DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 1/DEF/DGSIC portant sur les logiciels du ministère de la défense.

Du 17/10/2006.

NOR D E F M 0 6 5 2 8 9 7 X

Références :

Décret 2006-497du 02/05/2006 (JO n° 103 du 3 ; BOEM 160*).

Ordonnance 2005-1516 du 08/12/2005 (JO n° 286 du 9, texte n° 9 ; BOEM 120-0*).

Pièce jointe :

Une annexe.

Classement dans l'édition méthodique : BOEM nº 160*

Référence de publication : Texte inséré au BOC/PP 5, 2007, texte 8.

PREAMBULE

Ce document définit les orientations du ministère de le défense en matière de logiciels.Ces orientations concernent l'architecture logicielle des systèmes d'information et définissent des critères d'aide au choix en matière d'acquisition, de réalisation et de mise en oeuvre.Elles sont déclinées dans les documents de niveau schéma directeur(5), référentiels et cahier des charges techniques.

Ce document s'inscrit dans un cadre ministériel et interministériel notamment défini par :

— la stratégie ministérielle de réforme (SMR) qui prévoit, entre autres, la définition d'une politique sur les logiciels, comme un objectif à court terme ;

— la politique ministérielle des systèmes d'information et de communication (SIC) du ministère de la défense ;

— le décret 2006-497 du 02/05/2006 portant création de la direction générale des systèmes d'information et de communication (DGSIC) et fixant l'organisation des systèmes d'information et de communication du ministère de la défense ;

— le plan stratégique pour l'administration électronique qui comporte un volet sur l'emploi des logiciels par les administrations ;

— la politique de renforcement de la sécurité des systèmes d'information (PRSSI).

La présente directive concerne tous les composants(6), projets, programmes, opérations comprenant des logiciels, sous tous types de licences d'usage « propriétaires » ou « libres »(7), qu'ils soient :

— acquis sur étagère ;

— développés spécifiquement de façon interne ou externe au ministère.

Cette directive est complétée par des référentiels techniques et méthodologiques (cf annexe).

1. UNE DIRECTIVE SUR LES LOGICIELS POUR QUOI FAIRE?

La maîtrise de l'information est l'enjeu majeur de la politique ministérielle des SIC. Celle du système d'information et de communication du ministère de la défense en est un élément essentiel.

Celle-ci est rendue nécessaire par :

— l'exigence croissante des missions opérationnelles où l'utilisateur reste un acteur essentiel ;

— la mise en commun des réseaux d'infrastructure ;

— l'augmentation des menaces qui fait de la sécurité un élément prépondérant ;

— le besoin de réactivité au changement de l'environnement et de l'organisation ;

— l'accroissement à la fois des échanges interarmées, intraministériels, interministériels, européens et internationaux, mais aussi de l'interaction entre les SIC eux-mêmes ;

— le poids croissant de la complexité et de l'hétérogénéité du SIC du ministère de la défense ;

— l'évolution rapide de la technologie ;

— les contraintes de plus en plus importantes sur les ressources.

S'agissant des logiciels, cette maîtrise repose sur les principes suivants :

— favoriser l'interopérabilité par un recours aux standards, protocoles et formats d'échanges ouverts ;

— inscrire la sécurité comme un des critères majeurs de choix et de mise en oeuvre ;

(5) Schémas directeurs « métier » (SIOC, SIAG, IST) et « spécialisés » (formation, infrastructure et services, SSI, fréquences).

(6) Tout logiciel, y compris ceux qui sont embarqués dans les équipements d'infrastructure.

(7) Voir glossaire : logiciel libre/propriétaire.

— rechercher la plus grande indépendance technologique et commerciale possible ;

— pérenniser les données archivées ;

— préserver une diversité des choix technologiques offerts par le marché ;

— promouvoir le partage et la réutilisation des composants(8) ;

— maîtriser l'architecture du SI ;

— appréhender le coût global.

