases de données, par exemple). Les serveurs support sont de type « serveur d'application ».
Sur plate-forme UNIX/Linux	**ORACLE**, conforme à SQL, préconisé pour les bases importantes **MySQL** (logiciel libre) très rapide, fiable et facile à utiliser sous Linux, offre aujourd'hui un ensemble de fonctionnalités large et riche. Sa rapidité et sa sécurisation en font un outil idéal pour les applications Internet.
Sur plate-forme Windows NT/2000 Server	**ORACLE** dans la même version que sur serveur UNIX **SQLBase** (Société Gupta, ex Centura Software), associé à l'outil de développement Team Developer. La version minimum à utiliser sur plate-forme Windows 2000 Server est **SQLBase 7.6.1**. Cette version n'est pas compatible avec Novell Netware. **MySQL** : voir ci-dessus.
Sur plate-forme NETWARE	**ORACLE** **SQLBase** (Société Gupta, ex Centura Software) **version 7.5.1** minimum, associé à l'outil de développement Centura Team Developer ou SQL-Windows.
les services de fichiers	Ils sont de même type que ceux des bases de données. Pour toute application utilisant un SGBD, on cherchera donc à placer dans la base de données le maximum d'informations qui autrement seraient éparpillées dans des fichiers annexes. Les serveurs support sont le plus souvent de type « serveur local de ressources »
UNIX	C-ISAM : gestionnaire de fichiers séquentiels indexés
Sur plate-forme Windows NT/2000 Server ou Netware	MS ACCESS : version 2000 minimum préconisée. « Hyper File », moteur SGBD associé à l'outil de développement WinDev

BULL/GCOS7	• LINKED QUEUED : gestionnaire de fichiers partitionnés, intégré au système d'exploitation. • UFAS : gestionnaire de fichiers GCOS7, intégré au système d'exploitation.
les services d'extraction et d'injection	Ces services fournissent les mécanismes permettant d'extraire des données de fichiers ou de bases de données utilisées par les applications, selon certains critères, pour alimenter (injection) d'autres applications. Ils s'appuient sur des standards de formats de fichiers qui précisent la structure et le format des différents fichiers échangés par les applications. On choisira ceux fournis par l'éditeur du SGBD/R, ou liés à la nature de l'échange auquel il est destiné.
les services de tri	ces services s'appliquent sur tous les gestionnaires de données, ils sont accessibles depuis les applications Préconisation : on utilisera les outils livrés en standard avec les Systèmes d'exploitation.
les services de conversion de formats	Ces services comprennent les différents outils supportant la conversion de format des données. Pas de préconisation pour un outil général de conversion de données. Pour les formats bureautiques, les convertisseurs associés aux outils bureautiques sont recommandés pour basculer les documents dans un format pérenne comme XML. Pour les formats de document, la conversion en vue de l'impression peut être opérée à l'aide de l'outil ACROBAT (minimum version 5 recommandée). Suivre les recommandations de l'ADAE : Cadre Commun d'Interopérabilité (voir liens utiles § 1.5)

	Conditions d'application :
Produit	**commentaire**
SQL SERVER (SYBASE)	Base de données relationnelle limitée à l'application GIDE sur des serveurs sous LINUX.
IDSII	Ce SGBD non relationnel et propriétaire est lié aux applications développées sur plate-forme BULL/DPS7 sous le système d'exploitation GCOS7. Son utilisation restera limitée aux applications NCJ (casier judiciaire) et SIGMA/THEMIS (comptabilité budgétaire).
XBASE	XBASE est une norme définissant le format de fichiers de données structurées dans un environnement bureautique. Les fichiers XBASE sont normalement hébergés sur un serveur local de ressources. Ils peuvent avoir été créés par les programmes suivants : Microsoft Visual FoxPro, Visual dBASE, CA Visual Objects, Clipper et autres produits compatibles. Les utilisateurs d'applications s'appuyant sur des fichiers XBASE doivent être sur un même site (même serveur local de ressources).
Services de fichier	Dès lors qu'une Base de Données est utilisée par l'application, l'utilisation conjointe de fichiers classiques est à proscrire, ne serait-ce que pour les problèmes de journalisation.

3.2.5 Services de traitement

	Objectif
Ces services sont à mettre en œuvre pour exploiter des applications transactionnelles qui requièrent un bon niveau d'administration et de paramétrage permettant d'optimiser les performances	
	Produits préconisés :
champ d'application	**Commentaire**
Client sous Windows	Moniteur transactionnel TUXEDO (BEA System)
Client sous Navigateur HTML	Pour mettre en œuvre des applications intranet, les concepteurs d'applications internet/intranet s'appuient sur trois concepts : le web statique (cf. fiche 3.2.9 Services WEB Internet et Intranet), le web dynamique et le serveur d'application. En toile de fond de ces techniques on trouve la notion d'échange d'objets (page html, images,...) entre un serveur et un client léger de type navigateur (I.E. Microsoft et navigateur à base de Mozilla 1.6). Les échanges s'établissent suivant le protocole HTTP.
Web dynamique	Les pages dynamiques sont un « mélange » de langage HTML et de langage de script. Elles intègrent les aspects présentation, métier et accès aux bases de données. Ces pages, écrites en partie dans un langage de script, sont exécutées côté serveur par un moteur spécifique, en général une extension du serveur HTTP. Le résultat du traitement est une réponse conforme au protocole http (le plus souvent une page HTML renvoyée au poste client). La plupart des serveurs Web embarquant directement dans le serveur un interpréteur de script, il est désormais possible d'éviter la technique des scripts CGI (Common Gateway Interface) écrit dans un langage quelconque (C, Perl, shell) qui sont coûteux en charge système (lancement d'un interpréteur à chaque appel). Plusieurs éditeurs proposent des solutions pour générer des pages dynamiques : Microsoft avec les Active Server Page (.asp), dans le domaine libre ou open source Pretty Hypertext Processor (.php) et Perl (.pl), et Sun avec les Java Server Page (.jsp)[4]. Ces langages de script doivent pouvoir, grâce à des API, accéder aux principales bases de données (Oracle, MySQL, ...). Sous certaines conditions qui dépendent du langage utilisé ou du serveur HTTP, il est possible de gérer des transactions. Cette technique est bien adaptée pour des développements de petite envergure, et lorsque le développeur et l'intégrateur HTML sont la même personne. Les serveurs J2EE destinés à des applications n'utilisant pas d'EJB sont prioritairement : Tomcat (de la fondation Apache) et WebLogic Express (Bea). Les serveurs web dynamiques utilisables sont Apache (de la fondation Apache), Coldfusion (de Allaire-Macromedia) et IIS (Microsoft).

[4] La mise en oeuvre des jsp est particulière car elle s'appuie sur les servlets. En fait une page jsp est transformée en servlet et exécutée par le moteur de servlets

Serveur d'application Web	Le serveur d'application est la technique la plus élaborée pour concevoir des applications de type internet/intranet avec de nombreux utilisateurs simultanés (site e-commerce). Elle permet de dissocier la présentation, les composants « métiers » et les composants d'accès aux bases de données. Ce qui facilite le développement en équipe. Son architecture est centrée autour d'un serveur HTTP. Les techniques relatives à ces outils sont émergentes. Elles sont relativement lourdes, et doivent être réservées à des applications dont l'envergure ou la complexité justifie cet usage. Dans les autres cas, une solution à base de Web dynamique pourra être envisagée. Le ministère devant assurer la pérennité de telles applications, il doit considérer les possibilités de portage d'un serveur d'application à un autre. Ceci privilégie le choix de la norme recommandée par le CCI de l'ADAE. **J2EE** (Java 2 Entreprise Edition) est aujourd'hui une norme reconnue pour la construction d'applications en mode Web, pour laquelle une offre diversifiée existe. Des projets ministériels s'appuient sur cette norme. C'est pourquoi le ministère de la justice s'y réfère. J2EE couvre une dizaine de services techniques : accès à un annuaire, à une base de données, dialogues entre machines virtuelles Java, interfaçage entre composants, la finalité étant de rendre interopérables les composant développés dans le cadre des architectures distribués. Les **EJB** (Enterprise Java Beans) écrits en Java sont à la base de cette technologie. Les EJB sont notamment utilisés dans les domaines des transactions sécurisées. Le code de gestion des transactions est pris en charge par le système et donc le développeur peut se concentrer sur la création d'objets et de méthodes appropriées à une transaction particulière. Toutefois, chaque implémentation de produit J2EE répond d'une manière particulière aux questions que la norme ne traite pas ou pas encore. Pour limiter l'impact de solutions non normalisées, le ministère choisit une démarche méthodologique, fondée notamment sur les points suivants : • identification des classes non standard d'une implémentation (par ex. les EJB d'entités), de façon à limiter et tracer leur emploi dans l'attente d'une normalisation ; • conception de solutions pour la répartition de charge en amont du développement, pour éviter l'emploi de solutions non normalisées ; • identification et localisation de l'emploi de possibilités liées à la haute disponibilité des applications, ces possibilités étant non normalisées à l'heure actuelle ; • dissociation des objets et classes métiers (à la norme J2EE), et de ceux techniques pouvant faire appel à des spécificités du serveur d'application (parfois si ce n'est souvent à la marge des standards). Les produits préconisés sont les suivants : – les produits libres, notamment **JBoss** ou **JOnAS**, après consultation des analyses qu'en propose régulièrement la communauté du libre, – **WebLogic** de BEA.

