

Architecture commune d'applications informatiques

Cahier des clauses techniques ACAI

Clauses types pour les appels d'offres intégrant l'architecture ACAI

Annexe à la circulaire DPSM/SI n° 2005-25 du 30/03/2005
relative à la réalisation des applications informatiques

Version 1.5

Historique des versions du document

Versions	Dates	Commentaires
1.00	23 septembre 2002	Circulaire n°2002-58
1.50	mars 2005	actualisation et compléments

Affaire suivie par

Sous-direction des systèmes d'information
Bureau des techniques informatiques - DPSM/SI2

Tél. 01 40 81 74 40, fax 01 40 81 74 02
Mél. SI2.DPSM@equipement.gouv.fr

Documents annexes

Guide d'ergonomie des applications internet et intranet (version 1.5)

Guide de conception et réalisation des applications internet et intranet (version 1.5)

Guide de la persistance (version 1.5)

Guide de modélisation des applications (version 1.5) – non contractuel

Ces documents sont disponibles sur le site Internet du ministère (cf. infra).

Références intranet

<http://intra.dpsm.i2/si/si2/dossiers/developpement/acai>

<http://panda.cete-mediterranee.i2>

Références internet

<http://www.equipement.gouv.fr/informatique>

<http://www.adae.gouv.fr>

La loi pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées :

<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=SANX0300217L>

Sommaire

1. OBJET DU DOCUMENT.....	5
1.1. Définitions.....	5
1.2. Place du document dans un marché.....	5
1.3. Documents complémentaires.....	6
1.4. Priorité des règles.....	6
2. SPÉCIFICATIONS TECHNIQUES.....	6
2.1. Principes généraux.....	6
2.2. Postes clients.....	7
2.2.1. Normes de référence.....	8
2.2.2. Navigateurs cibles.....	9
2.2.3. Modules d'extension.....	9
2.2.4. Utilisation de témoins de connexion (cookies).....	9
2.3. Environnement serveur.....	9
2.3.1. Architecture applicative.....	9
2.3.2. Système et logiciels généraux.....	10
2.4. Contraintes d'exploitation et de sécurité.....	10
2.4.1. Paramétrage de l'application.....	10
2.4.2. Journalisation des événements et des erreurs.....	10
2.4.3. Traitements par lots.....	10
2.4.4. Supervision et aide au diagnostic.....	11
2.4.5. Information aux utilisateurs.....	11
2.5. Réseau.....	11
2.5.1. Débits.....	11
2.5.2. Protocoles.....	11
2.5.3. Accès aux serveurs.....	11
2.6. Échanges applicatifs.....	12
2.6.1. Échanges internes à une application.....	12
2.6.2. Échanges entre applications.....	12
2.7. Messagerie.....	13
2.8. Annuaire.....	13
2.9. Bureautique et format des fichiers.....	13
2.10. Cartographie.....	13
2.11. Authentification et droits applicatifs.....	14
2.12. Utilisation de certificats.....	14
3. RÉALISATION.....	15
3.1. Modélisation.....	15
3.2. Les schémas de données XML.....	15

3.3. Normes et règles.....	15
3.3.1. Règles de conception-réalisation.....	16
3.3.2. Règles pour l'utilisation de la persistance.....	16
3.3.3. Règles d'ergonomie et d'accessibilité.....	16
3.4. Développement des applications.....	16
3.4.1. Outil de développement.....	16
3.4.2. Utilisation de composants.....	17
3.4.3. Développement de composants serveur.....	17
3.4.4. Utilisation de composants génériques.....	18
4. CONDITIONS D'HÉBERGEMENT DES APPLICATIONS.....	18
5. PROCÉDURE DE VALIDATION DES APPLICATIONS.....	18
5.1. Points de validation.....	18
5.2. Fiche descriptive d'application.....	19
5.3. Réception d'une application.....	19
6. DÉROGATIONS.....	20
7. MODIFICATIONS DES SPÉCIFICATIONS.....	21
7.1. Évolutions du référentiel ACAI.....	21
7.2. Évolutions des conditions d'hébergement.....	21
7.2.1. Changements mineurs de version	21
7.2.2. Changements majeurs de version	21
8. LISTE DES PRICIPALES MODIFICATIONS DEPUIS LA VERSION 1 DU CCT.....	22

1. OBJET DU DOCUMENT

Ce document présente les clauses techniques générales applicables au ministère de l'Équipement, des Transports, de l'Aménagement du territoire, du Tourisme et de la Mer (METATTM) pour la conception et la réalisation d'applications informatiques de type Web. Il fixe les conditions à remplir pour que les applications puissent être hébergées dans les centres serveurs du ministère.

La circulaire du Premier ministre du 21 janvier 2002 précise l'utilisation d'un cadre commun d'interopérabilité des systèmes d'information publics et demande la certification des applications par rapport à ce cadre. Elle est complétée par la circulaire du 4 décembre 2002 relative à la mise en œuvre de la deuxième version du cadre commun d'interopérabilité des systèmes d'information publics

Les spécifications définies dans le cadre commun d'interopérabilité doivent donc être respectées. Elles sont publiées sur le site de l'Agence pour le Développement de l'Administration Électronique (Adaé).

