Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE



*BULLETIN OFFICIEL DES ARMEES*

**Edition Chronologique n°35 du 27 août 2010**

PARTIE PERMANENTE
Administration Centrale

Texte n°1

**DIRECTIVE N° 12/DEF/DGSIC**
portant sur la mobilité.

Du *1er juin 2010*

DIRECTION GÉNÉRALE DU SERVICE D'INFRASTRUCTURE DE LA DÉFENSE.

**DIRECTIVE N° 12/DEF/DGSIC portant sur la mobilité.**

*Du 1er juin 2010*

NOR D E F E 1 0 5 1 5 4 3 X

---

*Pièce(s) Jointe(s) :*

Trois annexes.

*Classement dans l'édition méthodique :* BOEM 160.11

*Référence de publication :* BOC N°35 du 27 août 2010, texte 1.

---

SOMMAIRE

4.1.1. Règles techniques liées à la mobilité interne.

4.1.2. Règles techniques liées à la mobilité externe.

4.1.2.1. Administration.

4.1.2.2. Sécurisation du canal de communication.

4.1.2.3. Configuration des ports de communication.

4.1.2.4. Cloisonnement des services.

4.1.2.5. Accès.

4.1.2.5.1. Infrastructure d'accès au service.

4.1.2.5.2. Point d'accès dédié.

4.1.2.5.3. Accès au réseau et systèmes d'information.

4.1.2.6. Sécurité.

4.1.2.6.1. Stockage de l'information.

4.1.2.6.2. Protection locale.

4.1.2.6.3. Utilisation de client « virtual private network (réseau privé virtuel) ».

4.1.2.6.4. Dispositifs de chiffrement.

4.1.2.6.5. Journalisation des évènements.

4.1.2.6.6. Synchronisation.

4.1.3. Accès au terminal mobile (concerne la mobilité interne et la mobilité externe).

4.2. Règles organisationnelles.

4.2.1. Sécurité.

4.2.2. Mobilité interne.

4.2.3. Utilisation des applications en mode déconnecté.

4.2.4. Infrastructures d'accès à la mobilité externe.

4.2.5. Rationalisation des achats.

4.3. Règles sémantiques.

ANNEXE(S)

ANNEXE I. TABLEAU RÉCAPITULATIF DE L'APPLICABILITÉ DES RÈGLES PAR TYPE DE POSTE TERMINAL ET PAR TYPE DE MOBILITÉ.

ANNEXE II. GLOSSAIRE ET ACRONYMES.

ANNEXE III. RÉFÉRENCES.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit les règles du ministère de la défense relatives à l'accès des utilisateurs en situation de mobilité aux systèmes d'information sensibles non classifiés de défense du ministère, à partir de leur poste terminal mobile professionnel ou d'un terminal mis à disposition (1).

Cette directive s'inspire du CCI (2) et du RGI (2) prescrit par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives. Elle décline des orientations du plan stratégique des SIC PSSIC (2).

La directive DGSIC001 (2) sur le système de postes terminaux s'applique aux terminaux mobiles.

1.2. **Niveaux de préconisation.**

Les règles présentées dans ce document ont différents niveaux de préconisation et sont conformes au RGI (2) et à la RFC 2119 (2) :

- 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. **Champ et modalités d'application.**

Ces règles définissent la cible et sont applicables aux solutions de mobilité mises en œuvre au sein du ministère. La trajectoire pour rejoindre la cible, dans les trois ans à partir de la date de parution de la directive, reste de la responsabilité des organismes, ou de la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) pour les organismes dont les attributions correspondantes lui ont été confiées.