Produit	**Conditions d'application : commentaire**
TDS	Ce moniteur transactionnel propriétaire est lié aux applications développées sur plate-forme BULL/DPS7 sous le système d'exploitation GCOS7. Son utilisation restera limitée aux applications NCP (nouvelle chaîne pénale), NCJ (casier judiciaire) et SIGMA/THEMIS (comptabilité budgétaire).

3.2.6 Services d'interface archivage

	Objectif
Permettre la conservation dans le temps (durée illimitée) pour des informations et documents à valeur probante ou à valeur historique, 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. Les données à pérenniser proviennent de systèmes de gestion de bases de données, soit d'une gestion électronique de documents, soit sont issues d'outils bureautiques.	
champ d'application	**Commentaire**
Les services d'archivage	Chaque applicatif devra comporter un module d'archivage dans lequel seront basculées, au-delà d'un délai déterminé (correspondant au délai d'utilisation courante pour les services producteurs), les données à pérenniser. Il s'ensuit que les données qui ne sont pas à pérenniser auront été effacées lors de ce basculement.
Format	
XML	Les données à pérenniser sont, avant leur basculement sur le module d'archivage, à convertir en utilisant le langage XML, préconisé par les services gouvernementaux en tant que format d'échange universel et par conséquent propre à une conservation pérenne. Les données ainsi pérennisées pourront faire l'objet de requêtes multicritères ou d'une interrogation plein texte. Elles resteront accessibles en ligne sur le serveur de données du service producteur durant une durée déterminée et feront l'objet d'un archivage (archives départementales, service d'archives du ministère de la justice) une fois que les données n'auront plus besoin d'être consultées par le service producteur. (Voir 3.3.6 Fiche « Archives »).
Au format natif	Les données à pérenniser sont basculées dans leur format natif dans le module d'archivage sur le serveur de la base de production et doivent pouvoir faire l'objet de requêtes sur la base de critères multicritères qui seront définis par accord entre le service producteur et l'administration des Archives. La conversion dans le format XML n'interviendra qu'au moment du transfert dans le service d'Archives.
les services d'extraction et d'injection	Ces services fournissent les mécanismes permettant d'extraire des données de fichiers ou de bases de données utilisées par les applications, selon certains critères, pour alimenter une base archive sur un serveur dédié ou non. On choisira ceux fournis par l'éditeur du SGBD/R, ou liés à la nature de l'échange auquel il est destiné.
	Conditions d'application :
Produit	**commentaire**
Conversion au format XML	Cette conversion au format XML suppose qu'une DTD ou un schéma aura été préalablement défini pour ces catégories de données et que les balises créées intégreront les métadonnées spécifiques aux applicatifs. Les fichiers de métadonnées doivent comporter les indications minimales en références au « Guide de conservation des informations et documents numériques » de l'ADAE (voir liens utiles § 1.5) Pour les métadonnées nécessaires à l'archivage des données issues de SGBD, on complètera les indications minimales par la documentation suivante concernant l'applicatif : couverture fonctionnelle, modèle des données, structure des tables, tables de références et nomenclatures datées.

3.2.7 Services de communications entre applications

	Objectifs :

Les services de cette classe sont des composants qui fournissent les services applicatifs (mécanismes) nécessaires à tous les types d'échanges entre les différentes applications informatiques (ou pseudo-applications intranet) hébergées sur les plates-formes serveurs de l'infrastructure du ministère, mais aussi avec celles des partenaires.

Cette classe de services regroupe les « services applicatifs communs » à plusieurs applications. Ces services (mécanismes) sont souvent masqués par les produits logiciels.

Un service applicatif de communication est un composant logiciel qui fait intervenir une ou plusieurs fonctions d'échange d'informations, transmises au travers des infrastructures locales ou distantes.

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

- le mode transfert de fichiers [5]
- le mode messagerie applicative [6]
- le mode transactionnel entre serveurs d'applications

Ces fonctions principales peuvent être complétées par des fonctions de traitement des données échangées, par exemple des services de conversion des formats de données ou processeur de transformation de type XSLT par exemple en environnement conforme aux standards de la famille XML.

En revanche, la définition du contenu (liste et codification des données) relève du domaine fonctionnel.

Le mode Transfert de fichiers

Qu'il soit :

- manuel sous forme d'échange de disquette ou de CD,
- conforme à un standard (FTP sous TCP/IP),
- issu d'une norme (FTAM de l'ISO),

le transfert de fichier est le mécanisme de communication le plus simple à mettre en œuvre seulement si sa réalisation s'appuie sur des environnements émetteurs et destinataires

- soit conformes par la disponibilité de protocoles et d'outils de transfert « standards »,
- soit, à défaut, homogènes par la disponibilité de part et d'autre d'outils conformes à un même protocole propriétaires.

Les conditions de sa mise en oeuvre 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.

Le mode Messagerie

Par définition la Messagerie électronique permet l'émission et la réception de messages entre utilisateurs ou 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. L'application réceptrice déposera sa réponse dans une boîte à lettre que l'émetteur initial pourra aller consulter à son initiative.

---

5 Ex : B1, Gibus, BAJ, CARPA, FND…

6 Ex : PACTI, ComCi/MsgCi, B2

Ce mode asynchrone est mis en œuvre dans le cadre de l'utilisation d'une messagerie inter-applications :

- entièrement automatisée (PACTI)
- avec contrôle humain (ComCICA)

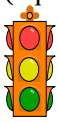
Le mode Transactionnel

Le mode transactionnel est caractérisé par la nécessité de synchroniser la communication entre deux applications. Une application serveur émet une requête de type transactionnel demande un service à destination d'un second serveur et se met en attente de la réponse de ce serveur.

Ce mode **synchrone** est requis lorsque l'applicatif est mis en oeuvre :

- sur un modèle serveur-serveur, à l'exclusion de la partie client des applications exécutées sur le poste de travail,
- à l'aide d'un moniteur transactionnel (propriétaire ou Systèmes ouverts)

	Produits préconisés :
champ d'application	**commentaire**
les services d'échanges synchrones entre applications	ces services permettent l'échange synchrone de données entre programmes et peuvent mettre en œuvre des outils de synchronisation de dialogue
Entre applications du même poste de travail	OLE (Objet Linking and Embedding) est le standard Microsoft qui gère l'échange entre applications des documents composites (texte, graphique, images fixes/encapsulés sous Windows).
Entre autres plates-formes	A l'intérieur de l'application, le middleware du SGBD est recommandé (SQL*Net pour ORACLE et Open Client pour Sybase). Des fonctionnalités associées au moniteur transactionnel TUXEDO permettent la mise en œuvre de tels échanges. Entre des applications différentes, l'utilisation du middleware du fournisseur de SGBD introduit un couplage très fort entre les deux applications. On préférera, lorsque c'est possible, mettre en oeuvre des solutions préservant mieux l'indépendance entre les applications (échanges de flux via un transfert de fichiers en mode batch ou via une messagerie applicative). Ce domaine semble être celui dévolu aux services et outils conformes à la famille de standards XML
les services de messagerie inter-applications	Ces services permettent l'échange asynchrone de données entre boîtes aux lettres d'applications • Composants de type ActiveX : fonction disponible dans les outils de développement pour accéder aux boîtes à lettres en utilisant les protocoles SMTP et POP3 • MAPI : interface unifiée de messagerie
les services de transfert de fichiers	Ces services permettent le transfert de fichiers entre plates-formes. Ils masquent l'hétérogénéité et la localisation des différentes plates-formes en utilisant les formats de fichiers conformes aux standards du cadre commun d'interopérabilité publié par l'ADAE (voir liens utiles § 1.5)

Produit	Conditions d'application : Commentaire
ODBC	L'interface ODBC permet de rendre l'application indépendante du SGBD/R utilisé. Cette indépendance, conforme au principe de non-adhérence, doit impérativement être recherché afin de rendre le système d'information robuste à d'éventuel changement d'outils d'infrastructure. La résolution d'éventuels problèmes de performance doit être traitée de préférence au travers de l'optimisation des traitements applicatifs, de la puissance informatique des serveurs ou de la répartition de charge entre serveurs, par exemple par le biais de serveurs d'application (cf. infra).
Echanges 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. Ces transferts électroniques s'appuient sur différents standards dont : • La norme internationale EDIFACT (ISO 9735) qui définit la structure et le contenu des documents échangés. • La norme internationale X400 qui définit les réseaux d'échange de Réseaux à Valeur Ajoutée. France Télécom (Transpac) l'a mis en oeuvre au travers de son offre de service public de messagerie ATLAS 400. TEDECO, un service d'EDI, initialement conçu pour les échanges entre le Ministère des Finances et l'ensemble de ces correspondants, TEDECO est un service de Transfert électronique de Données (EDI) dont l'architecture s'appuie sur le Réseau à Valeur Ajoutée ATLAS 400 de Transpac. Application de référence pour l'utilisation de TEDECO : demande de B2. **Cette technologie**, robuste et fiable, a peu été mise en œuvre sur nos applications et elle **n'est plus recommandée pour les nouveaux développements, qui doivent s'orienter vers des échanges de message ou des transferts de fichiers XML.**
Normes et protocoles	Pour chacune des classes de services de communication entre applications, des lignes directrices, des standards, des profils de standards, visent à organiser les échanges. Ainsi aux nécessaires protocoles de couches basses des réseaux (TCP/IP notamment), s'ajoutent : - des solutions techniques adaptées aux contraintes des EDI comme TEDECO, qui permet un contrôle de bout en bout et de la compression de données, - des normes sur le contenu, la syntaxe et les règles de définition et de structuration logique des données : les standards de la famille XML qui remplacent progressivement soit les formats propriétaires, soit les règles EDIFACT.
Interface de programmation avec les services de messagerie	CDO permet d'accéder aux BALs d'un serveur Exchange. L'API CDO encapsule la couche MAPI étendu permettant l'accès à une interface unifiée de messagerie (équivalent ODBC pour les bases de données)  Cette solution impose l'installation d'un client lourd OUTLOOK 2000 et est lourde de conséquences quant à l'accès distant et l'administration du serveur de messagerie et des clients. ***Elle n'est pas recommandée.*** Les études d'architecture devront privilégier la mise en place de service applicatifs, développé autour de fonctions utilisant les protocoles Internet permettant la réception de messages (POP3) et l'émission de message (SMTP).

