Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°26 du 24 juillet 2009

PARTIE PERMANENTE
Administration Centrale

Texte n°4

DIRECTIVE N° 8/DEF/DGSIC
définissant les règles à appliquer au système de postes terminaux.

Du *29 juin 2009*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 8/DEF/DGSIC définissant les règles à appliquer au système de postes terminaux.

Du 29 juin 2009

NOR D E F E 0 9 5 1 5 7 9 X

Référence :

Voir annexe III.

Pièce(s) Jointe(s) :

Trois annexes.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°26 du 24 juillet 2009, texte 4.

---

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit les règles d'usage et d'interopérabilité des postes terminaux du ministère de la défense.

Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

Cette directive s'inspire du cadre commun d'interopérabilité (CCI) du 4 décembre 2002, du projet de référentiel général d'interopérabilité (RGI) dans sa version provisoire V0.98 de juin 2007 et du projet de référentiel général de sécurité (RGS) dans sa version provisoire 0.98 de décembre 2008 prévu par l'ordonnance n° 2005-1516 (ORD) du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

1.2. **Niveaux de préconisation.**

Les règles présentées dans ce document ont différents niveaux de préconisation et sont conformes au RGI et à la RFC 2119 :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Modalités d'application.**

La présente directive s'applique à l'ensemble des postes terminaux du ministère de la défense, quels que soient l'objet de leur système d'information et leur niveau de classification. Elle ne concerne que le poste terminal et ses périphériques directs par les connecteurs installés qu'ils soient physiques ou virtuels. Le réseau et les ressources accessibles par le réseau sont exclus du périmètre de cette directive, sauf si leur accès a un impact direct sur le poste terminal.

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure concernant le poste terminal. La mise en application de ces règles dans les trois ans à partir de la date de parution de la directive reste de la responsabilité des organismes ou de la DIRISI pour les organismes dont les attributions correspondantes lui ont été confiées.

Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics en relation avec les postes terminaux.

1.4. **Gestion des dérogations pour les projets.**

Les dérogations sont instruites par un expert de haut niveau ou un directeur de projet, présentées en commission ministérielle technique des systèmes d'information et de communication (CMTSIC) et font l'objet d'une approbation par le directeur général des systèmes d'information et de communication. Elles concernent :

- les circonstances et justifications du non respect d'une règle recommandée ;

- les circonstances et justifications du non respect d'une règle déconseillée ;

- les justifications des exceptions à toute règle absolue (obligatoire ou interdit). Dans ce dernier cas, l'avis de la DGSIC doit être demandé au préalable et joint au dossier.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

- Ordonnance n° 2005-1516 du 8 décembre 2005 ;

- cadre commun d'interopérabilité ;

- référentiel général d'interopérabilité ;

- référentiel général d'accessibilité des administrations (RGAA) ;

- référentiel général de sécurité ;

- politique de référencement intersectoriel de sécurité (PRISv2) ;

- directive n° 1/DEF/DGSIC portant sur les logiciels du ministère de la défense (DGSIC001) ;

- directive n° 3/DEF/DGSIC/SDAI définissant les règles de la messagerie électronique (DGSIC002) ;

- directive n° 485/SGDN/DCSSI/DR du 1er septembre 2000 (1) : directive d'installation des sites et systèmes d'information : protection contre les signaux compromettants ;

- directive n° 495/SGDN/TTS/SSI /DR du 19 septembre 1997 (1) relative au zonage tempest ;

- directive n° 1223/SGDN/SSD du 23 décembre 2004 (1) relative à la protection physique des informations ou supports protégés ;

- instruction générale interministérielle n°1300/SGDN/PSE/SSD (1) relative à la protection du secret de la défense nationale ;

- instruction interministérielle n° 920/SGDN/DCSSI du 12 janvier 2005 (1) relative aux systèmes traitant des informations classifiées de défense de niveau « Confidentiel Défense » ;

- instruction n° 900/DEF/CAB/DR du 18 juin 2007 (1) relative à la protection du secret de la défense nationale au sein du ministère de la défense ;

- instruction n° 1591/DEF/CAB/C23/FSI/DR du 5 mai 1987 (1) relative aux mesures de sécurité informatique à appliquer au traitement des informations ne relevant pas du secret de défense ;

- instruction n° 133/DEF/SEC.DIR.SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense ;

- instruction n° 4281/DEF/SEC.DIR.SIC/DR (1) relative aux systèmes traitant des informations classifiées de défense de niveau secret ;

- recommandation n° 600/DISSI/SCSSI de mars 1993 (1) : protection des informations sensibles ne relevant pas du secret de défense. Recommandations pour les postes de travail informatiques.

2.2. **Normes et standards applicables.**

2.2.1. ***Définitions.***

Mots-clés pour niveaux d'obligation (RFC 2119).

2.2.2. ***Infrastructure réseaux (accès).***

Port based network access control (802.1x).

2.2.3. ***Aspects prévention hygiène sécurité condition de travail (HSCT).***

- Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (ISO 9241) ;

- exigences ergonomiques pour travail sur écrans de visualisation à panneaux plats (ISO 13406).

2.2.4. ***Autres documents et sites de référence.***

- Recommandations du cadre général d'architecture technique (CGAT) ;

- directive n° 7/DEF/DGSIC du 13 janvier 2009 portant sur la téléphonie sur le protocole Internet (DGSIC003) ;

- 347/DEF/DGSIC du 28 juillet 2006 (1) (DGSIC004) - CMTSIC n° 2 ;

- 31/DEF/DGSIC du 22 janvier 2007 (1) (DGSIC005) - CMTSIC n° 3 ;

- 137/DEF/DGSIC du 7 février 2008 (1) (DGSIC006) - CMTSIC n° 6 ;

- www.w3.org.

3. DOMAINE COUVERT ET EMPLOI.

Le poste terminal est un dispositif matériel ou logiciel (au sens du point 3.2.2) assurant l'interface entre l'utilisateur et le système d'information. En tant que moyen générique d'accès au système d'information, il est soumis à deux contraintes :

- la banalisation du terminal :

  - dont l'évolution rapide ne peut permettre de dresser une spécification technique figée [multiplication des moyens matériels et logiciels d'accès à l'information : poste terminal fixe ou itinérant, smartphone, assistant personnel (PDA), téléphone mobile,...] ;

  - dont la maîtrise passe par un standard d'interfaçage universel ;

- la maîtrise de bout en bout de la chaîne d'accès à l'information.

La maîtrise est la capacité à contrôler au juste niveau les différents équipements et tronçons du système mis en œuvre en fonction du contexte d'emploi pour les domaines liés à la politique d'achat, la politique des systèmes d'information, la sécurité, les réseaux, la gestion, l'administration, ...

3.1. **Services attendus du système.**

Le système de postes terminaux doit permettre d'accéder à tout ou partie du système d'information du ministère de la défense en tout temps et tout lieu sous réserve des droits attribués à l'utilisateur, du poste terminal utilisé et des règles de sécurité en vigueur.