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 spécialisée (CMTSIC (3) ou CMSSI (3)) 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 direction générale des systèmes d'information et de communication (DGSIC) doit être demandé au préalable et joint au dossier.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

CCI - Recommandations nationales du cadre commun d'interopérabilité ;

RGI - Référentiel général d'interopérabilité ;

RGS - Référentiel général de sécurité (2) ;

DGSIC001 - Directive n° 8 définissant les règles à appliquer au système de postes terminaux ;

DGSIC002 - Directive n° 10 sur la prévention contre les codes malveillants ;

Directive n° 1223/SGDN/SSD du 23 décembre 2004 (4) relative à la protection physique des informations ou supports protégés ;

Instruction n° 900/DEF/CAB/DR du 18 juin 2007 (4) 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 (4) 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° 2003/DEF/DGSIC du 20 novembre 2008 portant code de bonne usage des systèmes d'information et de communication (SIC) du ministère de la défense ;

Recommandation n° 600/DISSI/SCSSI de mars 1993 (4) pour la protection des informations sensibles ne relevant pas du secret de défense. Recommandations pour les postes de travail informatiques ;

Recommandation n° 901/DISSI/SCSSI du 2 mars 1994 (4) pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

2.2. **Normes et standarts applicables.**

*2.2.1.* ***Définitions.***

RFC 2119 (2) - Mots-clés pour niveaux d'obligation.

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

Site DGSIC (2) - Site intranet défense DGSIC ;

CGAT (2) - Recommandations du CGAT (3) ;

DGSIC004 (2) - 137/DEF/DGSIC du 7 février 2008 - CMTSIC n° 6 ;

DGSIC005 (2) - 851/DEF/DGSIC du 1er octobre 2008 - CMTSIC n° 7.

3. DOMAINE COUVERT ET EMPLOI.

Cette directive a pour objet de définir les principes d'implémentation des solutions de mobilité au sein du ministère.

La mobilité consiste en l'utilisation des technologies de l'information pour permettre à un utilisateur de travailler depuis n'importe quel lieu. Il y a lieu de distinguer la mobilité interne ou l'itinérance qui se limite au périmètre physique des locaux du ministère en utilisant les réseaux internes du ministère, de la mobilité externe ou « nomadisme » qui est l'accès en dehors des locaux, réseaux, matériels et logiciels du ministère par un utilisateur du ministère *via* un opérateur extérieur à la défense.

Les règles de la politique de sécurité d'un système, sur la protection des biens physiques et de l'‘information, s'appliquent pour l'accès en situation de mobilité externe aux services offerts par ce système.

La directive DGSIC001 (2) définissant les règles à appliquer au « système de postes terminaux » identifie les règles techniques et organisationnelles s'appliquant sur les terminaux, qu'ils soient fixes ou mobiles. Elle définit quatre types de terminaux : parmi eux, le terminal de type 2 concerne les terminaux mobiles de type ordinateurs portables, ordiphones, tablettes PC,...

Ceux-ci sont divisés en deux catégories :

- type 2a : les ordinateurs portables, utilisés couramment sur le réseau du ministère, offrant à l'usager la possibilité de l'extraire du SI (3) 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, les tablettes PC (3), les ultra-portables ;

- type 2b : matériels mobiles dotés de fonctionnalités IP (3) de type PDA (3) communicants ou non, ordiphones (3), UMPC (3)...

### 3.1. **Services attendus du système.**

Le service de mobilité fourni aux utilisateurs doit leur permettre, en fonction des terminaux mobiles professionnels dont ils sont dotés, en fonction du lieu où ils sont, d'accéder à un certain nombre de services clairement répertoriés.

#### *3.1.1.* ***Les services accessibles.***

Les solutions déployées dans le cadre de la mobilité permettent, en situation de mobilité tant interne qu'externe, et dans la limite des capacités du poste terminal :

- S1 - l'accès à la messagerie intradef, à l'agenda, aux contacts, avec synchronisation des contacts et de l'agenda de l'intradef ;

- S2 - l'accès aux sites et applications web, et si possible applications métiers non wébisées de l'intradef ;

- S3 - l'accès aux données professionnelles de l'utilisateur accessibles par le réseau intradef (hors données sauvegardées localement sur les postes terminaux fixes) ;

- S4 - l'accès aux services autorisés de l'internet *via* l'intradef et l'accès aux services autorisés de l'intradef *via* internet ;

- S5 - la télé-administration et la télé-maintenance des systèmes ou équipements techniques ;

La télé-administration est le contrôle, la surveillance du système d'information et des postes terminaux effectués par un administrateur du ministère depuis un lieu distant (exemple : personnels d'astreinte).