3.2.8 Services de Messagerie

	Objectif
Les services de messagerie sont des services ouverts aux applications, et notamment pour le transfert de fichiers, mais aussi utilisés par la partie « humaine » du système d'information pour permettre à 2 personnes de communiquer entre elles ou bien à une personne de communiquer avec une application de type « front office ». Cette fiche décrit des mécanismes plus généraux, utilisables en particulier pour les échanges d'informations inter-directions ou avec l'extérieur du Ministère. Ces services englobent : ⇒ les services de messagerie ⇒ les services de synchronisation des annuaires, ⇒ la sécurisation des flux de message ⇒ les services de sauvegardes ad hoc ⇒ les outils de télé administration depuis le niveau de consolidation national	
	Produits préconisés :
Champs d'application	**commentaire**
Service national de messagerie électronique	La mise en place d'une messagerie aux standards Internet est à privilégier par rapport à la mise en oeuvre, plus lourde, d'une messagerie propriétaire d'entreprise intégrée dans un outil de travail collaboratif (groupware). Une des principales raisons, outre la sécurité globale du système de messagerie justice, est la contrainte d'interopérabilité avec les services interministériels AdER. Parmi les solutions techniques disponibles sur le marché, le ministère a fait le choix de **Microsoft Exchange**, à savoir : **Microsoft Exchange Server 5.5** ou **Microsoft Exchange 2000**.
Systèmes locaux de messagerie	Pour 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 : **Microsoft Exchange** (les messageries Lotus Notes et GroupWise sont proscrites).
	Conditions d'application :
Produit	**commentaire**
Normes et protocoles	Parmi les standards[7] Internet pour la messagerie, citons POP3, IMAP4, BINHEX et MIME, et également LDAP pour l'accès à l'annuaire : voir Fiche « Travail collaboratif » 3.3.3 et autres liens utiles vers l'ADAE La mise en place d'un service de messagerie doit être compatible avec le cadre d'interopérabilité mis en place au niveau interministériel, et notamment les profils de messagerie édictés dans le cadre AdER (réseau d'interconnexion inter-administratif). Sur cette base, le ministère de la justice a fait le choix de mettre en œuvre un service national de messagerie conforme aux standards Internet SMTP et E-SMTP, POP3, MIME et S/MIME.
Microsoft Exchange	Les prérequis de normes de mise en œuvre de serveur dans le cadre de la messagerie nationale et locale sont sur : http://intranet.justice.gouv.fr/rpvj , rubrique : Documentation par domaines - Installation/Maintenance des serveurs de messagerie. Si la messagerie est la première application mise en service sous Windows 2000, la mise en œuvre d'un contrôleur de domaine Active Directory est nécessaire.

[7] Utilisation des termes du référentiel du cadre commun d'interopérabilité de l'ADAE

3.2.9 Services WEB Internet et Intranet

	Objectif

Le service WEB remplit plusieurs fonctions couvertes par des briques logicielles plus ou moins indépendantes ; il assure :

- la fonction serveur de présentation : préparation de l'affichage pour des clients légers ou universels dans le cadre d'applications nationales ou de portée départementale,
- le traitement,
- la gestion du contenu.

Il permet :

- **Publication sur Internet**

Le SCICOM a envisagé la mise au point un guide méthodologique qui servira de cadre national de règles de publication sur le WEB (tant technique que sur le contenu).

- **les téléservices et téléprocédures sur Internet**

Les référentiels interministériels sont sur : www.internet.gouv.fr et ADAE (voir liens utiles § 1.5)

Il faut également prévoir qu'on puisse transférer, avec leurs métadonnées sur un serveur d'archivage, des documents publiés sur le Web. Voir le manuel de la direction des archives de France sur l'archivage électronique : http://www.archivesdefrance.culture.gouv.fr/fr/archivistique/index.html

	Produits préconisés :
champ d'application	**Commentaire**
Système d'exploitation/ de présentation HTTP	
Linux/Apache	**Le couple Linux/Apache est le système d'exploitation et le serveur http préconisé pour les serveurs de présentation http.** Linux est un système d'exploitation largement répandu sur plate-forme à base de microprocesseur Intel et compatibles et profite par ailleurs d'une constante augmentation de puissance et de popularité, notamment auprès des éditeurs. Apache est un serveur web développé par une dynamique communauté de développeurs qui apporte régulièrement des améliorations à son produit (**gratuit hors support**).
Windows 2000 Server/Apache	**Windows 2000 est un système d'exploitation déjà présenté dans le CTT pour les serveurs locaux de ressources.** **Windows 2000 peut être utilisé en conjonction avec le serveur http libre Apache.** Ce type de configuration peut être envisagé si les compétences techniques des exploitants permettent une mutualisation avec d'autres serveurs utilisés en serveur locaux de ressource sous ce système d'exploitation. *La version 2.0 ou supérieure d'Apache est préférable, pour des raisons de stabilité en exploitation.*
Windows 2000 Server/IIS	***Ce couple reste acceptable à titre transitoire. Il doit toutefois faire l'objet d'un plan de migration vers les deux couples ci-dessus.*** *En effet, si ce couple présente des qualités indéniables en termes de facilité d'accès et d'intégration, il constitue une cible privilégiée pour les attaques malveillantes et impose un effort d'administration important et très souvent largement sous-évalué.*

Traitements	Pour mettre en œuvre des applications intranet, les concepteurs d'applications Internet/intranet s'appuient sur trois concepts : le web statique, le web dynamique et le serveur d'application. En toile de fond de ces techniques, on trouve la notion d'échange d'objets (page html, images,...) entre un serveur et un client léger de type navigateur (IE-Microsoft, Mozilla 1.6 voire Netscape). Les échanges s'établissent suivant le protocole HTTP.
Web statique	En général pour des Web informationnels, Le langage rudimentaire, à bases de balises utilisées par le développeur, est le HTML. Il permet, éventuellement associé à des feuilles de styles (CSS), de mettre en forme du texte et des images. Ces pages (.html) et ces images sont stockées dans l'arborescence du serveur HTTP. Celui-ci, à la requête de l'utilisateur, va renvoyer cette page et les images associées et c'est le navigateur (Internet Explorer, Mozilla, Netscape) qui interprétera le langage HTML. La page décrite précédemment est ultra simple, elle ne permet à l'utilisateur que de « cliquer » sur des liens. Si l'on souhaite rendre plus attrayante une page, il faudra y associer un langage de script, en général du Javascript. Ce code « embarqué » dans la page sera exécuté sur le poste utilisateur. DHTML est une amélioration apportée par Netscape et Microsoft au HTML. Chacun ayant proposé une technique différente, les pages DHTML ne sont donc pas portables. Il est également possible d'introduire dans la page HTML, des formulaires, des listes déroulantes et des cases à cocher, un appel à une applet Java avec ses paramètres. Les accès à une base de données ne peuvent pas être inclus.
Web dynamique	Convient pour des développements de petite envergure. Voir fiche 3.2.5 Services de traitement pour plus de détail.
Serveur Web d'application	Technique la plus élaborée pour concevoir des applications avec de nombreux utilisateurs simultanés (site e-commerce) Voir fiche 3.2.5 Services de traitement pour plus de détail.
Outils de conception de site (Editeur de pages HTML)	**Microsoft FrontPage** s'adresse plutôt à des utilisateurs du type « créateur de contenu ». Il est à noter que l'utilisation des Extensions Frontpage, propriétaires, est à banir. **DreamWeaver** (Macromédia) s'adresse aux professionnels de la création. **UltraDev** permet le développement d'applications.
	Conditions d'application :
Produit	**Commentaire**
Mutualisation des serveurs Apache	La capacité de mutualisation d'un serveur de présentation fonctionnant en mode http est *a priori* considérable. Apache (comme IIS) permet de mettre en œuvre plusieurs (les limitations sont liées à la puissance de la machine serveur) serveurs web virtuels sur une même instance logicielle (plusieurs sites accessibles à partir d'une même instance Apache).
Choix entre Linux et Windows 2000	Même critères que pour les serveurs d'applications. Les compétences locales sur Windows 2000 sont plus courantes mais une attention particulière doit être portée à la sécurisation de l'ensemble. L'utilisation de Linux doit être préférée principalement pour les serveurs exploités dans les CPR ou là où la compétence est déjà présente.
Exploitation du serveur	Les sauvegardes sont sous la responsabilité des administrateurs. Les supports changés quotidiennement, doivent être impérativement stockés dans un coffre ignifuge ou externalisés.
Caractéristiques des serveurs	Fonction de l'application cible. La plupart des configurations types sont utilisables, à l'exception des CT5 et CT8, plus spécialisées (cf. infra). La capacité disque doit notamment être évaluée en regard de la cible applicative visée.