1.1. Définitions

Certains termes pouvant présenter une ambiguïté sont définis de la manière suivante dans l'ensemble du présent document :

- Référentiel ACAI (architecture commune des applications informatiques) : Ce terme désigne l'ensemble des spécifications figurant dans le présent cahier des clauses techniques (CCT) et sur les compléments qu'il référence, ainsi que dans le cadre commun d'interopérabilité (CCI). Ces documents sont publiés respectivement sur le site internet du ministère <http://www.equipement.gouv.fr/informatique/> et sur celui de l'Adaé <http://www.adae.gouv.fr>.
- Marché : Ce terme désigne un contrat au sens de l'article 1^{er} du code des marchés publics, quelque soit son mode de passation, marché ou bon de commande.
- Maître d'œuvre d'application : Ce terme désigne le service responsable de la passation du marché au sens de l'organisation interne du ministère, agissant au nom et pour le compte du maître d'ouvrage.
- Titulaire : Ce terme désigne le candidat dans les étapes d'appel d'offres ou le titulaire du marché lorsque celui-ci est notifié.

1.2. Place du document dans un marché

Conformément à l'article 13 du code des marchés publics, le présent cahier des clauses techniques générales doit figurer dans la liste des pièces contractuelles régissant un marché après le cahier des clauses techniques particulières (CCTP) ou équivalent, les pièces particulières et les annexes éventuelles.

Conformément à l'article 56 du code des marchés publics et à l'article 2 du décret n° 2002-692 du 30 avril 2002 relatif à la dématérialisation des procédures de passation des marchés publics, et si mention en est faite dans l'avis d'appel public à la concurrence, le présent cahier

des clauses techniques et les documents qu'il référence peuvent être remplacés par leurs adresses sur internet définies à l'article 1.1.

Les cas de dérogations possibles aux clauses du présent document sont définis à l'article 5 « Dérogations ». Dans un marché, il est conseillé de récapituler les clauses dérogatoires dans un article nommé « Dérogations » placé à la fin du cahier des clauses administratives particulières (CCAP) ou équivalent.

1.3. Documents complémentaires

Sont annexés au présent cahier des clauses techniques quatre guides détaillant les règles techniques définissant le cadre de réalisation à respecter :

- Guide de modélisation des applications internet ou intranet
- Guide de conception – réalisation des applications internet ou intranet
- Guide d'ergonomie des applications internet ou intranet
- Guide de la persistance des applications internet ou intranet

Les projets réalisés pour le ministère doivent respecter les règles incontournables précisées comme telles dans les guides et tenir compte au maximum des règles ayant le statut « conseillé ».

Le guide de modélisation n'est pas contractuel. Il est proposé en tant qu'outil pédagogique.

1.4. Priorité des règles

En cas de contradiction dans les spécifications des documents régissant un marché, l'ordre de priorité est le suivant :

- les normes homologuées ou les normes applicables en France en vertu d'accords internationaux ;
- les spécifications figurant dans la liste des documents régissant le marché et placés avant le présent cahier des clauses techniques ;
- les spécifications du présent cahier des clauses techniques ;
- les conditions d'hébergement sur le centre-serveur telles qu'elles sont publiées sur le site Internet du ministère ;
- les règles incontournables mentionnées dans les guides référencés à l'article 1.3.;
- les spécifications du cadre commun d'interopérabilité.

2. SPÉCIFICATIONS TECHNIQUES

2.1. Principes généraux

Une architecture générale des applications informatiques a été élaborée sous le pilotage de la direction du personnel, des services et de la modernisation, sous-direction des systèmes d'information (DPSM/SI). Ce projet baptisé « architecture commune des applications informatiques (ACAI) » repose sur trois principes essentiels :

- Adoption d'une architecture logicielle de type Web, utilisant le client léger et respectant les normes et standards internet ;
- Hébergement des applications sur des plates-formes nationales centralisées ;
- Utilisation de l'environnement Java, et en particulier du standard J2EE.

Afin de garantir l'indépendance et la portabilité des développements par rapport aux plates-formes matérielles et logicielles, l'architecture technique de l'application doit appliquer ces principes généraux. La validation des applications sera réalisée dans les conditions définies au chapitre « Procédure de validation des applications ».

Dans tous les cas où ni le présent document, ni le cadre commun d'interopérabilité ne définissent de spécifications précises, le titulaire devra s'attacher à proposer des solutions conformes avec les normes et les protocoles standards du marché en veillant :

- à éviter autant que possible les choix propriétaires, par définition trop liés à un fournisseur et peu interopérables ;
- à privilégier les solutions faisant l'objet d'une activité de standardisation ;
- à privilégier les solutions basées sur des systèmes ouverts, modulaires et évolutifs ;
- à privilégier les composants libres jouissant d'une notoriété.

Les applications sont hébergées sur des plates-formes nationales mutualisées. Ceci implique que le titulaire doit respecter l'ensemble des contraintes techniques et des procédures, définies dans le présent document, les guides associés et dans ceux qu'il référence. Les éventuels aménagements ou outils complémentaires ne sont autorisés qu'après validation par le maître d'œuvre d'application et la DPSM/SI, dans les conditions définies ci-dessous au chapitre « Dérogations ».

2.2. Postes clients

Le client léger doit être utilisé. L'interface utilisateur est ainsi principalement constituée de code XHTML, de code Javascript et de feuilles de styles au standard CSS.

Les temps de réponse des applications sont conditionnés par de nombreux paramètres, en particulier la taille des pages.

De manière à les minimiser, les tailles de page suivantes devront être respectées :

- 15 Ko pour une page simple (ex : page d'accueil)
- 20 Ko pour un formulaire normal (exceptionnellement 30 Ko)

- 30 Ko pour une liste (exceptionnellement 50 Ko ou plus lorsque l'utilisateur choisit le nombre de lignes)
- 20 Ko pour un graphique généré (camembert, histogrammes,...)
- 100 à 150 Ko pour une image de cartographie (exceptionnellement 200 Ko ou plus sur demande spécifique de l'utilisateur)
- 200 Ko pour un fichier. Si le volume est supérieur, il faut prévenir l'utilisateur.
- 50 Ko au total pour les autres fichiers statiques mis en cache (feuilles de style, ECMAscript, imageries,...).