Enfin, dans le cadre d'une éventuelle démarche de « faire-faire », il convient de maintenir une réelle compétence interne de spécification, d'évaluation, d'intégration, et de développement.

2. LES ORIENTATIONS.

2.1. **Recourir aux standards ouverts.**

Les standards et formats ouverts, au sens de la loi pour la confiance dans l'économie numérique (LCEN), assurent un usage universel et non discriminatoire des logiciels. Ils favorisent leur interopérabilité. De plus, ils pérennisent les données et les architectures.

En conséquence :

— les standards et formats d'échange ouverts sont à privilégier pour la conception de nouveaux systèmes et lors d'évolutions majeures de systèmes existants ;

— un référentiel des standards et formats est élaboré et maintenu par la DGSIC. Il s'appuie sur les recommandations nationales du cadre commun d' interopérabilité des systèmes d'information publics(9) puis, sur le référentiel général d'interopérabilité et le référentiel général de sécurité(10). Ces documents s'inscrivent eux-mêmes dans une démarche européenne(11) et internationale.

2.2. **Atteindre et maintenir une hétérogénéité maîtrisée.**

Une homogénéité absolue est source de vulnérabilité et de dépendance. Elle est hors d'atteinte pour un parc matériel et logiciel aussi important que celui du ministère de la défense. A l'inverse, une hétérogénéité trop grande pose un problème de cohérence, de compatibilité et à terme de maîtrise du système d'information.

En conséquence :

— une hétérogénéité maîtrisée(12) doit être recherchée ;

— un référentiel de préconisations(13) de technologies logicielles explicitant l'apport et les limites de ces technologies est validé par la DGSIC sur proposition de la commission ministérielle des SIC (CMTSIC) par domaine technique ;

— les maîtrises d'ouvrage, dans le respect du code des marchés publics, doivent se conformer au référentiel pour l'élaboration des cahiers des charges techniques.

2.3. **Converger progressivement vers une architecture maîtrisée.**

Des choix d'architecture doivent être faits pour tenir compte des nouvelles technologies, des contraintes de mise en oeuvre et de l'hétérogénéité inévitable mais maîtrisée du parc.

Il faut privilégier(14) pour les nouveaux projets et les évolutions majeures qui constituent des opportunités de convergence :

— le poste de travail banalisé, le client léger / riche et la technologie du portail utilisateur qui facilitent l'accès aux applicatifs. Ils sont porteurs d'économies en matière de soutien et de potentialités dans le domaine de la mobilité ;

— les architectures orientées services, et notamment les services web, permettant la modularité et l'agilité rendues nécessaires par l'évolution permanente du système d'information. Les architectures orientées services permettront de passer d'une logique fondée sur les applications à une logique fondée sur les processus ;

— la modularité des composants logiciels qui favorise les évolutions et le maintien en condition de sécurité du système d'information. Cette approche modulaire s'accompagne d'une méthode autorisant une expression progressive du besoin et permettant une réalisation parallélisée des différents composants. Les composants logiciels seront stockés dans des bibliothèques et seront suffisamment génériques pour permettre leur réutilisation par d'autres applications et d'autres domaines. La certification de conformité des composants se fera sous la responsabilité de la DGSIC ;

(8) Voir glossaire : architecture logicielle.

(9) Circulaires du Premier Ministre des 21 janvier 2002 (JO du 5 février p. 2335) et 4 décembre 2002. (n.i. J.O.)

(10) Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

(11) Cadre général d'interopérabilité européen pour les services d'administration électronique V1.0.

(12) Hétérogénéité maîtrisée : recours à deux ou trois solutions maximum par catégorie de produit.

(13) Pouvant prendre la forme d'une répartition entre différents produits.

(14) Sauf à justifier que la solution préconisée n'est pas adaptée au besoin.