Publication sur Internet	Les services déconcentrés ont le choix entre deux modes d'hébergement (national sur justice.gouv.fr ou 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 2 serveurs supportent actuellement le dispositif : ➢ Serveur sous Linux Red Hat ; serveur HTTP : Apache et intègre la gestion de Perl, PHP4 ainsi que l'interface CGI ➢ Les fonctionnalités liées à l'indexation/recherche sont assurées par le moteur SEARCH intégré dans Microsoft Site Serveur. ➢ L'URL du site pourra être normalisée Site-Ville@justice[.gouv].fr en mettant en place des alias. • hébergement régional local : La plupart des fournisseurs d'accès proposent un service d'hébergement de pages WEB ou de serveur.

3.2.10 Services de présentation

Objectif
Le service de présentation est destiné à gérer l'affichage du système applicatif dans le cadre d'une architecture technique national ou départemental où le poste de travail de l'utilisateur final ne dispose que d'un client Citrix. La « citrixification » constitue une solution susceptible d'être mise en œuvre très tardivement dans la vie d'un projet informatique n'ayant justement pas fait le choix du mode web (application client-serveur classique), et ce même au bénéfice d'applications en fin de vie. Ce type d'architecture est notamment recommandé 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 en utilisant un client polyvalent (Citrix).

Produits préconisés :	
champ d'application	**commentaire**
Système d'exploitation du serveur	
Windows 2000 Server/Citrix Metaframe	**Le couple Windows 2000/Citrix Metaframe est préconisé dans le cadre de la migration d'une application client-serveur classique vers une architecture de type client léger** bien que les serveurs sous Unix supportent cette implantation. Toutefois, il doit être noté que la partie cliente de l'application client-serveur destinée à une « citrixification » doit impérativement être qualifiée en environnement Windows NT/2000 (cf. infra). Il faut aussi tenir compte de l'application (analyse de la bande passante, système d'impression), cela nécessite obligatoirement une étude poussée qui peut être effectuée en partenariat avec le centre de compétences (CPR d'Amiens).

Conditions d'application :	
Produit	**commentaire**
Mutualisation des serveurs Citrix	La mutualisation d'un serveur Citrix sur plusieurs applications est possible sous réserve que les parties clientes des applications en question présentent une compatibilité croisée en environnement NT/2000 (c'est-à-dire que les clients doivent simplement pouvoir fonctionner simultanément sur une machine NT) et que le dimensionnement mémoire du serveur soit calibré pour supporter l'ensemble. Par contre, la capacité de mutualisation au bénéfice de plusieurs services d'un serveur Citrix sur une application donnée de portée départementale dépend directement de la capacité de l'application cliente soit d'adresser plusieurs serveurs soit de pouvoir lancer plusieurs instances simultanément sur un même poste de travail.
Exploitation du serveur	Les sauvegardes sont sous la responsabilité des administrateurs. Les supports changés quotidiennement, doivent être impérativement stockés dans un coffre ignifuge ou externalisés.
Caractéristiques des serveurs Citrix	Les serveurs Citrix nécessitent une capacité mémoire importante. En effet, chaque utilisateur impose l'ouverture d'une session Windows sur le serveur. La configuration type 5 a été spécifiée avec cette typologie d'application en tête. La CT9 est également utilisable, notamment lorsque le nombre de clients simultanés potentiels est important. Dans tous les cas, la capacité mémoire doit faire l'objet d'une analyse préalable, pour laquelle la SDI dispose d'un centre de compétence interne (CPR d'Amiens).

3.3 Les Applications génériques

3.3.1 Fiche « Bureautique multimédia »

	Objectif :
Définir les outils bureautiques multimédia et les parties clientes des outils de partage de documents Les outils conformes aux standards Internet prendront une place de plus en plus importante dans le domaine de la bureautique communicante, domaine qui lui aussi s'étend au détriment de développements spécifiques, notamment pour les applications administratives d'édition et de circulation de formulaires.	
	Produits préconisés :
champ d'application	**commentaire**
Poste de travail	
Traitement de texte	**WordPerfect** (Corel) **Word** (Microsoft) } de préférence en version 32 bits Vérifier la compatibilité avec les versions des applications place sur le site : cf. tableau croisé des compatibilités : http://intranet.justice.gouv.fr/dage/sdi/sdi.old/SuiviOS.pdf **Writer (OpenOffice)** : ce logiciel libre convient dès lors que l'environnement applicatif n'impose pas des contraintes autres. Il peut être implanté sur le poste en parallèle des traitements de texte mentionnés ci-dessus. Il convient d'adopter un format de sauvegarde compatible (.rtf, .doc) pour les échanges.
Tableur	**Excel** (Microsoft) de préférence en version 32 bits **Calc (OpenOffice)** : ce logiciel libre convient dès lors que l'environnement applicatif n'impose pas des contraintes autres. Il peut être implanté sur le poste en parallèle d'Excel. Il convient d'adopter un format de sauvegarde compatible (.xls) pour les échanges.
Messagerie	**OutLook Express**, client de messagerie conforme aux standards Internet, fourni avec le navigateur Microsoft Internet Explorer ; simple d'utilisation et répondant aux besoins classiques de messagerie, compatible avec l'accès distant via un réseau IP. **OutLook** 2000 ou supérieur (Microsoft), peut être utilisé comme OutLook Express en client de messagerie conforme aux standards Internet ou en mode « Exchange Server » outre la messagerie, il permet alors la mise en œuvre d'outils de travail collaboratif (agenda, partage de ressources, dossiers, …).
Navigateur HTML	**Internet Explorer** de Microsoft: client universel permettant d'accéder à des serveurs INTERNET ou INTRANET. **Mozilla Firefox** est l'alternative logiciel libre à utiliser en complément d'Internet Explorer.
Anti-Virus	Viguard (Tegam)
	Conditions d'application :
Produit	**Commentaire**
Evolution vers le client universel	La présence sur chaque poste de travail d'un navigateur WEB et d'un client de messagerie au standard Internet permet d'accéder très simplement à partir de ces postes à une grande variété d'applications, sans que des démarches lourdes de déploiement et d'administration soient nécessaires. Il faut, pour cette raison, privilégier l'utilisation de ces composants du poste client.
OutLook	Les échanges entre ce client configuré en mode « Exchange Server » et le serveur de messagerie s'exécutent dans un protocole propriétaire ; sa mise en œuvre est donc réservée à un réseau local. Dans le cadre d'un accès distant, le recours à OutLook Web Access

	(fonctionnalité équivalente, mais via le protocole HTTP) sera nécessaire.
Format des messages	Le format « Texte brut » doit être privilégié, l'encodage MIME- UTF8. Voir http://www.adae.pm.gouv.fr/upload/documents/Profil_messagerie.rtf
Format d'échange pour les pièces jointes	Lors d'échange de textes, de tableaux ou de présentations, notamment par la messagerie interpersonnelle, par mesure de précaution, l'émetteur devra transmettre des documents aux formats **PDF** (Adobe) (pas de modification ultérieure de son contenu hors utilisation d'outils spécifiques, garantie de conservation de la mise en page initiale) ou **RTF** (Rich Text Format) pour récupération dans un traitement de texte. Sinon l'expéditeur devra s'assurer que le format du document transmis est compatible avec le produit bureautique du destinataire. Pour des raisons de sécurité, certains types de pièce jointe sont proscrits et filtrés sur les serveurs de messagerie en général : voir la liste dans le guide d'installation de l'anti-virus ScanMail, rubrique Documentation du site : http://intranet.justice.gouv.fr/ rpvj
Suite bureautique	Les logiciels bureautiques peuvent être installés sur un serveur local de ressources.
Suite OpenOffice	Suite bureautique (logiciel libre) présentant une opportunité technologique, et une alternative à l'utilisation des autres suites si l'environnement applicatif le supporte ou peut être implantée en parallèle. Toutefois, la compatibilité avec les fichiers Microsoft Office n'est pas totale.

3.3.2 Fiche « Gestion Documentaire » (GED)

	Objectif

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
- Fonction de recherche plein texte (« *full text* »)
- Fonction de gestion de thésaurus et de dictionnaire
- Fonction de recherche sémantique (distinguer « avocat » - le métier, d'« avocat » - le fruit par exemple)
- Fonction de sécurité : contrôle d'accès
- Fonction d'affichage : utilisation de bibliothèques de visualisateur (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 publication : possibilité de publier sous Acrobat pour envoi.
  - Enregistrement et suivi des demandes d'accès et des transmissions de documents
- Fonction de journalisation des accès avec tenue de statistiques
- Intégration de ces applicatifs dans un Intranet ou un Internet.

L'outil permet également d'intégrer dans la base documentaire de nouveaux documents, et doit pouvoir gérer la chaîne d'intégration : numérisation à partir d'un scanner, retouche d'image, reconnaissance de caractère (« *océrisation* »), [alternativement, intégration directe d'un document bureautique], indexation (basée sur des listes d'autorité, voire de thésaurus), voire un plan de classement.
Il doit aussi s'interfacer, si nécessaire, avec le système d'information du service (base de donnée existante, bureau d'ordre, …).

Les systèmes de GED offrent très fréquemment des fonctions de communication des documents, en interne (circuits de diffusion par exemple, ou en externe à l'organisation : transmission par messagerie ou fax...). La gestion de flux (Workflow) est un domaine distinct de la GED mais très complémentaire et de nombreux produits de GED sont interfacés avec des progiciels de workflow. Les fonctions de Workflow introduisent une dimension supplémentaire : la gestion des flux et des tâches associées. Ils automatisent le routage des documents et dossiers ainsi que certaines tâches n'exigeant pas d'intervention humaine.