Les cas particuliers au delà de ces limites doivent être signalés par les maîtres d'œuvre d'application à DPSM/SI dans le cadre de la procédure de validation.

2.2.1. Normes de référence

Les normes utilisées sont :

- XHTML, version 1.0 ;
- Feuilles de styles en cascade CSS, version 1 et 2;
- Javascript selon la norme ECMA-Script, version 1.5.

L'utilisation de ces normes doit être validée par les outils officiels du W3C (World Wide Web Consortium) et sera limitée aux seuls éléments correctement supportés par les navigateurs cibles définis au 2.2.2.

Par ailleurs, les directives gouvernementales concernant l'accessibilité doivent être respectées.

L'utilisation de l'interpréteur XML sur les postes client n'est pas autorisée, vu l'état actuel de la diffusion des navigateurs prenant en charge cette technique et surtout de leur non conformité aux standards.

Dans certains cas très spécifiques, l'utilisation d'appliquettes (applet) Java légères, non communicantes, peut être autorisée, sous réserve de justification et de respect des conditions minimales suivantes :

- Aucune utilisation d'ActiveX client ;
- Aucun protocole autre que HTTP entre le client et le serveur Web ;
- Pas de client-serveur au travers du Web. Le client ne peut, en particulier, pas dialoguer au travers du protocole RMI avec un composant EJB disponible sur un centre serveur sur le réseau I-carré ou sur internet ;
- Les tunnels applicatifs ne sont pas autorisés, même sur les ports 80 et 8080 ;
- Aucune communication directe entre le client et les serveurs de données ;
- Enrichissement du client par des appliquestes Java. Dans ce cas, la JVM doit supporter le JDK 1.1 minimum ;
- La taille de ces appliquestes ne devra pas excéder 100 ko.

Pour ce type de client, les seuls cas permis sont ceux pour lesquels il a été démontré l'impossibilité technique d'utiliser uniquement un client léger. Cette approche ne doit pas être généralisée et doit être restreinte au strict minimum.

L'utilisation de telles interfaces est considéré comme une dérogation et fait obligatoirement l'objet d'une validation par DPSM/SI.

2.2.2. Navigateurs cibles

Dans tous les cas, la validité d'une application doit passer par un test réel sur les navigateurs suivants :

- Mozilla Firefox version 1.0 et supérieures;
- Internet Explorer version 5.5 et supérieures.

2.2.3. Modules d'extension

L'utilisation de modules d'extension (plug-in) doit faire l'objet d'une validation par le ministère. Elle doit se limiter aux outils considérés comme faisant partie des standards du Web. Leur utilisation doit être proposée en cohérence avec la cible des utilisateurs de l'application (interne, externe, nombre limité, etc.).

Seuls les modules d'extension suivants sont autorisés par défaut :

- afficheur de fichiers PDF ;
- afficheur de fichiers SVG.

2.2.4. Utilisation de témoins de connexion (cookies)

Conformément à l'article 2.4 de la circulaire du Premier ministre du 7 octobre 1999 relative aux sites internet des services et établissements publics de l'État, l'emploi de témoins de connexion (cookies) permanents doit, de manière générale, être évité. S'il est néanmoins décidé d'y recourir parce qu'il apparaît de nature à améliorer significativement le service rendu à l'utilisateur, ce ne peut être que sous deux conditions cumulatives :

- l'utilisateur doit en être préalablement averti ;
- il lui est proposé un mode alternatif d'accès au service.

2.3. Environnement serveur

Les spécifications générales définies ci-dessous constituent la référence pour la validation des applications. Leur respect permettra un portage rapide des applications d'un centre serveur à un autre en fonction de l'évolution des besoins de l'application ou des orientations sur les centres serveurs (répartition des fonctions, changement de cible, choix des logiciels de base, etc.).

2.3.1. Architecture applicative

Le standard J2EE a été retenu pour les développements pour garantir leur portabilité entre différentes plates-formes.

Les développements réalisés sont validés sur la plate-forme Tomcat pour les JSP et les servlets, et JBoss pour le fonctionnement des EJB.

L'utilisation des EJB n'est autorisée que quand ils sont nécessaires et doit faire l'objet d'un accord de DPSM/SI préalable au développement de l'application. Celle-ci doit toutefois être réalisée conformément aux spécifications de l'article 3.4.3 sur le développement de composants serveur pour pouvoir facilement produire des EJB en cas de nécessité.

2.3.2. Système et logiciels généraux

Le système d'exploitation est Linux ou Unix.

Le serveur Web est Apache.

La base de données par défaut est PostgreSQL. L'utilisation d'Oracle est possible sur dérogation de DPSM/SI.

Les serveurs cartographiques implémentent les normes de l'OGC (Open GIS Consortium) et la persistance des données géomatiques est assurée par PostgreSQL et son extension PostGIS.

2.4. Contraintes d'exploitation et de sécurité

Les applications utilisent des ressources mutualisées. Elles ne sont pas autorisées à modifier le paramétrage d'exploitation et de sécurité dans lequel elles s'exécutent. Tout besoin spécifique en la matière doit être soumis à DPSM/SI et au centre serveur.

L'accès aux fonctions du système d'exploitation est interdit.

Les règles de l'art en matière de sécurité doivent être respectées. En cas de doute sur la conformité d'une pratique avec le référentiel de sécurité du ministère, un avis peut être demandé à DPSM/SI.