— les solutions multi-plates-formes, notamment celles indépendantes des systèmes d'exploitation ;

— les produits supportant le mécanisme de multilinguisme pour une utilisation dans un contexte international ;

— les produits intégrant l'accessibilité pour les personnes handicapées.

Pour l'ensemble du SIC du ministère de la défense, la continuité du service est une priorité, y compris durant les phases d'évolution majeure du système d'information.

Il n'est pas question de faire table rase de l'existant pour mettre en place un système cible. Ce dernier reste un objectif à long terme, hors d'atteinte dans l'immédiat, car les organisations et les méthodes de travail doivent s'adapter et accompagner le changement. Ce dernier point est de la responsabilité de la maîtrise d'ouvrage et des groupes utilisateurs.

Il s'agit donc d'une démarche par paliers privilégiant des phases courtes.

De plus, les réseaux et leurs capacités actuelles conditionnent les capacités d'évolution du système d'information (SI).

Enfin, la maîtrise de cette évolution suppose un suivi adapté des configurations(15).

2.4. **Avoir une démarche de confiance en matière d'acquisition et de développement.**

L'intégration, au sein d'un système d'information, de composants multiples interagissant, nécessite un haut niveau de confiance envers chacun d'eux notamment pour les composants de sécurité.

Cette confiance s'obtient de différentes manières, entre autres par :

— l'évaluation de sécurité d'un produit par un centre spécialisé qui est un préalable nécessaire à une qualification formelle ;

— la disponibilité du code source documenté avec le droit de le recompiler à des fins d'analyse qui est un facteur de confiance. Cette disponibilité peut être exigée, notamment pour les produits qui concourent à la sécurité ;

— la caractérisation des flux d'entrée/sortie aux frontières, tels les flux circulant entre un monde de confiance et l'extérieur ;

— l'application d'une directive « qualité des logiciels ».

(15) Voir glossaire : architecture logicielle.

De façon générale, en particulier pour les SIC opérationnels et de sécurité, la réalisation des logiciels doit s'appuyer sur un tissu industriel de confiance.

2.5. **Favoriser la concurrence et l'innovation face à une situation de monopole du marché.**

Dans un contexte de marché, le ministère de la défense doit s'appuyer sur la concurrence pour disposer du meilleur rapport qualité/prix. Cependant, le marché des logiciels présente une tendance à la constitution de monopoles.

C'est pourquoi, pour conserver une liberté de choix et de favoriser l'innovation, le ministère de la défense engage une démarche volontariste vis à vis des logiciels libres : il peut contribuer à des projets de logiciels libres lorsque c'est son intérêt (pérennité, indépendance,…). Cette démarche peut comporter une évaluation de sécurité visant éventuellement une attestation de la direction centrale de la SSI (DCSSI), voire un agrément.

2.6. **Privilégier les logiciels libres à coût global, risques et efficacité comparables.**

Outre les avantages liés à la disponibilité du code source, les logiciels libres permettent de vérifier le respect des standards et favorisent l'interopérabilité.

Le ministère de la défense doit s'efforcer, avant toute acquisition ou tout développement interne ou sous-traité, d'identifier des solutions alternatives en logiciels libres disponibles, de fonctionnalité équivalente ou voisine.

Il faut donc rechercher la libre disponibilité des logiciels acquis par le ministère de la défense :

— à coût global, risques(16) et efficacité opérationnelle comparables, le logiciel libre est privilégié ;

— l'utilisation de certains logiciels libres peut être imposée aux contractants ;

— le bien fondé de solutions comprenant tout ou partie de logiciels libres doit être systématiquement étudié ;

— en cas d'acquisition de logiciels « propriétaires », la solution d'une licence libératoire est systématiquement étudiée par le porteur du besoin.

Dans le cas de logiciels dont la divulgation du code source impacte la sécurité nationale, le recours à un produit logiciel sous une licence(17) obligeant à reverser le code à une communauté hors défense nationale est proscrit.