La conservation a plus long terme de ces documents doit être pris en compte dès le début du projet : combien de temps doit-il être conserver ? quand doit-il être détruit ou basculer sur un serveur d'archivage dans un format pérenne ? ….

	Produits préconisés :
champ d'application	**commentaire**
Outil de gestion documentaire	La mise en oeuvre d'outils du monde GED peut s'effectuer dans trois contextes principaux : ➢ **GED** isolé à orientation de gestion de **documents « papiers » numérisés**. Dans ce cas, on utilisera de préférence **l'outil Alchemy (IRM)** sélectionné pour l'application NADEGE : GED pour le bureau de la nationalité de la DACS ➢ **GED** isolé à orientation de gestion de **documents issus du monde bureautique**. Dans ce cas, les **produits de la gamme Domino** de l'éditeur Lotus sont recommandés. Toutefois, l'attention du lecteur est attirée sur le fait que ***la composante « messagerie » de ces produits NE DOIT PAS être utilisée pour rester compatible avec notre environnement messagerie (cf. 3.2.8).*** ➢ **GED au sein d'un projet informatique métier,** il est recommandé d'utiliser • **les technologies d'origine ZyLab**, déjà présentes par exemple dans l'application IAO,

	• **le SGBD Oracle** qui offre en standard à partir de la version 9 des fonctions d'indexation et de recherche documentaire très complètes (**InterMediaText**). Ces fonctions sont intégrées dans le noyau. InterMediaText est accompagné d'un dictionnaire français. Le système de consultation de la jurisprudence de la Cour de cassation et des cours et tribunaux (JURINET), application intranet, met en oeuvre InterMediaText.

	Produits préconisés :
champ d'application	**commentaire**
Formats recommandés	Le cadre commun d'interopérabilité indique des choix préférentiels : site ADAE Cadre Commun d'Interopérabilité (voir liens utiles § 1.5) Les conditions d'utilisation des formats de document dans un contexte GED sont précisées dans le « Guide de conservation des informations et documents numériques » de l'ADAE (voir liens utiles § 1.5)
Formats d'affichage	• Formats recommandés : TXT (le plus utilisé), XML (faiblement utilisé) • Formats possibles (très utilisés) : HTML, RTF et PDF. L'outil ACROBAT (minimum version 5 recommandée) pour le format PDF, qui offre des possibilités de visualisation, d'impression ou d'échange.
Formats d'échange d'images fixes	• Format recommandé : PNG (faiblement utilisé) • Formats possibles : JPEG (très utilisé), TIFF et GIF (faiblement utilisé)
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, 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 oeuvre sous forme de client universel (en mode web).

3.3.3 Fiche « Travail collaboratif »

	Objectif :

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.

	Produits préconisés :
champ d'application	**commentaire**
Client sur le poste de travail	Outlook en mode client lourd. Internet Explorer en accès intranet via Outlook Web Access (accès client léger). *Le produit IBM - Notes et son serveur Domino - ne doit pas être utilisé comme outil de travail collaboratif, faute de pouvoir communiquer avec notre environnement de messagerie/annuaire.*
Serveur	Exchange 5.5 SP (Service Pack) 4 ou Exchange 2000 serveur SP2. Pour des raisons de sécurité, on n'utilisera Outlook Web Access qu'avec la version Exchange 2000.
Liste de diffusion ou discussion	SYMPA, logiciel libre, dont le cœur de l'outil s'articule autour de la brique élémentaire qu'est une liste de diffusion ou de discussion; tous les messages envoyés à travers la liste peuvent être mémorisés, archivés et rendus consultables via l'interface web SYMPA (mise en commun et de partage de fichiers).
	Conditions d'application :
Produit	**Commentaire**
Exchange Serveur	Le couple Windows NT4 et Exchange 5.5 correspond à un existant au ministère de la Justice et ne doit plus être déployé. Les nouvelles implantations doivent impérativement être installées **avec Windows 2000** serveur et **Exchange 2000 serveur**.  ***voir 3.1.9 Fiche « Serveur d'applications ou de données » sous Windows 2000*** Les pré-requis de normes de mise en œuvre de serveur dans le cadre de la messagerie nationale et locale sont sur : http://intranet.justice.gouv.fr/rpvj rubrique : Installation/Maintenance des serveurs de messagerie Administration de la messagerie
Outlook 98/2000/2003	Poste de travail sous Windows 98 ou Windows XP.
MSN Messenger 4.5.	Produit de messagerie instantanée, il présente un intérêt en tant qu'opportunité technologique, il peut être expérimenté sur le réseau interne justice.
Visioconférence	Les outils de vidéoconférence font partie des applications de travail en groupe. Néanmoins ils ne doivent pas être utilisés sur l'infrastructure de communication du Réseau Privé Virtuel Justice (RPVJ) compte tenu de son dimensionnement actuel qui ne peut supporter les débits nécessaires à ce type d'application. Toutefois, son utilisation reste possible sur des liaisons dédiées spécifiques. La retransmission doit s'effectuer conformément aux normes H320 (RNIS) ou H323 (IP). La commande de la caméra doit supporter la norme H281.Tout chiffrement doit faire l'objet d'un dossier spécifique auprès du HFD.

3.3.4 Fiche « Infocentre »

	Objectif :
Le système d'information décisionnel est un ensemble de données 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'avantage de l'infocentre est de masquer la complexité technique du système d'information (sources de données multiples, formats hétérogènes…) et de fonctionner indépendamment des applications de production. Pour ce faire, l'infocentre fournit une série d'**indicateurs** exprimés dans un vocabulaire **métier**. Ceux-ci se fondent sur les données d'une base propre à l'infocentre, alimentée périodiquement depuis le système de production. 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 préconisés :
champ d'application	**commentaire**
Extraction, Transformation, Chargement	
scripts SHELL scripts SQL procédures PL/SQL	Les processus périodiques d'alimentation sont implémentés par des scripts shell (système d'exploitation) et SQL (langage de base de données) qui extraient les données des bases de production (mise à plat), les transforment et les stockent dans les bases décisionnelles.
Import/export de base de données	A partir d'une base de données ORACLE, les mécanismes d'import/export peuvent être mis en œuvre si les extractions sont simples sans transformation de données.
Applications décisionnelles	
BUSINESS OBJECTS	Produit de la société de même nom, un des leaders mondiaux de l'aide à la décision (Business Intelligence). Le produit comprend plusieurs modules qui s'appuient sur un **référentiel** commun : infoview — connexion au référentiel et accès aux rapports prédéfinis reporter — accès aux univers et définition de requêtes personnalisées explorer — navigation dans un rapport selon des axes hiérarchisés designer — définition des univers (indicateurs, connexion base) supervisor — gestion de la sécurité et des droits d'accès broadcast agent — outil d'automatisation et de diffusion de documents application analytics — progiciels décisionnels (ex. gestion des compétences) Seuls les modules suivants ont été mis en œuvre au sein du Ministère : infoview, reporter, designer et supervisor.

Produit	Conditions d'application : Commentaire
Environnements techniques	
Serveur	Unix (LINUX, AIX) cf. 3.1.9 Fiche « Serveur d'applications ou de données »
SGBD	Oracle recommandé cf. 3.2.4 Services de gestion des données
Poste de travail	Windows (≥ 98) cf. 3.1.2 Fiche « Système d'exploitation des postes de travail » Type 1 ou 3 selon l'architecture (cf. 3.1.1 Fiche « Poste de travail »)
Architectures BO	L'outil Business Objects comporte deux modes : - Mode client serveur (C/S), utilisé en particulier pour définir les univers, les utilisateurs avec leurs droits d'accès et des requêtes complexes (client lourd), - Mode Webi, utilisé par les utilisateurs pour accéder à l'infocentre (exécution des requêtes prédéfinies ou création de requêtes simples) (client léger). En terme de fonctionnalité, le mode Webi est moins riche que le mode C/S. Néanmoins, il est possible de transformer un client léger (Webi) en un client lourd (C/S) en téléchargeant l'interface (zéro administration).
client-serveur	Poste de travail : client lourd + interface client du SGBD Serveur : serveur de données Cette configuration donne accès à toutes les fonctionnalités
Web Intelligence	Poste de travail : client très léger (navigateur web) Serveur : Serveur Web (Apache), serveur de données fonctionnalités limitées, déploiement facilité, ouverture possible à l'extranet
Web Intelligence / zéro administration	Poste de travail : client très léger (navigateur web) + auto installation du client lourd Serveur : Serveur Web (Apache), serveur de données Donne accès à toutes les fonctionnalités du client-serveur en architecture trois tiers (client, serveur d'application, serveur de données)

3.3.5 Fiche « *e*-formation »

	Objectif :

L'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.

L'e-formation 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. www.educnet.education.fr/dossier/eformation/eLearning1.htm)

Trois fonctions de base sont concernées :

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

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

	Produits préconisés :
champ d'application	**commentaire**
Hébergement technique	Il doit répondre aux impératifs du RPVJ en particulier sur la sécurité. Si le service n'est accessible que sur l'intranet, il peut être hébergé un serveur interne comme un autre service Web à travers ou non un portail. Si le service est accessible aussi sur l'internet et au public, il doit être hébergé à l'extérieur comme un web internet.
Plateforme technique	Elle doit être ouverte et accueillir des modules de formation répondant aux standards : - **SCORM** (issu de l'administration fédérale des Etats-Unis). - **AICC** (issu des professionnels de l'aviation civile) .
Cours	Le respect de ces standards SCORM ou AICC assure le portage sur la majorité des plates-formes d'e-formation du marché. .