2.4.1. Paramétrage de l'application

Tous les paramètres de configuration et d'exploitation d'une application, comme les chaînes de connexion à la base de données ou à d'autres applications, les liens externes ou les emplacements des fichiers journaux seront définis dans un fichier de configuration au format texte ou XML, commenté au niveau de chaque champ et spécifique à l'application. Ce fichier sera livré avec une notice descriptive détaillée à l'usage de l'équipe d'exploitation du centre serveur d'hébergement au format HTML ou texte.

Tout besoin de paramétrage spécifique du contexte d'exploitation (réseau, serveur Web, serveur d'application, serveur de données) doit faire l'objet d'une demande motivée auprès de DPSM/SI. En cas d'accord, les directives nécessaires seront documentées sur la notice d'exploitation et mentionnées sur la fiche descriptive de l'application prévue au chapitre 4.2. L'application sera conçue pour minimiser le nombre des opérations de paramétrage.

2.4.2. Journalisation des événements et des erreurs

Les sorties standard et d'erreur du serveur d'application sont strictement réservées au fonctionnement du serveur et ne doivent pas être utilisées par les applications.

La génération des traces et des journaux des événements et des erreurs sera réalisée par l'utilisation de l'outil *log4J*.

Les spécifications détaillées de mise en œuvre des traces figurant dans le Guide de conception et réalisation devront être respectées.

2.4.3. Traitements par lots

Les traitements par lots (batch) sont réalisés par l'exécution de modules lancés ponctuellement ou régulièrement par l'utilitaire *cron*. Ces modules doivent être écrits, par ordre de préférence, en langage perl, en java (application console) ou en sh. Ils doivent être fournis avec leurs fichiers source et documentés.

2.4.4. Supervision et aide au diagnostic

Un dispositif automatisé de supervision de l'infrastructure commune et des applications sera prochainement réalisé.

Afin d'obtenir les informations permettant de déterminer le niveau de disponibilité et de qualité du service rendu, les applications devront intégrer dans leur distribution un composant logiciel qui sera fourni par DPSM/SI.

2.4.5. Information aux utilisateurs

L'information des utilisateurs sur les projets d'application doit être assurée par la maîtrise d'ouvrage.

À cet effet, il lui appartient de mettre en œuvre un site web ou une page accessible librement sur l'Internet et/ou l'intranet en fonction de la cible pour diffuser aux utilisateurs des informations sur ses applications en cours de réalisation ou exploitées.

Le site d'information doit a minima publier les informations suivantes : les adresses d'accès à l'application, les contacts pour l'assistance, la documentation utilisateur et les règles de paramétrage de l'environnement technique si elles existent.

2.5. Réseau

2.5.1. Débits

L'application doit être validée pour une bande passante disponible de 16 kb/s par client. Un test complémentaire permettant de vérifier la robustesse de l'application est également réalisé avec une bande passante de 4 kb/s.

2.5.2. Protocoles

Les protocoles autorisés entre les clients et les serveurs sont HTTP version 1.1 ou HTTPS version 1. Le protocole HTTPS ne doit être utilisé que dans les cas où la liaison doit être sécurisée et uniquement pour les dialogues qui le nécessitent. Une liaison HTTPS ne peut pas être initialisée par défaut au début d'une session utilisateur pour n'être libérée qu'en fin de session.

2.5.3. Accès aux serveurs

Les accès des postes clients depuis l'intranet s'effectue au travers de serveurs mandataires (proxy) dont l'utilisation du cache est conforme au standard RFC 2616.

Une application ou un site Web pouvant être rendu simultanément accessible sur le réseau intranet, le réseau interministériel Ader ou le réseau Internet disposant chacun d'un plan d'adressage distinct, tous les liens entre les pages de l'application ou du site doivent être relatifs à la page racine de l'application ou calculés en fonction de la localisation de l'utilisateur. Cette contrainte s'applique également aux liens vers d'autres sites ou applications internes au ministère ou accessibles par le réseau interministériel.

Les flux échangés avec le réseau Internet, le réseau interministériel Ader sont protégés par le centre d'hébergement par des serveurs inverses (reverse proxy). En conséquence, les serveurs d'application et les serveurs Web ne doivent pas être considérés comme accessibles directement et ceux-ci sont en général distincts.

Une interface de programmation sera prochainement disponible pour indiquer l'origine d'une requête à l'application. Cette interface devra être utilisée pour renforcer la sécurité interne de l'application et notamment permettre la restriction d'usage des fonctions d'administration.

Les applications nécessitant la mise à jour de fichiers par des administrateurs ou des utilisateurs doivent intégrer cette fonction par une interface Web. Les pages HTML ne pourront être modifiées qu'à la condition d'être externes à l'application J2EE ; elles seront alors stockées sur un autre serveur ou une arborescence différente.

2.6. Échanges applicatifs

2.6.1. Échanges internes à une application

Au sein d'une application, les protocoles autorisés entre serveurs d'un même centre sont : RMI, JDBC, SQL-Net et JNDI.

L'accès à la base de données doit être réalisé par un pool de connexions qui sera fourni par le centre serveur, la référence à la source de données (datasource) étant obtenue par une requête JNDI.

Si des composants d'une même application sont ou sont susceptibles d'être hébergés dans des centres serveurs différents, les règles définies au paragraphe ci-dessous doivent être respectées.