Les besoins d'accès à plusieurs réseaux de classification différente nécessitent actuellement plusieurs postes de travail dédiés par niveau de classification. Pour le long terme, l'objectif d'une part de rationalisation et d'autre part de simplification pour les usagers est la mise en place de postes multi-niveaux visant à mutualiser l'accès à plusieurs niveaux de confidentialité via un même poste physique en respectant les contraintes de sécurité.

3.2. **Périmètre et limites.**

Le système de postes terminaux est à la confluence de toutes les problématiques techniques et organisationnelles en matière de système d'information et de communication (SIC) :

- architectures et services : client léger/lourd/riche, architectures n-tiers et SOA, émergence du Web 2.0, poste multi-niveaux ;

- sécurité : gestion et protection de l'accès au poste, données transitant ou stockées sur le poste de travail, sécurisation des composants matériels ou logiciels, anti-virus, chiffrement des données, application des correctifs de sécurité...;

- gestion et supervision : administration et supervision du poste de travail dans un contexte encore très hétérogène, rôle des principaux acteurs, maintien de la configuration du poste, supervision de la sécurité ;

- acquisition, soutien : modes d'acquisition encore très variés [organismes, programmes pour les système d'information opérationnel et de communication (SIOC)...], rôle et capacité d'intervention des acteurs dans la chaîne de soutien, assistance à l'utilisateur (help desk, formation en ligne, formation...).

Enfin, le système de postes terminaux s'inscrit :

- dans des contextes d'emploi variés : sédentaire/mobile, infrastructure en et hors métropole/états-majors projetés, environnement tactique, média (téléphone, assistant personnels...) ;

- dans un contexte technologique en constante évolution, intégrant :

  - des systèmes d'exploitation diversifiés (Windows, Mac OS, Linux) ;

  - des technologies implémentées ou émergentes, notamment la virtualisation ;

- dans un contexte d'exigence où des utilisateurs avisés ne comprennent pas toujours pourquoi ils n'ont pas le même niveau d'offre en tant que professionnel que celui auquel ils accèdent en tant que consommateur privé et inversement. Lors des changements d'application ou de services susceptibles de modifier les habitudes de travail des utilisateurs, la mise en œuvre de programme d'accompagnement des utilisateurs est à systématiser.

Les systèmes d'armes, les systèmes d'information tactiques bas (systèmes d'information terminaux) sont exclus du périmètre de la présente directive.

3.2.1. ***Périmètre matériel couvert.***

- ordinateurs de bureau, portables et ultra-portables, « ultra mobile personnal computer » (UMPC) ;

- assistants personnels, tablettes PC dotées de fonctionnalités IP, téléphones portables et smartphones en tant que postes terminaux et non pas en tant que périphériques d'un poste terminal ;

- périphériques connectés en direct, périphériques sans fil : stockage, impression, scanner,...

3.2.2. ***Périmètre logiciel couvert.***

- les systèmes d'exploitation ;

- les logiciels courants indispensables au fonctionnement du poste terminal ;

- les logiciels courants de l'utilisateur (navigateur, suite bureautique, messagerie,...) ;

- les applications métiers.

Seuls les logiciels courants de l'utilisateur et les applications métiers nécessitant l'installation de composants sur le poste terminal ou une modification temporaire ou définitive de sa configuration sont concernés.

3.3. **Profil des postes.**

Quatre types de postes terminaux sont définis.

Les critères de différentiation portent sur le type de réseau auquel se connecte le poste terminal. Plus le réseau est contraint, plus le poste de travail devra être autonome.

- Type 1 : poste banalisé fixe non contraint en débit qui s'appuie sur un réseau fixe maîtrisé par le ministère de la défense ou sur un réseau civil non maîtrisé ;

- type 2 : poste banalisé mobile qui s'appuie sur un réseau fixe maîtrisé par le ministère de la défense ou sur un réseau civil non maîtrisé ;

- type 3 : poste banalisé permettant une autonomie complète qui s'appuie sur un réseau projetable contraint en débit, maîtrisé par le ministère de la défense ;

- type 4 : poste spécifique.

La contrainte de débit est liée aux fonctionnalités attendues (vidéo, mise à jour du système, traitement d'images,...) et à leurs adéquations par rapport au réseau support.

3.3.1. ***Type 1.***

Il s'agit de la grande majorité des postes du ministère, installés en fixe sur un réseau. Ils intègrent aussi bien des applicatifs courants que des applicatifs métiers. Connectés à un réseau non contraint, ils peuvent utiliser les ressources du réseau pour accéder à l'information ou disposer des ressources d'un serveur.

Les postes bureautiques de type tour ou desktop, les postes des systèmes d'information opérationnels (SIO) stratégiques, opératifs, et tactiques haut sont des postes de type 1 (non exhaustif).

3.3.2. ***Type 2.***

Le deuxième profil de postes terminaux regroupe les postes permettant la mobilité. Ceux-ci peuvent être divisés en deux catégories :

- type 2a : les ordinateurs portables [ceux utilisés couramment sur le réseau du ministère, mais offrant à l'usager la possibilité de l'extraire du système d'information (SI) du ministère pour travailler, connecté (dans le cadre d'une solution d'accès aux intranets via un réseau non maîtrisé) ou non connecté, en déplacement, et ceux des SIO tactiques standards (par exemple portables SICF)], les tablettes personnal computer (PC), les ultra-portables ;

- type 2b : matériels mobiles dotés de fonctionnalités Internet Protocol (IP) de type PDA communicants ou non, smartphones, UMPC*...

Ces équipements doivent intégrer la totalité des applicatifs d'usage courant et métiers nécessaires pour permettre, en tous lieux (2), et en tout temps à l'usager d'accéder aux informations localement, voire à distance en fonction de la politique d'emploi et de la politique de sécurité mise en œuvre.

3.3.3. ***Type 3.***

Les postes de type 3 regroupent les postes utilisés sur les réseaux contraints. Employés principalement sur les systèmes d'information opérationnels et de communication (SIOC), ils ont la particularité de devoir intégrer, sur le terminal, les applicatifs d'usage courant et métiers nécessaires.

Les SIO tactiques standards de type Maestro sont de type 3.

3.3.4. ***Type 4.***

Les terminaux ne rentrant pas dans les trois premiers types sont spécifiques.

Les postes téléphoniques IP, les terminaux isolés rentrent dans cette catégorie.

4. LES RÈGLES.

Les règles sont regroupées et énoncées suivant les aspects technique (RT), organisationnel (RO) et sémantique (RS). Elles sont numérotées séquentiellement par catégorie.

4.1. **Règles techniques.**

4.1.1. ***Adhérence.***

L'adhérence d'une application à un système d'exploitation ne permet pas le renouvellement du parc informatique, tant dans sa composante matérielle que dans sa composante logicielle dans de bonnes conditions. La non adhérence permet le remplacement d'un composant (nouvelle version, composant autre) sans impact ou modification du contexte dans lequel il agit.