(16) Vulnérabilité, pérennité, spécificités techniques et juridiques, support.

(17) Ce n'est pas le cas des principales licences de logiciels libres.

2.7. **Mettre en place une analyse de la valeur systématique.**

Le choix d'une solution est fondé sur une analyse de décision, telle l'évaluation du coût global de possession :

— de façon systématique pour tout nouveau projet de système d'information, métier ou service commun, et toute modification majeure ;

— s'appuyant sur une analyse de la valeur fondée sur les critères définis par la présente directive.

Un guide est établi en la matière et entretenu sous responsabilité de la DGSIC.

2.8. **Mutualiser les composants logiciels et les modèles de données.**

Le ministère de la défense engage une démarche visant à rationaliser les composants de logiciels par le recours à la mutualisation et à réduire la redondance des données par le partage des modèles et des référentiels de données. Cela nécessite la définition et la mise en place d'une organisation, de méthodes et d'outils.

Cette capacité de ré-emploi concerne notamment les logiciels spécifiques fournis dans le cadre de marchés. Elle implique que le ministère de la défense dispose des droits suffisants(18). Cela suppose la définition d'un cadre juridique adapté.

2.9. **Mettre en place une politique de gestion de compétences.**

En tant que maître d'ouvrage de systèmes, le ministère de la défense doit posséder une expertise en matière de logiciels, reposant sur des compétences spécifiques, approfondies, mises à jour régulièrement et en nombre suffisant. Le pilotage de cette expertise suppose la mise en place d'une véritable gestion des compétences en matière de SIC et l'établissement d'un schéma directeur de la formation en informatique et communications électroniques.

Afin de garantir la disponibilité d'une réelle expertise, notamment sur les nouvelles techniques informatiques, la formation en interne sera complétée par un examen de certification des connaissances pour les experts volontaires.

Une cellule de veille technologique complétera le dispositif de partage des connaissances et fournira études, rapports et conseils sur des technologies susceptibles de figurer au référentiel technique en tant que préconisations de technologies logicielles.

Cette gestion des compétences s'inscrit dans le contexte plus général de la gestion de compétence des domaines SIC. Appliquée aux logiciels, elle doit comprendre :

— le recensement des pôles de compétence(19) existants, de leur patrimoine technique et l'identification des compétences à acquérir ;

— la mise en réseau des pôles de compétence ;

— l'animation(20) de ces réseaux ;

— la mise en relation des maîtrises d'ouvrage avec les pôles de compétence ;

— la prise en compte des compétences SIC dans la gestion prévisionnelle des emplois, des effectifs et des compétences (GPEEC) par les directions de personnels. Par exemple, dans le contexte actuel, un des métiers à développer est celui d'intégrateur d'applications ;

— l'adéquation des formations des personnels du ministère de la défense aux technologies actuelles et futures et leur coordination.

2.10. **Renforcer la compétence juridique dans le domaine des marchés des technologies de l'information et en matière de sécurité.**

La DGSIC exprime auprès de la direction des affaires juridiques (DAJ) les besoins actuels et à venir du ministère en matière de SIC.

En particulier, le domaine des logiciels évolue très rapidement et se complexifie sur le plan administratif et juridique. Des compétences adaptées sont nécessaires en matière de licences, de droits d'usage des logiciels et de gestion des risques.

3. MISE EN OEUVRE

Les autorités responsables déclinent cette directive dans les projets et programmes du ministère de la défense.

La direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense (DIRISI), en tant qu'opérateur défense, décline cette directive pour les aspects transverses du SIC défense. Elle est l'interlocutrice privilégiée des maîtrises d'ouvrage en matière d'infrastructure technique, de mise en oeuvre et de soutien, dès les phases des projets entrant en amont de son périmètre de responsabilité.