2.6.2. Échanges entre applications

Suivant la rapidité de synchronisation souhaitée et le volume des données échangées, trois modes d'échange entre applications sont utilisables :

- Échanges immédiats (services web) : l'utilisation du standard Soap, basé sur le format XML et le protocole HTTP, est recommandée ;
- Échanges asynchrones de volume faible ou moyen : l'utilisation de la messagerie dans les conditions décrites au paragraphe ci-dessous est possible ;

- Échanges de volumes moyens ou forts : la mise à disposition de fichiers accessibles par téléchargement HTTP est recommandée. Le nom des fichiers ou des dossiers de stockage doit être aléatoire pour garantir un minimum de confidentialité, l'URL relative correspondante sera alors transmise par l'une des deux méthodes précédentes. L'utilisation de formats compressé sera la règle.

Les schémas de données XML, tels qu'ils sont présentés au chapitre correspondant ci-dessous, devront être utilisés chaque fois qu'ils auront été définis.

Pour les échanges de données cartographiques les protocoles spécifiés par l'OGC (Open GIS Consortium) doivent être utilisés (voir § 2.10).

2.7. Messagerie

Les règles d'usage de la messagerie Mélanie définies par la circulaire n° 2000-14 du 18 février 2000 ainsi que les règles de nommage doivent être respectées.

Une application doit envoyer ses messages en utilisant comme adresse d'émission (champ De) celle qui lui a été affectée (de la forme *Robot-Nom-application@equipement.gouv.fr*). Elle ne peut en aucun cas utiliser à la place l'adresse d'une autre boîte à lettres.

La taille maximum d'un message est limitée à 2 Mo. L'envoi régulier de messages volumineux à un même destinataire est interdit.

Les fonctions de messagerie au sein d'une application sont assurées au moyen de l'interface de programmation standard JavaMail.

Les applications doivent s'authentifier auprès du service de messagerie pour l'émission et la réception des courriels. Comme pour la connexion à la base de données, les informations de connexion au système de messagerie ne doivent pas être codées en dur dans l'application mais placées dans un fichier textuel éditable par le centre-serveur.

L'envoi en grand nombre de messages ou vers un grand nombre de destinataires est soumis à autorisation préalable par DPSM/SI.

2.8. Annuaire

Un annuaire d'entreprise « Amédée » est en cours de définition pour le ministère. Une interface de programmation sera mise à disposition des développeurs. Les spécifications correspondantes seront publiées sur le site internet du ministère.

2.9. Bureautique et format des fichiers

L'interfaçage des applications avec les outils bureautiques est réalisé de façon à garantir l'indépendance des développements vis à vis des outils bureautiques et de leur version, même pour un usage strictement interne au ministère. La liste des formats recommandés ou possibles qui doivent être utilisés figure en annexe du cadre commun d'interopérabilité. Les principaux formats sont les suivants :

- Fichiers textes TXT, HTML ou XML, pour un usage général ;
- Format XML OpenDocument 1.0 (extension ODF) normalisé par l'OASIS ;

- RTF est possible pour les fichiers qui doivent être repris par un traitement de texte ;
- Texte tabulé ou CSV, pour les fichiers qui doivent être repris par un tableur ;
- PDF est possible pour les documents en lecture seule. Dans le cas d'utilisation de ce format, il est nécessaire de se limiter aux fonctions d'affichage de base, car le module d'extension (plug-in) qui permet de l'afficher sur le navigateur des postes de travail comporte des niveaux de version ou peut nécessiter des ressources importantes.

2.10. Cartographie

Au sein d'une application, la mise en œuvre de fonctionnalités cartographiques est réalisée selon les principes de l'OGC (Open GIS Consortium) :

- La persistance des données est assurée par des serveurs de cartes WMS (Web Map Server) ou des serveurs d'objets géographiques WFS (Web Feature Server)
- L'accès à ces serveurs est assuré par les interfaces WMS (Web Map Service) ou WFS (Web Feature Service) sur le protocole HTTP.
- L'application en elle-même ajoute simplement à sa logique métier la gestion des images ou des flux GML rendus par ces interfaces.

Les serveurs OGC candidats doivent implémenter les spécifications OGC suivantes, selon les exigences fonctionnelles souhaitées : WMS, WFS, WFS-T, FEI, SLD.

La capacité transactionnelle des serveurs WFS est mise en œuvre grâce à des sources de données de type SGBD à extension spatiale, telles que PostgreSQL/PostGIS.

L'utilisation de formats vectoriels pour présenter une carte est limitée à des cas simples de cartographie statique ne nécessitant pas la mise en place de serveurs OGC. Pour être conforme au référentiel d'interopérabilité, seul le format SVG est admis dans ce cas.

2.11. Authentification et droits applicatifs

Le ministère dispose de deux systèmes de gestion de sécurité pour les applications :

- l'un pour les applications intranet, interministérielles ou extranet nommé Cerbère,
- l'autre pour les téléprocédures vers les entreprises, nommé Cactus.

Chacun des systèmes gère, à partir d'une base de comptes des utilisateurs, leur authentification et leurs droits applicatifs associés.

L'utilisation de ces composants est obligatoire. Ils permettent, au delà des aspects harmonisation et réutilisation de la distribution des droits sur les applications, de rendre transparent, pour les applications, le mécanisme d'authentification des utilisateurs (mot de passe, carte à puce, etc.) et d'en permettre l'évolution sans modification des applications.

Les spécifications des interfaces applicatives (API) de ces systèmes ainsi que des exemples sont fournis sur le site internet du ministère.

Une application nommée « Cerbère/Cactus bouchon » permet de simuler le fonctionnement de ces systèmes. Elle est fournie au titulaire lors de la passation du marché.

Les paramètres d'habilitations tels que les profils d'utilisateurs, les portées de droit et les restrictions complémentaires sont consignés dans la fiche de définition des règles d'habilitation Cerbère et doivent être validés par DPSM/SI.

2.12. Utilisation de certificats

L'utilisation de HTTPS est autorisée, le certificat étant fourni par le serveur.