Il est donc important que les nouvelles applications utilisées au sein du ministère ne soient pas adhérentes au système d'exploitation.

- RT ADH1 : il est recommandé que les nouvelles applications utilisées ne soient pas adhérentes au système d'exploitation ;

- RT ADH2 : il est recommandé de mettre en œuvre des mécanismes minimisant la dépendance au poste terminal pour les applications adhérentes existantes : webisation, virtualisation, déport d'affichage, émulation, client lourd multi plateforme,...

- RT ADH3 : il est recommandé d'utiliser des technologies applicatives indépendantes du système d'exploitation du poste terminal ;

- RT ADH4 : il est obligatoire de mettre en place des périphériques non adhérents au système d'exploitation (pilotes et protocoles utilisables par les différents systèmes d'exploitation déployés au sein du ministère).

4.1.2. ***Contrôle d'accès.***

Plusieurs contrôles d'accès sont à distinguer :

- le contrôle d'accès de l'utilisateur au poste terminal ;

- le contrôle d'accès du poste terminal au réseau ;

- le contrôle d'accès de l'utilisateur à un service accessible par le réseau.

4.1.2.1. Contrôle d'accès de l'utilisateur au poste terminal (identification/authentification).

- RT CAUT 1 : il est obligatoire de procéder à une identification et à une authentification pour accéder à un poste terminal de type 1 ou 2a ;

- RT CAUT 2 : il est recommandé de procéder à une identification et à une authentification pour accéder à un poste terminal de type 2b, 3 ou 4 ;

- RT CAUT 3 : il est obligatoire que le processus d'identification initial sur le poste terminal (hors type 2b) identifie une personne physique, et non une fonction ou une organisation.

Par exemple, les administrateurs doivent s'identifier en tant qu'individu et ensuite faire connaître du système leur fonction (ou mieux que le système sache quelle est leur fonction). Il découle naturellement de cette règle qu'un identifiant ne peut donc pas être partagé.

- RT CAUT 4 : il est recommandé que le processus d'identification initial sur le poste de travail de type 2b identifie une personne physique, et non une fonction ou une organisation ;

- RT CAUT 5 : il est interdit de stocker en clair les clefs privées sur le poste terminal pour les postes traitant des informations classifiées de défense. Ces dernières doivent se situer sur un support

extérieur et être protégées. L'interdiction peut être levée à la condition de disposer sur le poste de travail d'un dispositif de chiffrement agréé CD permettant de protéger la clef même chiffrée par le dispositif de sécurité d'utilisation du certificat. Cela contribue également à mettre en œuvre une authentification forte (exemple : solution de sécurité Muse).

4.1.2.2. Contrôle d'accès du poste terminal au réseau.

- RT CATR 1 : il est obligatoire de mettre en place des mécanismes de contrôle d'accès au réseau physique pour les terminaux mobiles (terminaux de type 2) reposant sur les standards 802.1x ;

- RT CATR 2 : il est obligatoire de mettre en place les mécanismes appropriés pour vérifier automatiquement la bonne conformité du poste terminal par rapport à la politique de sécurité et de configuration de l'entité ;

Les mécanismes appropriés seront définis par les politiques de sécurité technique des réseaux supports.

- RT CATR 3 : il est recommandé que la mise à jour des composants de sécurité (anti virus, anti pourriels, firewall,...) et des correctifs de sécurité des logiciels installés sur le poste terminal se fasse automatiquement à sa connexion au réseau local.

Le reste des mises à jour relève de la politique de gestion de parc.

4.1.2.3. Contrôle d'accès de l'utilisateur à un service accessible par le réseau.

Le contrôle d'accès de l'utilisateur à un service accessible par le réseau sera traité dans une directive à paraître.

- RT CAUR 1 : il est interdit d'utiliser les variables d'environnement du système d'exploitation du poste pour identifier un accès à une application critique ;

- RT CAUR 2 : il est déconseillé d'utiliser les variables d'environnement du système d'exploitation du poste pour identifier un accès à une application non critique.

- Il est nécessaire de différencier les applications critiques des applications banales. Les commissions métiers détermineront la criticité des applications.

- RT CAUR 3 : pour chaque application, le directeur d'application devra obligatoirement définir les conditions de stockage de l'information « Login/mot de passe » en local, selon la criticité de l'application et du besoin de traçabilité ;

- RT CAUR 4 : il est recommandé de mettre en place des mécanismes de mutualisation des accès aux applications (Certificats, SSO, ...) ;

- RT CAUR 5 : il est obligatoire que l'authentification soit forte pour les abonnés mobiles d'un réseau sensible ou relevant du classifié de défense, se connectant à distance via un réseau non maîtrisé à son système d'information.

4.1.3. ***Administration et configuration du poste terminal.***

- RT ADM1 : il est interdit de déployer des multiboots sur les postes terminaux de type 1, 2, et 3 ;

- RT ADM2 : il est recommandé d'activer la fonctionnalité de surveillance des disques durs (technologie smart) sur les postes terminaux (hors type 2b), afin de permettre de détecter une éventuelle défaillance du disque dur lors de son démarrage.

*4.1.4. **Virtualisation.***

La virtualisation est une solution envisageable pour traiter l'adhérence d'une application à un composant physique du poste terminal. Elle ne permet pas de résoudre l'adhérence d'une application au système d'exploitation, mais d'éviter le blocage du choix d'un composant (système d'exploitation ou logiciel) sur le poste terminal, au prix d'un surcoût d'administration du à un composant supplémentaire (hyperviseur).à administrer.

Elle permet d'éviter ainsi que l'adhérence ne se propage à l'ensemble du poste terminal.

Lors de la mise en place de solutions de virtualisation, un accès console sur le serveur physique ou sur l'hyperviseur peut compromettre l'ensemble des serveurs virtuels hébergés. En conséquence, il est primordial de séparer en terme d'administration, l'administration du serveur physique et de la virtualisation et l'administration des serveurs virtuels.

L'ensemble des règles énoncées dans la présente directive s'applique autant pour le poste hôte que pour le poste virtuel.

*4.1.5. **Système d'exploitation.***

Le middleware identité authentification signature (IAS) a pour objectif de permettre et de faciliter les déploiements de cartes à puce au sein des administrations françaises. Les cartes à puce sont des supports matériels permettant de contribuer à l'établissement de la confiance dans les relations entre administrations et entre les usagers et les administrations.

Les systèmes d'exploitation utilisés sur les postes terminaux du ministère doivent pouvoir implémenter le middleware IAS.

RT SE : Il est obligatoire que le système d'exploitation du poste terminal (hors type 2b) soit compatible avec le middleware IAS.