3.3.6 Fiche « Archives »

	Objectif :

Cette mission d'archivage repose sur le ministère de la justice et le ministère de la culture en charge de la conservation des archives définitives (centre des archives nationales de Fontainebleau pour les documents produits par l'administration centrale et services d'archives départementaux pour les documents produits par les services déconcentrés de la justice) : le ministère de la justice doit transférer au-delà de délais déterminés par accord entre les services producteurs et l'administration des Archives (correspondants à la fin des délais d'utilité administrative pour les services producteurs), les données destinées à être conservées définitivement.

Les données destinées à être pérennisées, sont transférées à terme (voir service d'interface) dans les services d'archives concernés.

Une fois dans les services d'archives nationaux ou départementaux, ces données pourront être communiquées aux services producteurs demandeurs, ou serviront aux besoins de la recherche historique pour des utilisateurs extérieurs clients des services d'archives.

Une fois les délais d'utilité administrative expirés (durée au-delà desquels les données ne sont plus qu'exceptionnellement consultées par les services producteurs), les données (avec leurs métadonnées) au format XML sont gravées sur des supports d'archivage fiables : support actuellement recommandé par l'ADAE : le disque compact enregistrable (CD-R) ; support également accepté par la direction des archives de France : la cassette DLT.

Des procédures de vérification permettront de s'assurer de l'intégrité des données transférées.

Le déroulement des opérations et les données complémentaires indispensables figurent au

« Guide de conservation des informations et documents numériques » de l'ADAE :

(voir liens utiles § 1.5)

et dans le manuel de la direction des archives de France sur l'archivage électronique :

http://www.archivesdefrance.culture.gouv.fr/fr/archivistique/index.html

4. Architecture d'administration

4.1 Administration

4.1.1 Fiche « Services d'administration »

Les traitements et actions associées à ces services sont manuels ou outillés. Elles sont mises en œuvre par les exploitants et les administrateurs quel que soit le niveau d'hébergement des infrastructures. Le tableau ci-après décompose chacun des services de cette classe :

Gestion des installations et des changements	Gestion des opérations et des ressources	Comptabilité / Facturation	Gestion de la sécurité	Gestion des performances	Gestion des incidents
• Planification de l'installation • Installation et désinstallation • Configuration • Diffusion (télé-) • Activation et désactivation • Gestion de l'inventaire • Gestion du parc	• Gestion des données des ressources • Réorganisation • Sauvegarde/ restauration • Archivage • Gestion des ressources physiques • Planification et contrôle des travaux • Exploitation automatisée • Contrôle des ressources • Surveillance des états • Compression des fichiers	• Enregistrement comptable • Rapport comptable • Contrôle comptable • Facturation	• Contrôle de la sécurité • Mise en oeuvre de la sécurité • Surveillance de la sécurité • Rapport de sécurité	• Capacity planning • Analyse des performances et tuning • Rapport de performances • Surveillance des performances • Métrique des performances	• Diagnostics et isolation • Trace et alarmes • Prévention • Détection des erreurs • Reprise • Réparation • Suivi des appels

	Produits préconisés :
champ d'application	commentaire

	Produits préconisés :
champ d'application	**commentaire**
Gestion de parc	• **ACTIMA Winpark** constitue le cœur de la solution globale pour la gestion de parc informatique du ministère ; Composée de 6 bases régionales hébergées dans les CPR et d'une base nationale de consolidation, il permet de suivre les évolutions de l'ensemble des équipements informatiques. • **Check-up IV** a été conçu pour une mise en œuvre entièrement automatisée et un déploiement extrêmement rapide. L'inventaire est multi-sites, sans limitation du nombre de PC à inventorier et détecte automatiquement tout nouveau poste connecté au réseau. **Guide de mise en œuvre** : http://intranet.justice.gouv.fr/dage/sdi/sdi.old/guide.pdf
Télédiffusion	• Dans le cadre de la télédistribution des sites XTI, les fonctionnalités de l'outil LANDESK sont utilisées. • Pour la mise à jour des postes clients de l'application GIDE (sous Sybase), le produit libre RPM (distribué par Red Hat) est utilisé. Pour toute nouvelle application de télédiffusion ou mise à jour, on utilisera de préférence une de ces solutions.
Réorganisation	Plate-forme BULL / GCOS 7 : • DBREORG + kit de migration : outils natifs. • SYNDBAD : outil complémentaire de réorganisation des bases de données IDS II. Plate-forme UNIX : • Pour le système : pas de préconisations. • Pour les SGBDR : outils standards associés.
Sauvegarde / Restauration	Plate-forme BULL / GCOS 7 : • OPENSAVE avec solution STORAGETEK Plate-forme Intel UNIX : • Arcserve (Computer Associates) Plate-forme NT (hors serveur de messagerie): • Backup Exec (Véritas) Plate-forme Netware : • Arcserve (Computer Associates) Serveurs de messagerie Exchange (Microsoft) : • Ntbackup (Microsoft) fourni en standard avec Windows NT/2000
Compression des fichiers	Plate-forme PC : • WinZip : Le standard, en version française, pour compresser, décompresser, archiver et décoder les fichiers. Shareware pour Windows 95, Windows 98, Windows NT, Windows XP. . • PKZIP/PKUNZIP : l'un des utilitaires de compression et de décompression les plus connus de fichiers sur PC. Cet utilitaire s'intègre parfaitement dans l'environnement Windows.
Gestion de la sécurité	Plate-forme BULL / GCOS 7 : PROTECTION CATALOGUE : intégré aux logiciels système.
Gestion des incidents	• SAMS, application générique développée par la société AROBASE pour le compte du ministère, elle est utilisée vis à vis des applications civiles.
Surveillance - Gestion des performances	Plate-forme BULL / GCOS 7 : • SBR : outil natif BULL / GCOS 7. • SYSFLOW : représentation graphique de la charge machine. • SYSLOAD : analyse dynamique de charge en temps réel. Plate-forme serveur UNIX et Windows 2000 Server: • Outils standards du système + ISM. • SYSLOAD.

	Produits préconisés :
champ d'application	**commentaire**
Antivirus	Plate-forme PC (WIN 3.1 Win 95/98, Win 2000 et Windows XP) • Protection virale : Viguard (Tégam) • Décontamination virale : Norton (Symantec), Virus Scan (Macfee) Plate-forme serveur Windows NT/ 2000 : • Protection recommandée, mais pas de préconisation de produit aujourd'hui. Bien appliquer les patchs en référence et respecter les consignes d'installation. Plate-forme serveur UNIX : • Pas de préconisation particulière Bien appliquer les patchs en référence et respecter les consignes d'installation. Serveurs de messagerie Exchange (Microsoft) : • ScanMail (Trend Micro)

	Conditions d'application :
Produit	**Commentaire**
Antivirus	Pour des besoins locaux, la solution antivirus avec mise à jour peut être retenue, sous réserve du respect des dispositions suivantes: • l'antivirus individuel installé sur les postes de travail doit provenir d'un autre éditeur différent de ceux installés sur les serveurs nationaux ou régionaux ; • la mise à jour « automatique en ligne (live update) » des signatures de l'antivirus sur les postes de travail depuis l'Internet est interdite ; • le service ou l'entité doit mettre en œuvre les ressources techniques et humaines afin que les mises à jour soient effectuées dans les délais compatibles avec les enjeux.

4.1.2 Fiche « Services d'annuaires »

Objectifs
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 oeuvre 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...). Associé à cette double problématique, et dans un contexte d'incertitudes concernant la volonté de l'incontournable fournisseur d'annuaire messagerie (Microsoft, cf. infra), la stratégie suivie par le ministère s'articule autour d'une forte volonté de recourir à une double source, sur un modèle proche de celui concernant les systèmes d'exploitation pour serveur (cf. supra).

Produits préconisés :	
champ d'application	**commentaire**
Systèmes d'annuaire	
Active Directory	***Le choix stratégique d'utiliser les outils de la gamme Microsoft Exchange dans le cadre du service de messagerie électronique entraîne, dans un objectif clair d'homogénéisation et de limitation des risques opérationnels, l'utilisation d'Active Directory, uniquement en environnement Windows 2000.*** ***Pour pouvoir exploiter les applications dans de bonnes conditions de disponibilité et de sécurité, un domaine enfant doit comporter au moins 2 contrôleurs de domaine (DC). Le serveur régional de messagerie Windows 2000 Server / Microsoft Exchange 2000, lorsqu'il existe sur le site, est contrôleur du domaine enfant.***
Serveur ldap v3 à définir ultérieurement	Afin de couvrir des besoins liés à l'identification/authentification des utilisateurs, notamment dans le cadre des applications sensibles, nécessitant par exemple une sécurité forte, le ministère choisit de s'appuyer sur des produits strictement alignés sur l'environnement normatif, en l'occurrence ldap v3 (RFCs 2251 à 2255).

Conditions d'application :	
Produit	**Commentaire**
Choix entre AD et ldap v3	Active Directory (AD) doit être utilisé dans le contexte messagerie, imposé par le choix d'Exchange. AD peut être utilisé pour la sécurisation de l'accès à des applications client-serveurs dont le serveur fonctionne effectivement en environnement Windows 2000. ldap v3 est recommandé dans tous les autres cas. Il devient obligatoire pour les applications à base nationale unique ayant des besoins de gestion des utilisateurs autorisés et dont le développement est engagé postérieurement au 1er janvier 2002.
Contraintes techniques pesant sur les annuaires ldap v3	Ce ou ces serveurs doivent pouvoir fonctionner sur des serveurs conformes au présent CCT. Par ailleurs, ils doivent être en mesure de gérer des certificats conformes à la norme x509v3.