Toute autre utilisation de certificats doit faire l'objet d'une validation par DPSM/SI qui reste seul habilité à en autoriser l'usage au ministère.

3. RÉALISATION

3.1. Modélisation

La modélisation UML (Unified Modelling Language) a été retenue au ministère, notamment dans le cadre de la méthode Khéfren de conduite de projets informatiques du ministère. UML doit donc être utilisé lors de la conception des applications Web. Le Guide de modélisation contient des recommandations d'usage d'UML.

Les livrables liés à la modélisation objet seront fournis dans un format compatible avec les outils suivants :

- Rose Modeler : modélisation graphique ;
- Rose Entreprise Edition (tous langages + Modeler) ou Rose J (Java uniquement) : génération et reverse de code ;
- SoDA : génération de documentation.

Si un outil est utilisé lors de la conception du modèle relationnel, il devra produire des documents compatibles avec AMC-Designor.

Les livrables doivent respecter les plans types définis dans le cadre de la méthode Khéfren (plans disponibles sur le site intranet du ministère).

3.2. Les schémas de données XML

Pour favoriser l'interopérabilité et la dématérialisation des échanges et faciliter la conservation des documents échangés, l'élaboration de schémas de données XML est fortement incitée et leur publication sur le site de l'Adaé recommandée. Cette démarche vise à encourager la réutilisation des schémas spécifiés par les partenaires publics ou privés de l'administration et d'améliorer l'interopérabilité globale de ses systèmes d'information.

Les schémas figurant ou référencés dans le cahier des charges du marché, sur le site du ministère ou sur celui de l'Adaé doivent être obligatoirement réutilisés.

Dans le cas contraire, le titulaire proposera soit l'utilisation de modèles standard s'il en existe, soit la définition de schémas, conformes au cadre commun d'interopérabilité, correspondant aux besoins à satisfaire et susceptibles d'être étendus et généralisés.

L'utilisation de schémas XML sera préféré à celle des DTD.

3.3. Normes et règles

Conformément à l'article 6 du code des marchés publics, les prestations qui font l'objet du marché sont définies par référence aux normes homologuées, ou à d'autres normes applicables en France en vertu d'accords internationaux, dans les conditions et avec les dérogations prévues par le décret n° 84-74 du 26 janvier 1984 fixant le statut de la normalisation.

Dans la mesure où elles ne sont pas en contradiction avec ces normes officielles, les règles incontournables citées dans le présent cahier des clauses techniques et dans les documents qu'il référence doivent être appliquées.

Les guides mentionnés dans ce chapitre sont disponibles sur le site internet du ministère.

Ces guides comportent trois niveaux de règles :

- Les règles incontournables qui doivent impérativement être respectées ;
- Les règles conseillées qui formalisent l'exercice de bonnes pratiques mais dont la prise en compte n'est pas impérative;
- Les règles suggérées qui relèvent du simple conseil de mise en œuvre de certaines techniques

Certaines règles conseillées ou suggérées peuvent être rendues obligatoires dans le cadre d'un projet. Elles sont alors stipulées en tant que tel dans le marché (annexe au CCTP par exemple).

3.3.1. Règles de conception-réalisation

Le Guide de conception-réalisation définit les normes et règles de développement des applications dans l'environnement technique retenu par le ministère.

3.3.2. Règles pour l'utilisation de la persistance

Le Guide de la persistance décrit les règles d'accès aux ressources persistantes de l'application (base de donnée, système de fichiers).

3.3.3. Règles d'ergonomie et d'accessibilité

Le ministère possède également des règles en matière d'ergonomie des applications Web contenues dans deux types de documents :

- Le Guide d'ergonomie pour les applications et les modèles de pages associés ;
- Les chartes graphiques internet et intranet du ministère.

Ces documents sont soit accessibles sur le site internet du ministère, soit consultables auprès du maître d'œuvre d'application.

3.4. Développement des applications

3.4.1. Outil de développement

L'outil utilisé pour les développements par les services du ministère est Eclipse, environnement de développement sous licence libre. Le titulaire peut toutefois utiliser l'outil de son choix.

Quel que soit l'outil de développement utilisé, la livraison de l'application finale doit être accompagnée des sources, fournis avec les fichiers de configuration permettant de recompiler l'application à l'aide l'utilitaire « Ant » . Ceci permet de vérifier que les sources livrés sont bien indépendants de l'environnement de développement, et que l'ensemble des classes java nécessaires sont bien présentes et également indépendantes de tout outil.

L'intégration de composants ou de bibliothèques externes préexistants, appartenant ou non au prestataire, ne peut être fait qu'avec l'accord de la personne publique. En cas d'intégration, les sources et la documentation associées sont remises au ministère qui doit disposer de la libre utilisation de celles-ci.

La documentation au sein des codes sources est réalisée au format Javadoc. Ce format de documentation vient en complément de tous les autres documents imposés par le marché ou dans le cadre de la méthode Khéfren.

3.4.2. Utilisation de composants

Le tableau suivant préconise un certain nombre de composants déjà identifiés. Il n'est pas exhaustif. L'utilisation de tout composant nouveau doit faire l'objet d'une déclaration préalable auprès de DPSM/SI.