*4.1.6. **Logiciels.***

Afin d'optimiser le déploiement et l'administration des postes de travail, les axes suivants sont systématiquement à privilégier :

- améliorer l'interopérabilité :
    - favoriser l'harmonisation des versions des logiciels ;
    - privilégier l'utilisation de formats standards (png, pdf,...), à défaut, systématiser les visionneuses.
- s'assurer de la compatibilité des produits ;
- améliorer la sécurité des systèmes d'information ;
- favoriser la mutualisation de l'acquisition des logiciels : rationalisation des achats ;
- homogénéiser les besoins en logiciels ;
- réduire le nombre de masters logiciels ;
- banaliser le poste de travail ;

- privilégier les logiciels multi plateformes.

4.1.7. ***Applications services à l'utilisateur.***

4.1.7.1. Navigateur et client riche.

RT NAV : Il est recommandé d'utiliser un navigateur conforme à plus de 70 p. 100 du test Acid3.

4.1.7.2. Bureautique.

- RT BUR1: il est recommandé de déployer la suite bureautique multi-plateforme OpenOffice (hors terminaux inadaptés) ;

- RT BUR2 : il est obligatoire que la version OpenOffice déployée sur un poste Windows soit la version interministérielle MiMOOo.

4.1.8. ***Utilisation de solutions de partage de périphérique clavier, écran, souris.***

L'emploi d'une solution de partage de périphériques écran, clavier et souris est autorisée si le dispositif ne permet pas de stocker d'informations résiduelles. Les deux règles suivantes visent à définir une cible à atteindre en terme de qualification de produits à utiliser sur les intranets du ministère de la Défense. Elles ont pour objectif, à terme d'être rendues obligatoires. La règle RT KVM1 est pour le moment recommandée.

- RT KVM1 : dans le cas ou un organisme met en place des solutions de partage de périphériques clavier écran souris entre postes « non protégé » (pouvant être connecté à l'Internet) et « diffusion restreinte », il est recommandé que la solution choisie soit qualifiée au niveau standard ;

- RT KVM2 : dans le cas ou un organisme met en place des solutions de partage de périphériques clavier écran souris entre postes « confidentiel défense » et « diffusion restreinte », il est obligatoire que la solution choisie soit qualifiée au niveau renforcé.

Les niveaux « standard » et « renforcé » sont définis dans les règles relatives à la qualification des produits de sécurité par la DCSSI, version 1.1, n° 451/SGDN/DCSSI/SDR du 26 février 2004 (1).

4.1.9. ***Sauvegarde des données de travail hébergées sur le poste terminal.***

La politique de sauvegarde doit être décrite dans les politiques d'exploitation des systèmes d'information.

RT SVG : il est obligatoire pour les organismes de disposer d'une politique de sauvegarde des données hébergées localement sur les postes terminaux. Cette politique doit être connue des utilisateurs.

4.1.10. ***Protection physique du poste de travail.***

RT PRO : il est obligatoire pour les organismes de faire connaître aux utilisateurs les règles de protection physique des postes terminaux qu'ils utilisent.

4.2. **Règles organisationnelles.**

4.2.1. ***Administration, configuration.***

Le système d'exploitation virtualisé peut avoir accès aux ressources de la machine et utiliser directement les différents ports, par ailleurs éventuellement verrouillés par l'application de la politique de sécurité en vigueur. Il est donc indispensable de bloquer les ports de l'OS virtualisé :

- RO ADM1 : il est obligatoire que toute entité ait une politique de configuration et de sécurité du poste terminal intégrant sa vérification et sa mise à niveau ;

- RO ADM2 : il est obligatoire d'administrer un poste de travail virtualisé à l'identique d'un poste de travail classique ;

- RO ADM3 : il est obligatoire que tout logiciel exécutable sur un poste terminal ait été préalablement validé sous les axes gouvernance, emploi, SSI, intégration.

À titre d'exemple, un logiciel relevant d'une politique ministérielle doit être validé par un organisme ministériel (DGSIC, FSSI, commissions métiers pour l'emploi,...). Sinon, il peut être validé par un service central (bureau SIC d'organisme, centre référent, DIRISI).

- RO ADM4 : il est obligatoire d'avoir une gestion financière, technique (version), juridique et administrative des licences des systèmes d'exploitation et des logiciels installés sur le poste terminal au niveau national, à défaut au niveau régional, à défaut au niveau local ;

- RO ADM5 : il est obligatoire de mettre en place des procédures de reconditionnement du poste terminal lors d'un changement d'affectation administratif du matériel. Ces procédures de reconditionnement doivent permettre de disposer de postes vierges de toutes données antérieures.

Cette règle est applicable notamment lors de changement d'affectation de matériel, et lors de mise en réparation de tout terminal SIAG, SIOC, SIST à l'extérieur du ministère. En cas de mutation, les données professionnelles seront transmises au successeur sous la responsabilité de l'utilisateur.

- RO ADM6 : il est déconseillé de déployer des systèmes d'exploitation sans capacité de mise à jour centralisée (3) pour les terminaux de type 1, 2a et 3.

Pour les postes utilisés sur des réseaux contraints, il s'agit de prévoir le dispositif permettant la mise à jour de manière centralisée de plusieurs terminaux en même temps.

- RO ADM7 : il est obligatoire d'avoir une mise à disposition centralisée des mises à jour des systèmes d'exploitation et des logiciels des postes terminaux ;

- RO ADM8 : il est recommandé de mettre en œuvre une procédure de mise à jour centralisée des logiciels le permettant et des systèmes d'exploitation des postes terminaux.

Cette règle rationalise la mise à jour des logiciels. Pour les postes utilisés sur des réseaux contraints, il s'agit de prévoir le dispositif permettant la mise à jour de manière centralisée de plusieurs terminaux en même temps ;

- RO ADM9 : il est obligatoire qu'un responsable de déploiement de logiciels définisse des procédures de déploiement et de mise à jour des logiciels ;

- RO ADM10 : il est interdit de donner la totalité des droits d'administration du poste terminal à l'utilisateur. Une délégation partielle (limitée) des droits d'administration est tolérée si elle est prévue dans les procédures d'exploitation et/ou politiques de sécurité informatique.

4.2.2. ***Développement local.***

RO DEV : il est interdit aux utilisateurs d'effectuer tout développement d'applications locales ou impactant le poste terminal.

Cette règle a pour objectif d'interdire l'informatique noire. Les utilisateurs développant sous leur responsabilité des applications ne pourront s'en prévaloir en cas de non compatibilité avec une évolution logicielle.

Les besoins nouveaux des utilisateurs doivent être fédérés par le responsable de la zone fonctionnelle concernée du plan d'occupation des sols.

4.2.3. ***Rationalisation des postes de travail et des périphériques associés.***

Afin d'assurer la cohérence des systèmes d'information, et surtout de réduire les coûts d'acquisition et de possession, les postes terminaux et leur périphériques doivent être rationalisés.

Cette rationalisation implique d'une part une standardisation de la configuration matérielle et logicielle des postes terminaux et de leurs périphériques directs et d'autre part, des mesures organisationnelles permettant de faciliter l'administration des postes.