	Produits préconisés :
champ d'application	**commentaire**
Serveur supportant le service d'annuaire	En règle générale, il convient d'implanter le service d'annuaire sur un serveur dédié calibré en fonction du site, le secours pouvant se trouver sur un SLR ou SA existant. Dans le cas de la messagerie, l'AD doit impérativement être installé sur le serveur de messagerie et sur un serveur dédié de type SLR ou SA à calibrer en fonction du site.

4.1.3 Services de sécurité

Objectif

D’après 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.

NB : Toute mise en place d'un système d'information (système d'exploitation, application, communication) devra se conformer aux directives diffusées par le FSSI (Fonctionnaire de Sécurité des Systèmes d'Information).

Voir consignes de sécurités :
http://intranet.justice.gouv.fr/securite/accueil.htm

	conditions d'application :
Produit	**commentaire**
Habilitation	La gestion des habilitations devra être effectuée par les applicatifs en mettant en œuvre les paramétrages proposés par les applications et éléments des réseaux. La mise en place de profils d'accès différenciera l'utilisation des systèmes d'information accédés (utilisateur titulaire, utilisateur intérimaire, administrateur, ...)
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 : 1- **simple mot de passe** : il doit être au minimum composé de 8 caractères, accepter les lettres, les chiffres et les caractères spéciaux. L'élaboration d'un tel mot doit être la combinaison des trois : Ex : !t0-t014 Guide de la bonne utilisation du mot de passe : http://intranet.justice.gouv.fr/dage/sdi/sdi.old/securite.pdf 2- **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 3- **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**. Pour alléger sa gestion, on peut tolérer la mise en commun d'un tel mot au sein d'un même bureau ou service.
Confidentialité	Ce service peut être assuré par le seul fait d'empêcher le démarrage d'un poste ou la connexion à un réseau (ou application) si la fonction d'authentification est correctement activée. 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).
Non-répudiation	Ce service n'est assuré qu'au moyen d'outils cryptographiques permettant les signatures des émissions et des réceptions.
Infrastructure de gestion des clés publiques (IGC)	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 reste autorité de certification validée par l'IGC/A de la DCSSI. Pour toute information complémentaire, prendre contact avec le FSSI (Fonctionnaire de Sécurité des Systèmes d'Information) fssi@justice.gouv.fr

4.1.4 Services de télémaintenance

	Objectif
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.	

	conditions d'application :
Produit	**Commentaire**
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 coté 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. Il est obligatoire de définir le périmètre des opérations de télémaintenance laissées aux prestataires en précisant leurs obligations en terme d'engagement de service, de protection des données et de confidentialité. Les serveurs en télémaintenance doivent être 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	L'utilisation d'un portail sécurisé de type extranet, avec un accès restreint après authentification depuis internet, permettrait de respecter ces conditions tout en autorisant un partage clair du financement des moyens techniques nécessaires au prestataire. L'étude correspondante doit être conduite pendant la durée du présent schéma directeur.
Connexion directe RTC ou RNIS	Ces connexions doivent strictement respecter la directive numéro 3 sur la sécurité des systèmes d'information, ce qui interdit à l'équipement télé-maintenu d'être inter-connecté, directement ou indirectement, au RPVJ. Ce type de solution doit donc progressivement migrer vers l'utilisation du portail sécurisé.

4.2 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.

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.

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.

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.

Sauvegardes

Les sauvegardes seront conçues dans l'optique de privilégier une restauration rapide et fiable. On préférera par exemple les sauvegardes totales de bases fermées. Plus généralement, 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.
Les procédures de sauvegarde devront être modifiables afin de les aménager ou d'utiliser une solution transversale.

Impressions

Les impressions à la demande sont privilégiées.
La problèmatique des éditions dans le contexte d'application « client léger » et serveur distant doit être examiné avec grand soin pour préserver les performances et l'optimisation de la bande passante du réseau.

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, ...).

5. Architecture de développement

5.1 Règles de mise en oeuvre

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.

5.1.1 Règles générales de conception de l'architecture de l'application

Elaborer 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 oeuvre, 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).

5.1.2 Choix du type d'architecture physique

5.1.2.1 Rappels des enseignements des précédents schémas directeurs

Les difficultés rencontrées lors du développement des applications client-serveur sont généralement d'autant plus grandes que la partie des traitements qui est exécutée sur le poste de travail est importante.

Ceci est du principalement aux raisons suivantes :

- les outils de développement sur poste de travail ne sont pas bien adaptés au développement d'applications lourdes
- il est difficile de diffuser jusqu'aux postes de travail des applications volumineuses
- les équipes qui développent les applications sur le poste de travail sont généralement plus compétentes sur les aspects liés à l'interaction homme-machine que sur la structuration des traitements ou des données
- les développements visant des postes clients « lourds » débouchent parfois sur des applications encore plus gourmandes que prévues, qui ne fonctionnent sur aucun poste de travail du marché
- les évolutions applicatives imposent souvent d'augmenter les configurations des machines, ce qui génère des coûts importants lorsque ce sont les postes de travail qui doivent être changés ou augmentés.

Ces éléments conduisent à orienter les applications vers la mise en oeuvre de clients légers. 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.

Les traitements sont alors codés le plus possible sur le serveur sous forme Servlets (code java), de procédures stockées et de déclencheurs (« *triggers* »), et les outils de développement du poste de travail sont alors utilisés pour développer la couche de présentation.

5.1.2.2 Principes et règles

☛ **Toute application doit être conforme à un des 4 types d'architecture définis en *2.1.1 Types de répartition des données et des traitements*.**

☛ **On choisira généralement l'architecture de type « C/S Client léger »**

> **L'architecture de type « C/S Client léger » est l'architecture client-serveur de référence.** Elle doit être fortement privilégiée, notamment par rapport à l'architecture de type « C/S client lourd » qui présente le double inconvénient de ne pas pouvoir en l'état s'adosser au RPVJ, d'être plus complexe en terme d'administration et de diffusion, et d'obliger au maintien d'exploitation de serveurs locaux d'application.

☛ **L'architecture de type « local type monoposte » ou « C/S Client lourd » est envisagée uniquement en complément d'environnement déjà existant sur un site**:

On choisira l'architecture de type « local type monoposte » si

il n'y a aucun partage de données entre les utilisateurs : les données sont consultées et mises à jour uniquement par la personne qui en est responsable.

On choisira l'architecture de type « C/S Client lourd » si

- la visibilité sur les données reste locale au site où elles sont produites ;
- il existe déjà sur les sites d'exploitation, une application dans ce contexte.

Les architectures « locale de type monoposte » ou fichiers partagés et « C/S client lourd », pour lesquelles l'exploitation est nécessairement locale, doivent donc être écartées dans les cas suivants :

- si un problème sur les données est susceptible d'avoir une incidence sur d'autres applications ;

- si les données sont reconnues comme stratégiques ou confidentielles (par ex. des flux financiers) ;
- si l'application est destinée à un déploiement national ou si le nombre de sites concernés est important en s'adossant au RPVJ ;
- si le profil, la localisation ou la nature du métier des utilisateurs se prêtent mal à ce qu'ils exploitent l'application ;
- si des contraintes organisationnelles rendent difficile l'exploitation par les utilisateurs, par exemple si dans certains sites il n'y a qu'un ou deux utilisateurs de l'application, qui ne seront alors pas assez nombreux pour en organiser l'exploitation.

Rappelons que la meilleure application est vouée à l'échec si elle n'est pas exploitée dans de bonnes conditions.

S'il s'avère nécessaire de s'écarter des quatre architectures de référence, une attention particulière devra être apportée à la charge des éléments transverses (serveurs et réseau) ainsi qu'à l'ensemble des procédures techniques (reprises après incident, montée de niveau/redéploiement).

L'ensemble de ces éléments devra faire l'objet d'une documentation et d'un arbitrage formel SDI ou Comirce

☛Les architectures hybrides à éviter sont en particulier :

- Client/serveur distant avec données persistantes sur le poste de travail.

  Ces combinaisons correspondent à une architecture client/serveur qui aurait en plus des données persistantes sur le poste de travail. Si une architecture de type « C/S distant » est retenue, des données peuvent être descendues sur le poste de travail, mais elles ne doivent pas y persister au-delà d'une session de travail.

- De type C/S local avec un accès distant à des serveurs de réseau local.

- « C/S client lourd + serveur distant » avec mises à jour sur le serveur local.

  Une application ne doit pas effectuer des mises à jour à la fois sur le serveur local et sur un serveur distant. Les mises à jour imbriquées sont également à éviter.

5.2 Typologie des architectures cibles

5.2.1 Typologie des systèmes d'information

Le présent cadre de cohérence technique reconnaît trois types de systèmes d'information :

- Les systèmes d'information à base nationale unique,
- Les systèmes d'information à base départementale et à multiples occurrences,
- Les systèmes d'information destinés à des utilisations individuelles ou à de très petits groupes de travail sur un même site physique.

Par « base départementale à multiples occurrences », il faut comprendre une application déployée sur plusieurs services avec une base de données par service. L'occurrence est alors constituée par la base de données d'un service et les postes de travail associés à cette base. Le terme « départemental » lui-même est ici pris au sein informatique (dérivé de « département » au sens de service au sein d'une organisation plus importante, sans aucun lien avec la notion administrative éponyme).