(18) A titre d'exemple, pour les logiciels spécifiques : droits d'usage sans limitation de durée du logiciel, droit de dupliquer ou de faire dupliquer, droit de modifier ou de faire modifier, droit d'intégrer ou de faire intégrer tout ou partie du logiciel dans le cadre d'autres projets, droit d'accéder en permanence à tous les éléments nécessaires à la génération du logiciel.

(19) Organismes et / ou personnes.

(20) Animation : veiller à ce que chaque réseau dispose d'un expert référent (modérateur) désigné et à l'absence de redondance dans les thèmes traités.

Les commissions « métier » (CSIOC, CSIAG et CIST) et les commissions ministérielles spécialisées veillent au respect de cette directive.

Les formes du contrôle d'application de cette directive tiennent compte :

— des contraintes de calendrier sur les projets et programmes ;

— du respect des règles de la mise en concurrence pour les projets en acquisition, à charge pour le cahier des clauses techniques particulières (CCTP) de tenir compte des orientations de cette directive ;

— des règles d'application du code des marchés publics.

Les dérogations font l'objet d'une saisine de la DGSIC par l'organisme d'appartenance de la maîtrise d'ouvrage concernée. Les cas structurants sont débattus en commission ministérielle technique des SIC. Les questions d'interopérabilité opérationnelle interalliée sont traitées de façon prioritaire.

Pour la ministre de la défense et par délégation :

Le directeur général des systèmes d'information et de communication,

Henri SERRES.

ANNEXE

GLOSSAIRE

Agrément (voir aussi évaluation de sécurité) : reconnaissance formelle qu'un produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies. [900/DISSI/DCSSI]

Architecture logicielle : l'architecture d'un système d'information (SI) se décline sous forme matérielle (équipements qui le supportent) mais aussi logicielle car un SI est composé de plusieurs applicatifs qui interagissent et nécessitent une compatibilité/interopérabilité parfaite pour garantir le service rendu par le SI. L'ensemble de ces applicatifs ou composants logiciels, constitue la configuration logicielle du SI et l'ajout, l'évolution, la suppression, le remplacement d'un composant doit faire l'objet d'un contrôle de compatibilité appelé « intégration ». La maîtrise du SI passe par la capacité à gérer la configuration logicielle et à intégrer les composants.

Architecture orientée services ou SOA / web service : cette approche repose sur la réorganisation des applications en ensembles fonctionnels appelés services. Un service n'est autre qu'une application, ou composant, exposée par le biais d'une interface XML standard (langages « SOAPSimple Object Access Protocol/WSDL-Web Services Oriented Architecture), connue sous le nom de Web Service. Les logiciels écrits dans divers langages de programmation et sur diverses platesformes peuvent employer des services Web pour échanger des données à travers des réseaux informatiques. Cette interopérabilité est due à l'utilisation de normes ouvertes regroupées au sein du terme générique de **SOA** (Service Oriented Architecture). Au sein d'un tel environnement, des services (dits « producteurs ») sont ainsi exposés à d'autres services (dits « consommateurs »).

Client léger / riche : l'interface « client léger » est limitée à l'utilisation du navigateur avec un paramétrage permettant l'accès au service web concerné. Le « client riche » permet d'avoir une interface client avec des fonctionnalités graphiques évoluées. Une partie des traitements est ainsi déportée sur la machine cliente. L'échange des données entre le « client riche » et le serveur se fait via XML. Le déploiement du « client riche » se fait via le Web. Cette architecture est un mélange des architectures web de type « client léger » et des architectures client-serveur de type « client lourd ».

Coût global ou de possession : ensemble des coûts liés à l'acquisition, l'entretien, l'emploi et l'élimination d'un système (exemple : achat, développement, déploiement, intégration, mise en oeuvre, exploitation, migration, accompagnement, maintenance,...).

Evaluation de sécurité/agrément : la DCSSI a élaboré et entretient un catalogue des produits de sécurité « d'usage général » ayant fait l'objet d'une évaluation de sécurité débouchant sur une attestation de sécurité.