Concernant les ordinateurs de bureau, deux configurations de terminaux sont possibles :

- un ordinateur de bureau standard, doté d'une configuration matérielle non évolutive (configuration mémoire et disque dur figées) permettant l'utilisation des logiciels d'utilisation courants (bureautique, messagerie, navigation,...) ;

- un ordinateur de bureau hautes performances, doté d'une configuration matérielle évolutive (modifications possibles des configurations matérielles) permettant l'utilisation de logiciels spécifiques requérant des ressources système exigeantes.

Pour les ordinateurs portables (type 2), les configurations matérielles suivantes sont possibles :

- un ordinateur ultraportable ;

- un ordinateur portable standard ;

- un ordinateur portable hautes performances ;

- un ordinateur portable durci.

Les énumérations ci-dessus correspondent à la terminologie utilisée dans le marché d'acquisition des postes terminaux.

Afin de rationaliser l'utilisation des périphériques et s'inscrire dans une dynamique de développement durable, le recours à des périphériques partagés est à privilégier. Tout périphérique dédié devra faire l'objet d'une justification fonctionnelle.

- RO RAT1 : il est recommandé de mettre en place des imprimantes avec une interface réseau, à capacité recto verso et multipages et de limiter au strict minimum les périphériques non partagés ;

- RO RAT2 : il est déconseillé d'avoir des imprimantes dédiées à un utilisateur ;

- RO RAT3 : il est déconseillé de mettre en place des imprimantes jet d'encre pour un usage bureautique ;

- RO RAT4 : il est obligatoire que les marchés d'approvisionnement du ministère imposent aux fournisseurs une compatibilité des pilotes vis à vis des systèmes d'exploitation autorisés au sein du ministère ;

- RO RAT5 : il est obligatoire d'acquérir des périphériques non adhérents au système d'exploitation (pilotes et protocoles utilisables par les différents systèmes d'exploitation déployés au sein du ministère).

4.2.4. ***Chiffrement des mémoires de masse.***

Le chiffrement des mémoires de masse permet de protéger la confidentialité des données. Des précautions doivent néanmoins être prises afin de pouvoir recouvrir les données en cas de perte de mot de passe, de besoin d'accéder aux données en l'absence de l'utilisateur,...

RO CHI1 : il est obligatoire que la qualification (au sens des critères communs) de l'outil de chiffrement de la mémoire de masse soit adaptée au niveau de confidentialité des données stockées :

- standard pour la protection des données sensibles ;

- renforcé pour la protection des données classifiées « confidentiel défense » ;

- élevé pour la protection des données classifiées « secret défense ».

En l'absence de produits qualifiés au niveau adapté disponibles sur le marché, une tolérance d'utilisation de produits de moindre qualification peut être autorisée sous couvert du FSSI.

RO CHI2 : Il est obligatoire de disposer d'une solution de recouvrement des informations (clé, certificats,...) ayant permis l'opération de chiffrement de manière technique ou organisationnelle dans le cadre d'un chiffrement local des données.

4.2.5. ***Prévention hygiène sécurité condition de travail (HSCT).***

RO HSCT : il est recommandé d'aménager l'environnement du poste terminal de façon ergonomique, en tenant compte des caractéristiques physiques de l'utilisateur conformément aux normes ISO 9241 et ISO 13406.

4.3. **Règles sémantiques.**

Sans objet.

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

Henri SERRES.

---

(1) n.i. BO.

(2) Tout en respectant les réglementations spécifiques des pays hôtes (crytographie notamment dans certains pays).

(3) Capacité du système d'exploitation à être mis à jour à partir d'une seule source distante (un ou plusieurs serveurs synchronisés sur un serveur maître) mettant à disposition les mises à jour des composants du système d'exploitation.

ANNEXE I.

TABLEAU RÉCAPITULATIF DE L'APPLICABILITÉ DES RÈGLES PAR TYPE DE POSTE TERMINAL.

	Poste banalisé fixe non contraint en débit qui s'appuie sur un réseau fixe maîtrisé.	Poste banalisé mobile qui s'appuie sur un réseau fixe maîtrisé (ordinateurs portables, tablettes Pc, ultraportables).	Poste banalisé mobile qui s'appuie sur un réseau fixe maîtrisé (PDA, smartphones, UMPC).	Poste banalisé permettant une autonomie complète qui s'appuie sur un réseau projetable contraint en débit.	Poste spécifique.
RT ADH1	R	R	R	R	R
RT ADH2	R	R	R	R	R
RT ADH3	R	R	R	R	R
RT ADH4	O	O	O	O	O
RT CAUT1	O	O	-	-	-
RT CAUT2	-	-	R	R	R
RT CAUT3	O	O	-	O	O
RT CAUT4	-	-	R	-	-
RT CAUT5	I	I	I	I	I
RT CATR1	-	O	O	-	-
RT CATR2	O	O	O	O	O
RT CATR3	R	R	R	R	R
RT CAUR1	I	I	I	I	I
RT CAUR2	D	D	D	D	D

RT CAUR3	O	O	O	O	O
RT CAUR4	R	R	R	R	R
RT CAUR5	-	O	O	-	-
RT ADM1	I	I	I	I	-
RT ADM2	R	R	-	R	R
RT SE	O	O	-	O	O
RT NAV	R	R	R	R	R
RT BUR1	R	R	-	R	R
RT BUR2	O	O	-	O	O
RT KVM1	R	R	R	R	R
RT KVM2	O	O	O	O	O
RT SVG	O	O	O	O	O
RT PRO	O	O	O	O	O
RO ADM1	O	O	O	O	O
RO ADM2	O	O	O	O	O
RO ADM3	O	O	O	O	O
RO ADM4	O	O	O	O	O
RO ADM5	O	O	O	O	O
RO ADM6	D	D	-	D	-

RO ADM7	O	O	O	O	O
RO ADM8	R	R	R	R	R
RO ADM9	O	O	O	O	O
RO ADM10	I	I	I	I	I
RO DEV	I	I	I	I	I
RO RAT1	R	R	R	R	R
RO RAT2	D	D	D	D	D
RO RAT3	D	D	D	D	D
RO RAT4	O	O	O	O	O
RO RAT5	O	O	O	O	O
RO CHI1	O	O	O	O	O

ANNEXE II.

GLOSSAIRE ET ACRONYMES.

802.1x : 802.1x est un standard de l'IEEE pour le contrôle d'accès au réseau basé sur les ports. C'est aussi une partie du groupe de protocoles IEEE 802 (802.1). Ce standard fournit une authentification aux équipements connectés à un port Ethernet. Il est aussi utilisé pour certains points d'accès Wi-Fi et est basé sur EAP (RFC 2284, obsolète avec l'arrivée de RFC 3748). 802.1x est une fonctionnalité disponible sur certains commutateurs réseau.

Acid3 : publié en mars 2008, Acid3 désigne un test pour navigateur web destiné à soumettre les moteurs de rendu à un panel de tests vérifiant leur capacité à supporter un choix de fonctionnalités relevant de différents standards du Web.