Composants et Interfaces de programmation		
Obligatoires	Cerbère, Cactus Struts Log4J JAXP Jakarta Commons	Authentification - habilitations Framework MVC2 Journalisation Traitements XML Utilitaires techniques
Recommandés	Apache AXIS JFreeChart Xerces et Xalan	Services Web Génération de graphiques Implémentations JAXP
Suggérés	Hibernate, Castor JDO, OJB Castor XML iText FOP JasperReport Lucene, DocSearch Quartz JCS	Mapping objet-relationnel Mapping objet-XML Génération de PDF et RTF Processeur XSL-FO Génération de rapports Recherche plein texte Programmateur de tâches Gestion de cache applicatif

3.4.3. Développement de composants serveur

L'architecture J2EE propose différentes solutions d'architecture pour le développement d'application. Les développements devront respecter au minimum une structuration de type MVC 2 (modèle – vue – contrôleur), utilisant les Java Server Page (JSP), les servlets et les composants serveurs.

L'architecture J2EE propose une modélisation objet par les Entreprise JavaBean (EJB). Les EJB seront, à terme, les composants qui modéliseront la logique métier des applications. Le niveau de norme EJB à respecter est publié sur le site internet du ministère.

Sauf besoins spécifiques à justifier, il est demandé dans un premier temps d'utiliser de simples classes Java (Javabeen) pour développer les composants. Dans ce cas, il est obligatoire d'adopter une démarche permettant leur conversion future en EJB. Cette démarche se traduit par l'application de deux modèles de conception :

- Façade : Utilisation de classes permettant l'accès à la logique. Pour chacune de ces classes une interface Java est définie, c'est cette interface java qui est manipulée par le code client. Cette classe est un JavaBean ;

- Factory : Les classes façades doivent faire appel à une classe implémentant le modèle de conception Factory chargée de fournir des instances de classes. L'instanciation directe des classes façades est interdite dans le code des classes clientes.

3.4.4. Utilisation de composants génériques

Pour faciliter le développement des applications et en réduire les coûts, des composants génériques ont été et seront mis à disposition. Ils réduisent les risques d'incompatibilité avec les spécifications ACAI aussi bien maintenant que dans l'avenir, car leur interface de programmation sera plus stable.

L'utilisation est soit obligatoire comme pour le module d'authentification et de gestion des droits, soit recommandée.

Les composants génériques disponibles recommandés sont soit disponibles sur le site internet du ministère, soit fournis par le maître d'œuvre d'application lors de la passation du marché.

4. CONDITIONS D'HÉBERGEMENT DES APPLICATIONS

Les centres-serveurs du ministère hébergent les applications réalisées selon les spécifications et dans l'environnement technique défini par le présent cahier des clauses techniques (CCT).

La maîtrise d'ouvrage, si elle le souhaite, est autorisée à héberger son application à l'extérieur d'un centre-serveur du ministère. Cependant, cette possibilité ne l'exempte pas du respect des conditions de réalisation définies par le présent CCT et les guides annexés.

Des dérogations aux règles sont envisageables dans les conditions définies à l'article 6.

5. PROCÉDURE DE VALIDATION DES APPLICATIONS

5.1. Points de validation

Les applications étant installées sur des environnements mutualisés, elles doivent respecter l'ensemble des spécifications définies dans le présent document et celles du cadre commun d'interopérabilité, mais également les contraintes liées à la validation des solutions techniques proposées. Cette validation est réalisée dans une première phase sous la responsabilité du maître d'œuvre d'application, puis sous celle de DPSM/SI.

L'annexe 1 « Procédure de validation ACAI » de la circulaire DPSM/SI référencée en tête du présent document décrit les modalités de validation des applications informatiques du ministère.

Quatre points de validation donnent lieu aux autorisations correspondantes par DPSM/SI pendant la durée de conception et de réalisation d'une application :

1. l'autorisation du projet à la fin de l'étude d'opportunité ;
2. l'autorisation du développement avant le lancement de la réalisation ;
3. l'autorisation de mise en sites pilotes après la recette fonctionnelle et technique dite « usine » (cf 5.3) et la validation d'intégration sur le site d'hébergement et la qualification;
4. l'autorisation de mise en exploitation à la fin de la phase pilote et après les corrections éventuelles.

Le titulaire d'un marché s'engage à fournir toutes les informations qui lui seraient demandées dans le cadre d'une de ces validations.

5.2. Fiche descriptive d'application

Toute application fait l'objet d'une fiche descriptive dont le modèle est disponible sur le site internet du ministère et qui constitue la carte d'identité de l'application et décrit ses principales caractéristiques. Elle contient une description générale (nom de l'application, principales fonctionnalités, nombre d'utilisateurs, utilisateurs cibles, etc.), une description technique (outils utilisés, versions, etc.) et, le cas échéant, les demandes particulières (matériels, logiciels, versions des logiciels, etc.) liées à cette application. Ces dernières doivent impérativement être mentionnées sur la fiche descriptive pour garantir la prise en charge de l'application par le centre d'hébergement.

Avec son offre, le titulaire d'un marché doit fournir au maître d'œuvre d'application toutes les informations qui le concernent sur la fiche descriptive de l'application. Il doit notamment y faire figurer tous les éléments non conformes au présent document ou au cadre commun d'interopérabilité ainsi que ceux dont la déclaration est obligatoire.

Au cours de la vie du projet, le titulaire du marché peut demander à modifier des informations portées sur la fiche auprès du maître d'œuvre d'application pour validation par DPSM/SI. Les délais liés au traitement de demandes d'évolution de la fiche dont l'origine est le titulaire du marché lui-même ne sont pas imputables à l'administration.

Au moment du passage sur la plate-forme d'exploitation, toute différence entre les caractéristiques de l'application finale et celles contenues dans la fiche descriptive peut entraîner soit un ajournement de la réception des prestations réalisées par le titulaire et un retard de mise en exploitation correspondant au minimum au délai d'évaluation de l'impact de ces modifications sur la plate-forme d'exploitation, soit un rejet de l'application dans les cas de contraintes techniques trop importantes.