Plusieurs types d'attestations de sécurité peuvent être délivrés par la DCSSI :

— certificat en vertu du décret n^{o}2002-535 du 18 avril 2002 (JO du 19, p. 6944) (critères communs) ;

— qualification (au niveau standard, renforcé ou élevé) ;

— agrément ou caution (jugeant de l'aptitude à assurer la protection d'informations classifiées de défense ou d'informations sensibles non classifiées de défense).

Intégrateur d'applications/architecte/urbaniste : au sens du club informatique des grandes entreprises françaises (CIGREF), sous la responsabilité du chef de projet maîtrise d'oeuvre, l'intégrateur d'applications participe au choix des différents composants logiciels (progiciels, bases de données, développements spécifiques…) et en assure l'assemblage dans le respect du plan d'urbanisme des systèmes d'information de l'entreprise et de l'architecture retenue pour le projet.En ce qui concerne les développements spécifiques, les travaux sont effectués soit en interne par le développeur, soit en externe avec l'aide d'une société de services.

L'architecte définit l'architecture du système d'information. Il garantit la cohérence de l'ensemble des moyens informatiques (matériels, applicatifs, bases de données, réseaux, middleware, système d'exploitation) et de leur évolution, en exploitant au mieux les possibilités de l'art, dans le cadre du plan d'urbanisme de l'entreprise. De ce fait, l'architecte technique est en relation étroite avec l'urbaniste du système d'information, qui en garantit l'évo-

lution cohérente dans le respect des objectifs de l'entreprise, du domaine fonctionnel…et des contraintes externes et internes (de risques, de coûts, de délais…).

Interopérabilité : l'interopérabilité des SIC traduit la capacité à échanger des informations et à créer les conditions d'un véritable travail en commun dans le respect des règles de sécurité appropriées.Ceci implique que des informations ou des services puissent être échangés directement et de façon satisfaisante entre les SIC eux-mêmes ou leurs utilisateurs (Politique des SIC du ministère de la défense). On identifie généralement trois niveaux d'interopérabilité : technique, sémantique et organisationnelle.

LCEN : loi 2004-575 du 21/06/2004 (JO du 22, p.11168) pour la confiance en l'économie numérique.

Licence libératoire : un logiciel est un produit spécifique, conçu pour un usage donné et développé généralement par un éditeur ou une société de service ; on n'achète pas un progiciel, on en acquiert un droit d'usage. Le propriétaire d'une licence acquiert le droit d'utiliser le progiciel conformément aux conditions stipulées par le titulaire des droits d'auteur et aux dispositions prévues par la loi. Les logiciels en « OpenSource » sont également protégés par un droit d'auteur et il convient de lire précisément la licence qui les accompagne.

Les entreprises utilisatrices et les éditeurs interprètent parfois différemment la notion de droit d'usage des logiciels. Ce constat, dressé par Gartner, incite le cabinet à conseiller aux utilisateurs de définir clairement dans leurs contrats cette notion, en indiquant, dans l'hypothèse d'un audit, comment sera mesuré l'usage des logiciels. Cet aspect se révèle d'autant plus important que les modèles de licences sont de plus en plus compliqués. Dans ce contexte, une licence libératoire vise à acquérir un droit d'usage libre de toute nouvelle dette ou obligation sur un périmètre donné, par exemple l'ensemble du ministère de la défense, voire l'administration.

Logiciel : ensemble des programmes, des procédures et de la documentation, et des données éventuellement associées (ISO CEI 12207), relatif au fonctionnement d'un ensemble de traitement de l'information.