Pour passer le test, un navigateur doit, avec ses réglages par défaut, faire le rendu fluide d'une animation dont l'image finale doit correspondre exactement à une image de référence, avec un score de 100/100. Pour cela, le navigateur doit implémenter correctement certains aspects du DOM2, d'ECMAScript, des CSS, du SVG, du XML et des URIs. Le test Acid3 n'est donc pas un test de conformité global à ces spécifications, comme le sont en revanche les tests suites du W3C concernant DOM, CSS, SVG et XML.

Adhérence : l'adhérence du poste de travail qualifie la relation exclusive à un système d'exploitation ou à une autre brique logicielle et correspond à la dépendance d'une application envers une version donnée d'une suite bureautique ou d'un système d'exploitation ou d'une brique sur socle de base du poste terminal (messagerie, environnement...) fourni par un éditeur ou un fournisseur unique.

La non adhérence traduit la capacité de remplacement d'un composant sans impact ou modification du contexte dans lequel il interagit.

Authentification : voir Identification.

CGAT : cadre général d'architecture technique.

Client/Serveur : au sens général, le client est un composant qui émet des requêtes à destination d'un fournisseur de services connu de ce client. Ce terme a un sens matériel (machine client) mais aussi un sens logique (logiciel client). Le serveur est ce fournisseur de services qui va à l'inverse recevoir des appels provenant parfois d'un nombre très élevé de clients et fournir en retour les réponses attendues. Au sens logiciel, la notion client/serveur peut sous-entendre un lien très étroit entre les deux parties : on parle alors de client lourd. Lorsqu'il n'y a pas de lien étroit autre que celui du respect des protocoles standards pour échanger de l'information, on parle de client léger ou de client riche.

Client lourd : c'est une application en architecture client/serveur dont la partie cliente intègre une grande partie du code applicatif. Le client lourd est donc dédié, c'est à dire spécifiquement écrit pour optimiser les communications et faciliter les traitements. Pour ce faire, il présente souvent des adhérences au système d'exploitation parce qu'il en utilise certaines couches logicielles (réutilisation du code présent dans les bibliothèques de fonctions partagées).

Historiquement, les programmes client/serveur étaient basés sur un client lourd. Le problème qu'ils posent est la complexité de leur déploiement. À chaque nouvelle version du logiciel, il est nécessaire de l'installer sur tous les postes qui l'utilisent.

Client léger au sens logiciel : dans l'architecture client-serveur, c'est un logiciel dont le rôle est limité à de simples tâches, essentiellement d'affichage. On parle d'outil de présentation de l'information. La configuration matérielle nécessaire peut être particulièrement légère, sauf dans le cas de la manipulation d'objet multimédia (son, vidéo, etc.).

En général, le client léger est constitué par un navigateur Web qui communique avec un serveur à travers des protocoles standards tels que HTTP. Ce navigateur est un logiciel permettant d'accéder et d'afficher des pages

Web incluant des objets multimédias. On parle aussi de client pauvre du fait des limitations du langage HTML.

Il peut, moyennant l'adjonction de logiciels complémentaires ou l'utilisation de logiciels coexistants sur le poste de travail ou le réseau, afficher d'autres types de documents ou offrir des capacités de traitement particuliers. Ces adjonctions peuvent à nouveau conduire à l'adhérence au système d'exploitation.

Par opposition au client lourd, un client léger ne nécessite pas de déploiement lié aux évolutions d'une application, puisque la logique applicative est entièrement implémentée du côté du serveur : le client n'effectue que des tâches d'affichage, de saisie et de validation simples.

Client riche : on oppose le client riche au client pauvre. Le client riche est un programme qui permet d'afficher l'interface utilisateur d'une application distante, une application web la plupart du temps, tout en conservant le comportement et l'ergonomie identiques à ce que l'on trouve proposé par l'interface graphique offerte par le système d'exploitation (copier/coller, déplacer, glisser/déposer entre applications, etc.). Le client riche conserve la caractéristique principale du client léger qui est de ne pas assurer la partie traitement métier toujours dévolue au serveur.

Client léger au sens matériel : poste de travail partiellement ou complètement dépourvu de capacités d'extension et de stockage (pas de lecteur de cédérom, ni de disque dur, etc) supprimant le risque de contamination et simplifiant le déploiement. Il charge son système au démarrage depuis le réseau : système complet ou sous la forme de microcode permettant la présentation d'une interface graphique à l'utilisateur et lui offrant la possibilité d'interagir avec celui-ci (écran/clavier/souris). La capacité de traitement et la persistance des données sont en général totalement confiées à un serveur distant (déport d'affichage) mais il peut éventuellement embarquer des capacités de traitements graphiques et de compression/décompression des flux réseau.

CMTSIC : commission ministérielle technique des systèmes d'information et de communication.

CSS : cascading style sheets : feuilles de style en cascade) est un langage informatique servant à décrire la présentation des documents HTML et XML. Les standards définissant CSS sont publiés par le World Wide Web Consortium (W3C). Introduit au milieu des années 1990, CSS devient couramment utilisé dans la conception de sites web et bien pris en charge par les navigateurs web dans les années 2000.

DOM : le document object model (ou DOM) est une recommandation du W3C qui décrit une interface indépendante de tout langage de programmation et de toute plate-forme, permettant à des programmes informatiques et à des scripts d'accéder ou de mettre à jour le contenu, la structure ou le style de documents. Le document peut ensuite être traité et les résultats de ces traitements peuvent être réincorporés dans le document tel qu'il sera présenté.

Emulation : simulation par un logiciel du comportement d'un autre système d'exploitation accédant à une couche matérielle différente de celle de l'environnement d'accueil. Il s'agit d'une représentation virtuelle mais limitée d'un appareil (un ordinateur ou une console de jeux) sur une autre machine. Le principe consiste à convertir les commandes non comprises par l'une des machines à l'aide d'un logiciel, c'est à dire à interpréter toutes les instructions du processeur émulé. Cette solution est très coûteuse en ressources mais permet une totale indépendance entre l'architecture physique et l'architecture émulée. Elle ne permet pas d'offrir les mécanismes assurant la répartition équitable des ressources employées, à la différence de la virtualisation.

HSCT : hygiène sécurité condition de travail.

KVM : keyboard video mouse. Commutateur permettant de partager un écran, un clavier, une souris entre plusieurs ordinateurs.

Identification/Authentification : l'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire connaître du système par un élément dont on l'a doté. S'identifier, c'est communiquer son identité. S'authentifier, c'est

apporter la preuve de son identité sous l'une des formes suivantes :

- ce qu'il sait (facteur mémoriel : mot de passe, code PIN, phrase secrète,...) ;

- ce qu'il possède (facteur matériel : carte magnétique, carte à puce, clé USB, token,...) ;

- ce qu'il est (facteur corporel : biométrie : empreinte digitale, empreinte rétinienne, structure osseuse du visage,...) ;

- ce qu'il sait faire (facteur réactionnel) biométrie comportementale : signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul,....