Le titulaire d'un marché pourra être tenu pour responsable des délais et des conséquences financières encourus par la fourniture d'informations erronées ou incomplètes ou par la non fourniture des informations demandées.

5.3. Réception d'une application

Chaque application livrée passe par trois phases de vérification distinctes :

- Une phase dite de « recette usine » qui sera entièrement réalisée sous la responsabilité du maître d'œuvre de recette d'application. La localisation de cette plate-forme doit être définie dans le CCAP ou le CCTP du marché. Cette phase a pour objet de valider l'ensemble des aspects fonctionnels et techniques de l'application, et de supprimer les anomalies.
- Une phase dite « d'intégration sur le site d'hébergement et de qualification ». Cette phase a pour objet de valider le fonctionnement et la stabilité de l'application dans l'environnement du centre serveur, et de vérifier la conformité de l'application par rapport aux spécifications du référentiel ACAI.
- Une phase dite « de site pilote ». Cette phase a pour objet d'évaluer les conditions de diffusion de l'application et de son usage par les utilisateurs.

La recette usine est obligatoire. Les tests d'intégration sur le site d'hébergement ne peuvent avoir lieu que sur une application ayant subi avec succès la recette dite usine.

Sauf stipulation particulière dans le marché, la réception sera prononcée à la fin des trois phases de vérification. Pour procéder aux vérifications et notifier sa décision, la personne publique dispose d'un délai de trois mois à compter de la date de livraison de l'application, de la documentation associée et de toutes les prestations prévues par le marché. Ce délai est identique en cas d'ajournement des prestations.

6. DÉROGATIONS

Les demandes de dérogation sont justifiées dans les cas où le référentiel ACAI et le cadre commun d'interopérabilité semblent ne pas proposer de solution adaptée aux besoins et où aucune alternative n'est disponible.

Des clauses dérogatoires aux spécifications ACAI et à celles du cadre commun d'interopérabilité peuvent être imposés dans le cahier des charges d'un projet. Il est conseillé de les récapituler dans un chapitre nommé « Dérogations » placé à la fin du cahier des clauses administratives particulières (CCAP) du marché.

Le titulaire pendant l'élaboration d'une offre ou le maître d'œuvre d'application pendant l'examen des offres peuvent demander à DPSM/SI une dérogation aux référentiels.

Pour réduire le risque de rejet de validation de l'application, cette facilité est également offerte pendant sa phase de réalisation. Le titulaire ne pourra néanmoins se prévaloir du délai d'instruction de la demande de dérogation ou de son refus pour exiger une modification de ses engagements dans le cadre du marché, tant en terme de résultats que de dates de livraison.

Une dérogation est par nature accordée à titre provisoire et est conditionnée à une mise en conformité dès que l'objet de la dérogation aura été intégré dans le référentiel ACAI ou qu'une alternative sera proposée.

En aucun cas, les dérogations ne pourront porter sur des normes homologuées ou des normes applicables en France en vertu d'accords internationaux.

7. MODIFICATIONS DES SPÉCIFICATIONS

7.1. Évolutions du référentiel ACAI

L'état de l'art et le contexte informatique du ministère évolue sans cesse. C'est pourquoi, il sera nécessaire de faire évoluer les spécifications ACAI figurant dans le présent document ainsi que dans le cadre commun d'interopérabilité.

Les projets d'évolution et les évolutions retenues seront annoncées respectivement sur le site internet du ministère et sur celui de l'Adaé.

Sauf cas de force majeure ou de contrainte de sécurité, un délai minimum de stabilité des spécifications sera garanti au titulaire. Ce délai sera de deux mois pour les évolutions qui auront été annoncées depuis au moins deux mois sur l'un des deux sites, et de quatre mois dans le cas contraire.

7.2. Évolutions des conditions d'hébergement

7.2.1. Changements mineurs de version

Sauf cas de force majeure ou de contrainte de sécurité, les changements mineurs de version des logiciels disponibles sur un centre serveur peuvent être effectués dans un délai de un mois après leur publication sur le site internet du ministère.

7.2.2. Changements majeurs de version

Sauf cas de force majeure ou de contrainte de sécurité, les changements majeurs de version des logiciels disponibles sur un centre serveur ainsi que les modifications de produits ou de marques pour des fonctions similaires peuvent être effectués dans un délai de deux mois pour les évolutions qui auront été annoncées depuis au moins deux mois sur le site internet du ministère, et de quatre mois dans le cas contraire.

– 0 – 0 – 0 –

8. LISTE DES PRICIPALES MODIFICATIONS DEPUIS LA VERSION 1 DU CCT

<i>Paragraphe</i>	<i>Description</i>
1.3	Documents complémentaires
2.2	Poste client
2.3	Mise à jour du choix de la base de données. Ajout des serveurs cartographiques
2.4.4	Ajout de la supervision
2.4.5	Information aux utilisateurs
2.5.3	API à venir pour la détermination de l'origine des connexions clientes
2.6.1	Reformulation de l'accès au pool de connexion
2.6.2	Échanges entre applications : ajout des normes de l'OGC
2.7	Messagerie : utilisation de Javamail
2.10	Prise en compte des choix en matière de cartographie
2.11	Authentification : intégration de CACTUS Identification de la fiche de description des droits
3.1	Référence au guide de modélisation
3.3	Normes et règles : reformulation
3.4.1	Libre choix de l'utilisation de l'environnement de développement
3.4.2	Ajout de la liste des composants identifiés dans ACAI
4	Conditions d'hébergement des application
5.2	Description de la fiche ACAI
5.3	Reformulation des phases de réception