Logiciel libre/propriétaire : l'expression «Logiciel libre» fait référence à la liberté et non pas au prix ; liberté pour les utilisateurs d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel. Plus précisément, elle fait référence à quatre types de liberté pour l'utilisateur du logiciel :

— La liberté d'exécuter le programme, pour tous les usages (liberté 0) ;

— La liberté d'étudier le fonctionnement du programme, et de l'adapter à ses besoins (liberté 1) ;

Pour ceci l'accès au code source est une condition requise ;

— La liberté de redistribuer des copies, donc d'aider son voisin, (liberté 2) ;

— La liberté d'améliorer le programme et de publier ses améliorations, pour en faire profiter toute la communauté (liberté 3). Pour ceci l'accès au code source est une condition requise.

Un programme est un logiciel libre si les utilisateurs ont toutes ces libertés (définition Free Software Foundation). Par opposition, un logiciel est propriétaire si une de ces libertés n'est pas garantie ; son utilisation est généralement encadrée par un contrat de licence. Il est à noter que les logiciels freeware et shareware, dont on ne dispose généralement pas du code, sont propriétaires.

Maître d'ouvrage (MOA) : personne physique, ou le plus souvent morale, qui exprime le besoin, fixe les objectifs, l'enveloppe budgétaire et les délais souhaités pour le projet (dictionnaire du management de projets AFNOR).

Maître d'oeuvre (MOE) : personne physique ou le plus souvent morale, qui réalise le projet à partir des besoins, des objectifs, des délais et des coûts fixés par le maître d'ouvrage. Il est responsable des méthodes, techniques et personnes qu'il mobilise pour réaliser le projet (dictionnaire du management de projets AFNOR).

Mobilité : en pleine expansion, la mobilité doit permettre à un utilisateur, doté de plus en plus souvent d'équipements portables, d'accéder au système d'information de l'entreprise en tout lieu et tout instant. Cette mobilité idéale peut être déclinée en une mobilité interne sur les sites de l'intranet et en une mobilité externe, communément appelée nomadisme. Ce dernier, plus particulièrement, doit concilier les enjeux et les risques de l'accès distant.

Modèle (conceptuel) de données : ensemble de concepts et de règles permettant de définir comment représenter des informations dans un système informatique.

Multilinguisme : capacité d'adapter le logiciel, et notamment son interface homme/machine, à l'utilisateur en proposant le même contexte dans différentes langues. Cette caractéristique revêt un intérêt particulier pour l'emploi du logiciel en milieu international ainsi que dans le cas d'une exportation vers un pays tiers.

Multi-plates-formes : capacité d'un logiciel à être exploité sur des ordinateurs indépendamment de leur système d'exploitation (Windows, UNIX, LINUX, etc).

Service web : voir architecture orientée services.

Standard et norme : une norme est une définition détaillée validée par un organisme de normalisation qui regroupe des représentants des Etats. Un standard est une définition détaillée validée par un organisme de standardisation qui regroupe des industriels et/ou des associations d'utilisateurs. Un standard de fait est le résultat de la prédominance d'un acteur industriel du marché qui seul maîtrise et fait évoluer ce standard.On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données, interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en oeuvre (LCEN, Chapitre 1er, article 4).

Système d'information (SI) : il définit, en prenant en compte les règles du jeu ou de gestion de l'entreprise (ou du système considéré), l'information nécessaire à la décision, à la gestion et à la production de l'entreprise. Il définit également les moyens matériels et humains nécessaires au recueil et à l'utilisation de l'information, notamment ceux liés à la transformation de cette information en données. (norme NF Z 67-103)

Système informatique : sous-ensemble de systèmes de traitement de l'information, qui au moyen d'outils appropriés, permet d'assurer la collecte, le stockage, la transformation et la transmission des informations. (norme NF Z 67-101)

Système d'information et de communication (SIC) : le SIC recouvre les applications métiers SIOC, SIAG et IST, mais aussi les services transverses et les infrastructures physiques et logicielles.

SIOC : Systèmes d'information opérationnels et de communication.

SIAG : Systèmes d'information d'administration et de gestion.

SIST : Systèmes d'information scientifiques et techniques.