Authentification simple ou faible : l'authentification ne repose que sur un seul élément ou « facteur » (exemple : utilisation d'un mot de passe).

Authentification forte : l'authentification repose sur deux facteurs ou plus (ex : authentification réalisée par un mot de passe à usage unique ou infrastructure de gestion de clés).

IAS : identité authentification signature. Spécification technique de la carte à puce intégrant la plate-forme commune pour l'eAdministration. Elle est établie par le groupement des industriels de la carte à puce (sous groupe carte à puce du GIXEL) à la demande du SDAE. Elle a pour objectif de mutualiser le développement des masques de cartes à puce en prévision d'une diminution des coûts et d'un accroissement de l'interopérabilité. La PRIS V2.x spécifie qu'une carte à puce respectant les exigences du socle commun IAS, sous réserve de certification au niveau approprié (EAL 4+) répond aux exigences de la signature présumée fiable.

IP : internet protocol.

Machine virtuelle : une machine virtuelle est un conteneur totalement isolé capable d'exécuter ses propres systèmes d'exploitation et applications et de gérer les ressources qui lui ont été allouées (CPU, mémoire RAM, disque durs et cartes d'interface) à l'instar d'un ordinateur physique.

Les machines Java sont les plus connues et leur intérêt réside dans le fait qu'elles rendent possible l'écriture de programmes indépendants du matériel utilisé en final. En effet, un programme développé pour la machine virtuelle pourra fonctionner sur n'importe quel ordinateur possédant une version installée de l'interpréteur qui reste nécessaire.

Avec l'arrivée de la virtualisation, le terme hérite d'une seconde définition. La machine virtuelle dans cette optique est la représentation logicielle, chargée en mémoire par la machine d'accueil, du couple « système d'exploitation invité, périphériques qui lui ont été présentés » et constituant un poste de travail ou un serveur virtuel.

Middleware (Logiciel médiateur) : logiciel qui permet le fonctionnement de plusieurs ordinateurs en coordination, en attribuant à chacun une tâche spécifique, comme les échanges avec les utilisateurs, l'accès aux bases de données ou aux réseaux.

Note : le terme « logiciel médiateur » désigne aussi un logiciel qui permet de coordonner le fonctionnement de plusieurs logiciels au sein d'un même ordinateur.

Middleware IAS : un pilote générique de carte à puce qui offre une interface générique côté matériel pour tous les lecteurs et cartes à puce certifiés IAS et trois interfaces de programmation (API) intermédiaires entre les applications et la carte à puce : deux interfaces standards dont la Crypto API Microsoft et le PKCS#11, plus une API IAS seule API permettant d'envisager de la signature présumée fiable.

PC : personnal computer : ordinateur personnel.

PDA : personnal digital assistant : assistant personnel.

Poste multiniveaux : poste permettant le traitement co-localisé d'informations de sensibilités (classifications) différentes.

Poste vierge : poste configuré par le service informatique avec les applicatifs d'usage courant et les applications métiers nécessaires à l'utilisateur et ne contenant aucune donnée utilisateur.

RGAA : référentiel général d'accessibilité pour les administrations.

RGI : référentiel général d'interopérabilité.

RGS : référentiel général de sécurité.

UMPC : ultra mobile personnal computer.

SI : système d'information.

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

SIC : système d'information et de communication.

SICF : système d'information et de commandement des forces.

SIOC : système d'information opérationnel et de communication.

SIST : système d'information scientifique et technique.

SMART : (self-monitoring, analysis, and reporting technology, littéralement technologie d'auto-surveillance, d'analyse et de rapport) est un système de surveillance du disque dur d'un ordinateur. Il permet de faire un diagnostic selon plusieurs indicateurs de fiabilité dans le but d'anticiper les erreurs sur le disque dur. Il permet de détecter les défaillances prévisibles, qui surviennent suite à la dégradation lente de certains composants, en particulier à cause de l'usure et du vieillissement des pièces mécaniques. La plupart des principaux fabricants de disques durs et de cartes mères supportent le système, au moins en partie. De nombreuses cartes mères afficheront un message prévenant d'une panne imminente du disque dur. L'implémentation n'est cependant pas effectuée de manière uniforme et les remontées d'erreurs dépendent des constructeurs.

Smartphone : téléphone mobile couplé à un assistant personnel.

Station blanche : poste isolé du système d'information permettant l'analyse contre les codes malveillants des supports amovibles en transit entre réseaux différents.

SOA : service oriented architecture : modèle d'interaction applicative mettant en œuvre des connexions entre divers composants logiciels. Un service désigne une action exécutée par un composant « fournisseur » à l'attention d'un composant « consommateur », fondé éventuellement sur un autre système.

SVG : scalable vector graphics (graphique vectoriel adaptable) est un format de données conçu pour décrire des ensembles de graphiques vectoriels et basé sur XML. Ce format est spécifié par le World Wide Web Consortium.

Variables d'environnement : les variables d'environnement sont des variables dynamiques utilisées par les différents processus d'un système d'exploitation (Windows, Unix, etc). Elles servent à communiquer des informations entre programmes qui ne se trouvent pas sur la même ligne hiérarchique, et ont donc besoin d'une convention pour se communiquer mutuellement leurs choix.

Virtualisation : technologies logicielles qui vont permettre l'exécution concurrentielle de plusieurs systèmes d'exploitation sur une seule machine physique, tout en garantissant leurs cloisonnements et la répartition optimale et contrôlée des ressources matérielles disponibles, comme s'ils fonctionnaient sur des machines physiques distinctes. Le logiciel de virtualisation va piloter l'installation puis l'exécution de chaque système d'exploitation et ne leur présenter que des périphériques standards en lieu et place des composants réels. Cela va masquer la complexité de la couche matérielle (il existe des milliers de pilotes de périphériques) et faciliter la substitution partielle de composants (remplacement d'une carte réseau, augmentation des capacités mémoire ou de la fréquence processeur, etc.) ou totale (déplacement vers une autre machine physique) sans devoir ni réinstaller ni reconfigurer le moindre pilote. Ce mécanisme va rendre indépendant le système d'exploitation et les applications qu'il héberge de la couche matérielle sur lequel il s'exécute. Ces technologies mettent alors un terme avec la luxueuse habitude de déployer un nouveau serveur physique, en général sur-dimensionné, pour accueillir un nouveau système d'information qui ne l'exploitera bien souvent qu'à un faible pourcentage de ses capacités. L'apparition de l'assistance matérielle à la virtualisation (prise en charge de fonctionnalités spécifiques par le matériel), la présence de plusieurs cœurs dans les microprocesseurs actuels et l'arrivée de mémoires RAM de très grandes capacités permettent alors la rationalisation des serveurs.

Il existe 3 types de virtualisation : la virtualisation hébergée, la virtualisation par hyperviseur simple (virtualisation matérielle) ou avec paravirtualisation.