5.2.2 Composition générique d'un système d'information

Un système d'information quelconque peut, dans pratiquement tous les cas, être décrit comme étant composé des éléments suivants (de forte inégale complexité) :

- un poste client,
- un réseau de communication,
- un serveur.

En pratique, le poste client est constitué d'un micro-ordinateur (parfois réduit à sa plus simple expression : le terminal Windows), une application cliente (parfois réduite à sa plus simple[8] expression, le client léger : navigateur Internet ou client Citrix) et des périphériques associés à l'application (lecteurs de carte à mémoire, douchette code barre, dispositifs d'impression, caméra numérique, périphériques de gravure...).

Le réseau de communication est typiquement constitué par un réseau local d'établissement coté site client, un réseau d'interconnexion grande distance (le RPVJ dans le contexte justice) et un réseau local de production coté site d'exploitation.

Le serveur peut lui-même être complexe. Il est décomposable en un certain nombre de services :

- un service de présentation, assurant l'interface avec le poste client,
- un service d'application, gérant la logique métier sous-jacente du système d'information,
- un service de données, assurant les opérations de gestion de la ou des bases de données de l'application,
- un service de sauvegarde, destiné à la sauvegarde de l'ensemble,
- un service de sécurité, destiné à vérifier les droits applicatifs et techniques des utilisateurs et administrateurs.

Bien sûr, ces différentes fonctions peuvent être très limitées. Par ailleurs, l'énumération ci-dessus utilise le terme « service »: rien n'interdit *a priori* de mutualiser plusieurs – voire tous – services sur une même machine physique (cf. toutefois infra pour quelques directives dans ces domaines).

5.2.3 Application à base nationale unique

Les applications à base nationale unique doivent respecter les préconisations suivantes :

- Utilisation d'une architecture n-tiers avec client léger,
- Le client léger doit impérativement être un navigateur standard. L'utilisation de JavaScript est autorisée. L'utilisation d'autres types de programmes additionnels téléchargeables (« *plugs ins* ») et/ou de langages de scripts est autorisée sous réserve que la compatibilité soit assurée avec au minimum deux navigateurs standards différents (IE et Mozilla). L'application doit permettre d'utiliser les navigateurs standards dans leur version courante deux ans avant la mise en service opérationnelle de l'application.
- Les communications entre client (léger) et serveur doivent intégralement respecter les standards du monde IP.
- En fonction de la criticité du système d'information, la partie serveur sera exploitée en centre de production informatique.
- Lorsque la sensibilité de l'application l'exige, elle utilisera les services de l'infrastructure de gestion de clés publiques mise en œuvre par le ministère. Sinon, l'application offrira au minimum un service – administré – d'identification/authentification par identifiant/mot de passe.
- La présence d'un module d'archivage et d'un module statistique doit avoir été impérative étudiée.

[8] L'utilisation de l'adjectif « simple » ne signifie en aucune manière que le code – programme – est simple à réaliser...

5.2.4 Application régionale ou locale à multiples occurrences

Les applications régionales ou locales à multiples occurrences doivent respecter les préconisations suivantes :

- ***Utilisation préférentielle d'un client léger.***

  Dans le cas où un client léger ne serait pas utilisé, la partie cliente de l'application doit :

  - être qualifiée en environnement Citrix afin de permettre, chaque fois que nécessaire, soit un déport de la partie serveur vers un centre de production, soit un déport de la partie cliente vers un site distant du site principal d'exploitation ;
  - présenter, au niveau du dossier d'exploitation, une analyse complète des besoins et contraintes réseau, précisant notamment la bande passante nécessaire par client et une analyse des performances (précisant notamment le nombre de postes clients susceptibles d'être mis en oeuvre sur site distant) en fonction des hypothèses standards de paramétrage réseau.

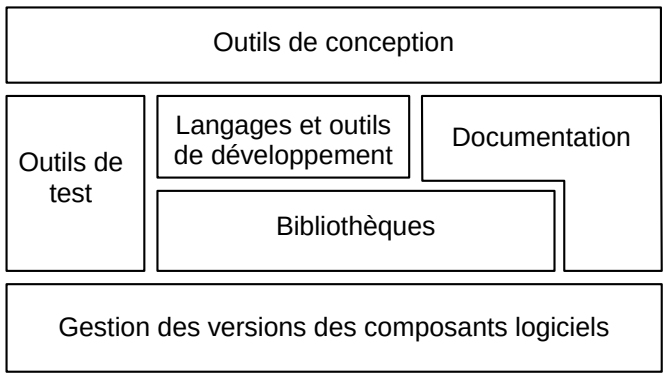
- ***Les communications entre client (léger) et serveur doivent intégralement respecter les standards du monde IP.***
- Lorsque la sensibilité de l'application l'exige, elle utilisera les services de l'infrastructure de gestion de clés publiques mise en œuvre par le ministère. Si l'exigence de sécurité est moins forte, l'application utilisera les mécanismes d'identification/authentification offerts par l'environnement du système d'exploitation. Si l'application ne présente pas de caractère sensible, elle offrira au minimum un service – administré – d'identification/authentification par identifiant/mot de passe.
- La présence de modules archivage ou statistiques doit être impérativement étudiée.

5.2.5 Applications destinées à un usage individuel ou collectif mono-site

Les applications destinées à un usage individuel ou à un usage collectif limité à de très petits groupes de travail sur un même site physique doivent néanmoins de préférence être réalisées en respectant les préconisations de la section précédente, sauf celles réalisées sur la base de la programmation d'outils bureautiques standards (voir fiches 3.3.1et 3.3.3). Toutefois, cette préconisation n'est pas absolue et peut être transgressée après avis de la sous-direction de l'informatique (ou de ses services régionaux) ou de la Comirce.

5.3 Services de développement

Cette classe regroupe les services supportant l'activité de développement d'applications de production ou d'infocentre.



Les services appartenant à cette classe sont :

- **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

5.3.1 Outils de conception d'application

Que ce soit pour assurer la reprise de données d'applications existantes ou la modélisation de nouvelles applications, en particulier dans le contexte client/serveur, les outils de conception et de modélisation doivent s'appuyer sur la méthode de conception et de réalisation de Système d'information MERISE étendu (MERISE/2, MERISE – OBJET-UML).

Ils respectent les trois niveaux de modélisation (conceptuelle, organisationnelle et physique) et fournissent des fonctionnalités de maquettage/prototypage et des interfaces permettant la génération automatique de scripts SQL.

Les préconisations sont les outils : AMC DESIGNER et Rational Rose

5.3.2 Logiciels de développement

	Objectif

Le contexte des applications a été exposé sur la 3.2.5 Services de traitement.

Pour les nouveaux développements, pour rester aussi proche que possible de la norme J2EE, le ministère adopte une stratégie préconisée par la plupart des organismes de veille technonlogique en matière de choix de serveur d'application :

- développer sur un produit libre, ces produits étant presque toujours les plus proches de la norme,
- au moment de la mise en production, comparer les résultats du produit libre avec ceux d'un produit d'éditeur.

Cette méthode permet de rester aussi proche que possible de la norme, et par ailleurs donne une certaine indépendance vis-à-vis de l'éditeur.

	Champ d'application
Produits préconisés :	**commentaire**
Outils pour application « client léger »	Le ministère veille à la conformité à la norme la norme J2EE des composants. Tout écart par rapport à cette norme doit être identifié.
Eclipse	Il s'agit d'une plate-forme d'environnement de développement comprenant des fonctions de bases et des interfaces graphiques en logiciel libre. Des éditeurs de plus en plus nombreux (dont IBM) proposent leurs produits sous forme de composant (« plug-in ») intégrable à cette plate-forme. Cette plate-forme est préconisée.
Borland Jbuilder	Préconisé, en raison de sa capacité à générer du code normalisé et à produire du code destiné à différents serveurs d'application. La version intégrable à Eclipse sera choisie de préférence.
Outils pour application « client lourd »	
Team Developer (TD) (anciennement Centura Team Developer	Editeur : société GUPTA (anciennement CENTURA CORPORATE SOFTWARE) retenu pour son bon niveau général, sa fiabilité et ses performances. En outre, il est bien intégré avec le moniteur transactionnel TUXEDO. **La version CTD 1.5.**1est compatible avec la **version 7.5.1 de SQLBase**. Elle permet uniquement la maintenance d'applications sur des environnements de serveurs **d'application Novell Netware**. **La version TD 2.1** est compatible avec un client **Windows XP Pro et la version 7.6.1 de SQLBase**. Les applications développées sous CTD 1.5.1 ou SQL-Windows peuvent être facilement portées sous cet environnement.
Windev	Editeur : Société PC SOFT Permet de développer des applications utilisant Hyperfile ou des bases de données relationnelles. Il est retenu pour son faible coût, sa richesse et sa simplicité de mise en œuvre.
Powerbuilder	Editeur : Société Sybase/Powersoft utilisé pour l'application GIDE en relation avec la base de données SYBASE Pour utilisation du serveur d'application Linux et de client sous Windows 2000, **la version 7** au minimum est retenue par le ministère.
Outils pour application mainframe (émulateur)	**Cités pour mémoire**, ils **ne doivent plus être utilisés** pour de nouveau développement
PACBASE	Editeur : Société IBM (CGI), outil en environnement GCOS7
CARIATIDES	Editeur : Société STERIA, outil en environnement GCOS7 et Unix