La virtualisation hébergée : la virtualisation est réalisée par un service ajouté à un système d'exploitation tout à fait standard, qu'il soit destiné à un serveur (solutions Microsoft Virtual Server, VMWare Server) ou à un poste de travail (solutions Virtual PC, VirtualBox, etc). Cette technologie, apparue la première dans le monde x86, offre une grande souplesse à la manipulation des machines virtuelles mais ne peut toutefois garantir le même niveau de performances que celui des technologies employées par hyperviseur : le système hôte n'étant pas dédié offre d'autres services qui entrent en concurrence avec les ressources accédées par les invités. De plus, les mises à jour correctives ou de sécurité sont susceptibles de perturber le fonctionnement des machines invitées et une anomalie d'un composant logiciel de l'hôte peut rendre instable l'ensemble des machines hébergées.

La virtualisation par hyperviseur dite virtualisation matérielle : le moniteur de machines virtuelles est dans ce cas un noyau hôte allégé et optimisé pour ne réaliser qu'une seule tâche : faire fonctionner des machines virtuelles. Il s'agit donc d'un système d'exploitation dédié et épuré de toutes fonctionnalités non utiles (ex: VMWare ESX, Microsoft Hyper-V), réduisant considérablement les surfaces d'attaques, les contraintes de mises à jour et garantissant des performances optimales.

La virtualisation par hyperviseur avec paravirtualisation : ce moniteur, proposé par l'architecture Xen, va offrir en plus un moyen d'ouvrir des communications spécialisées avec les noyaux des systèmes d'exploitation invités qui ont été adaptés. Les techniques mises en œuvre permettent à la machine virtuelle invitée d'avoir conscience de son état virtuel et donc de profiter pleinement des fonctionnalités spécifiques offertes par l'hyperviseur afin d'optimiser certaines tâches. Cette technologie est en mesure de garantir les meilleures performances mais elle n'est réservée qu'à une gamme très limitée de systèmes d'exploitations invités (ceux qui peuvent être modifiés pour intégrer au sein de leur noyau certains appels spécifiques à l'hyperviseur). Avec l'arrivée de l'assistance matérielle à la virtualisation, Xen n'est plus limité à l'hébergement des seuls systèmes modifiés : AMD, Intel et autres constructeurs de périphériques proposent déjà des extensions pour les instructions x86 facilitant la virtualisation. Xen peut alors être considéré comme un hyperviseur simple lorsqu'il gère une machine virtuelle non adaptée, mais il sera encore plus efficace si son invité détient les modifications du noyau permettant la pleine coopération.

W3C : le World Wide Web Consortium, abrégé par le sigle W3C, est un organisme de normalisation à but non-lucratif, fondé en octobre 1994 comme un consortium chargé de promouvoir la compatibilité des technologies du World Wide Web telles que HTML, XHTML, XML, RDF, CSS, PNG, SVG et SOAP. Le W3C n'émet pas des normes au sens européen, mais des recommandations à valeur.

Webisation : c'est l'opération de migration d'une application informatique vers une solution de type Web (utilisation des techniques de l'Internet, c'est à dire HTTP, HTML, etc.). Un chantier de webisation intervient généralement sur un logiciel existant depuis longtemps et nécessitant une refonte. Un exemple typique est la

réécriture d'une application fonctionnant sur un mode connecté terminal (textuel ou semi-graphique) dans un mode Intranet où chaque utilisateur interagit avec l'application grâce à son navigateur. Cette opération peut, selon les cas, être iso-fonctionnelle si l'application web réécrite conserve les mêmes fonctionnalités que la précédente. À l'inverse, une webisation peut être l'occasion de faire une sélection des fonctionnalités à conserver, voire de mettre en place de nouvelles fonctionnalités utiles.

Web 2.0 : l'expression « Web 2.0 » a été proposée pour désigner ce qui est perçu comme un renouveau du World Wide Web. L'évolution ainsi qualifiée concerne aussi bien les technologies employées que les usages. En particulier, on qualifie de Web 2.0 les interfaces permettant aux internautes d'interagir à la fois avec le contenu des pages mais aussi entre eux. L'infrastructure du Web 2.0 est complexe et changeante, mais elle inclut les logiciels de serveur, la syndication de contenu, les protocoles de messagerie, des standards de navigation, et des applications clientes diverses (les plugins, ou greffons, non-standards sont généralement évités). Ces approches complémentaires fournissent au web 2.0 les capacités de stockage, de création et de diffusion qui vont au-delà de ce qui était précédemment attendu des sites web.

XML : XML (extensible markup language : langage extensible de balisage) est un langage informatique de balisage générique servant essentiellement à stocker/transférer des données de type texte Unicode structurées en champs arborescents. Ce langage est qualifié d'extensible car il permet à l'utilisateur de définir les balises des éléments. L'utilisateur peut multiplier les espaces de nommage des balises et emprunter les définitions d'autres utilisateurs.

ANNEXE III.

RÉFÉRENCES.

- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

- référentiel général d'interopérabilité (RGI) défini par ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives ;

- référentiel général d'accessibilité des administrations (RGAA) défini par ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives ;

- référentiel général de sécurité (RGS) défini par ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives ;

- exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (ISO 9241) ;

- exigences ergonomiques pour travail sur écrans de visualisation à panneaux plats (ISO 13406) ;

- directive sur les logiciels n° 1/DEF/DGSIC du 17 octobre 2006 (DGSIC001) ;

- directive n° 3/DEF/DGSIC/SDAI du 8 janvier 2008 (DGSIC002) définissant les règles de la messagerie électronique ;

- directive n° 7/DEF/DGSIC du 13 janvier 2009 (DGSIC003) portant sur la téléphonie sur le protocole Internet ;

- recommandations nationales du cadre commun d'interopérabilité (CCI) des systèmes d'information publics. Circulaires du Premier Ministre du 21 janvier 2002 et du 4 décembre 2002 (1) ;

- note n° 347/DEF/DGSIC du 28 juillet 2006 (1) (DGSIC004) - Compte rendu de la deuxième commission ministérielle technique des systèmes d'information et de communication (CMTSIC) ;

- note n° 31/DEF/DGSIC du 22 janvier 2007 (1) (DGSIC005) - Compte rendu de la troisième commission ministérielle technique des systèmes d'information et de communication (CMTSIC) ;

- note n° 137/DEF/DGSIC du 7 février 2008 (1) (DGSIC006)- Compte rendu de la sixième commission ministérielle technique des systèmes d'information et de communication (CMTSIC) ;

- politique de référencement intersectoriel de sécurité (PRIS) v2.1 du 6 novembre 2006 (ADAE et DCSSI) ;

- (RFC 2119) - Key words for use in RFCs to Indicate Requirement Levels (Best Current Practice 03/1997) ;

- (802.1x) - IEEE Std 802.1X - 2004 Port-based network access control ;

- recommandations du cadre général d'architecture technique (CGAT) - P06 F31 Rapport de synthèse 3 janvier 2007 v1.5.

(1) n.i. BO.