La télé-maintenance est la maintenance d'un système par un technicien du ministère à distance, *via* un moyen de communication.

La télé-maintenance de matériels ou de composants par des sociétés tierces ne rentre pas dans le périmètre de la présente directive.

L'accès à des services différenciés sera fonction du terminal, voire du type d'accès (interne et externe) :

- l'utilisateur de terminaux mobiles de type 2b n'aura accès qu'à sa messagerie (y compris au contenu des pièces jointes de type image et bureautique, possibilité de suppression des mails sur le terminal sans les supprimer du serveur), ses contacts et son agenda, aux sites de l'intradef (5) (S1 et en partie S2), voire aux autres services dans la mesure du possible ;

- les utilisateurs de terminaux de type 2a pourront avoir accès, sous réserve des contraintes de sécurité, à tous les services (S1 à S5) en situation de mobilité interne et de mobilité externe.

| | TERMINAL PERSONNEL. | TERMINAUX PROFESSIONNELS. | | |
|---|---|---|---|---|
| | | TYPE 2A : SMARTPHONE, PDA COMMUNICANTS. | TYPE 2B : ORDONNATEUR. | |
| | | | MOBILITÉ INTERNE. | MOBILITÉ EXTERNE. |
| MESSAGE, AGENDA, CONTACT INTRADEF. | Interdit. | X | X | X |
| WEB INTRADEF. | Interdit. | si possible. | X | X |
| DONNÉES UTILISATEURS. | Interdit. | | X | X |
| SERVICES AUTORISÉS DE L'INTERNET. | Interdit. | si possible ; *via* intradef. | *via* intradef. | *via* intradef. |
| TÉLÉADMINISTRATION, TÉLÉMAINTENANCE. | Interdit. | | X | souhaitable. |

Le système déployé devra aussi permettre le télétravail (3) des utilisateurs et la télé-administration de certains systèmes par les administrateurs.

Il doit pouvoir permettre un accès depuis l'étranger, sous réserve d'être sous couverture des réseaux d'opérateurs de téléphonie mobile et de l'existence d'accords de roaming ou de disposer d'un accès à l'internet. Toutefois, certains pays filtrent volontairement les flux internet chiffrés, empêchant ainsi l'accès à l'intradef.

Le service d'accès à l'internet depuis l'intradef s'effectue au travers de passerelles d'interconnexion dédiées mises en place dans le cadre d'opérations ou de marchés spécifiques. Le service de mobilité permettant l'accès avec des terminaux mobiles à l'internet ou à l'échange de mail utilise ce service pré-cité, qui est indépendant des infrastructures mises en place au titre de la mobilité. Ces passerelles d'interconnexion spécifiques n'entrent pas dans le périmètre de la présente directive.

Le service d'accès à l'intradef depuis l'internet se fait au moyen de poste informatique particulier (poste multiniveau DR/NP (3)) et d'une passerelle d'interconnexion.

### *3.1.2.* ***Les profils d'utilisateurs.***

Plusieurs profils d'utilisateurs émergent des recensements effectués au sein du ministère par la DGSIC et l'EMA. Ces profils regroupent en trois familles tous les cas de mobilité, tant interne, qu'externe :

- décideurs, directeurs.

Ce profil concerne les hautes autorités du ministère (cabinet du ministre), de l'EMA, du SGA, de la DGA et

des entités qui leur sont subordonnées.

- fonctionnement organique :

  - chefs de grands services, d'entités organisationnelles, de projet (sont concernés les chefs de corps, commandant de base aérienne, commandant de bâtiment, chef de services de l'administration centrale, les sous-directeurs,...) ;

  - rédacteurs d'état-major et d'administration centrale ;

  - experts métiers (ressources humaines, informatique, ...) ;

  - utilisateurs amenés à travailler à domicile ;

- soutien :

  - personnels d'astreinte informatique ;

  - administrateurs assurant la télé-maintenance des systèmes ;

  - personnels assurant le soutien de proximité multi site.

*3.1.3.* ***Les typologies d'accès.***

Le service de mobilité interne est dit de type A.

Le service de mobilité externe peut offrir plusieurs types d'accès depuis l'extérieur du ministère :

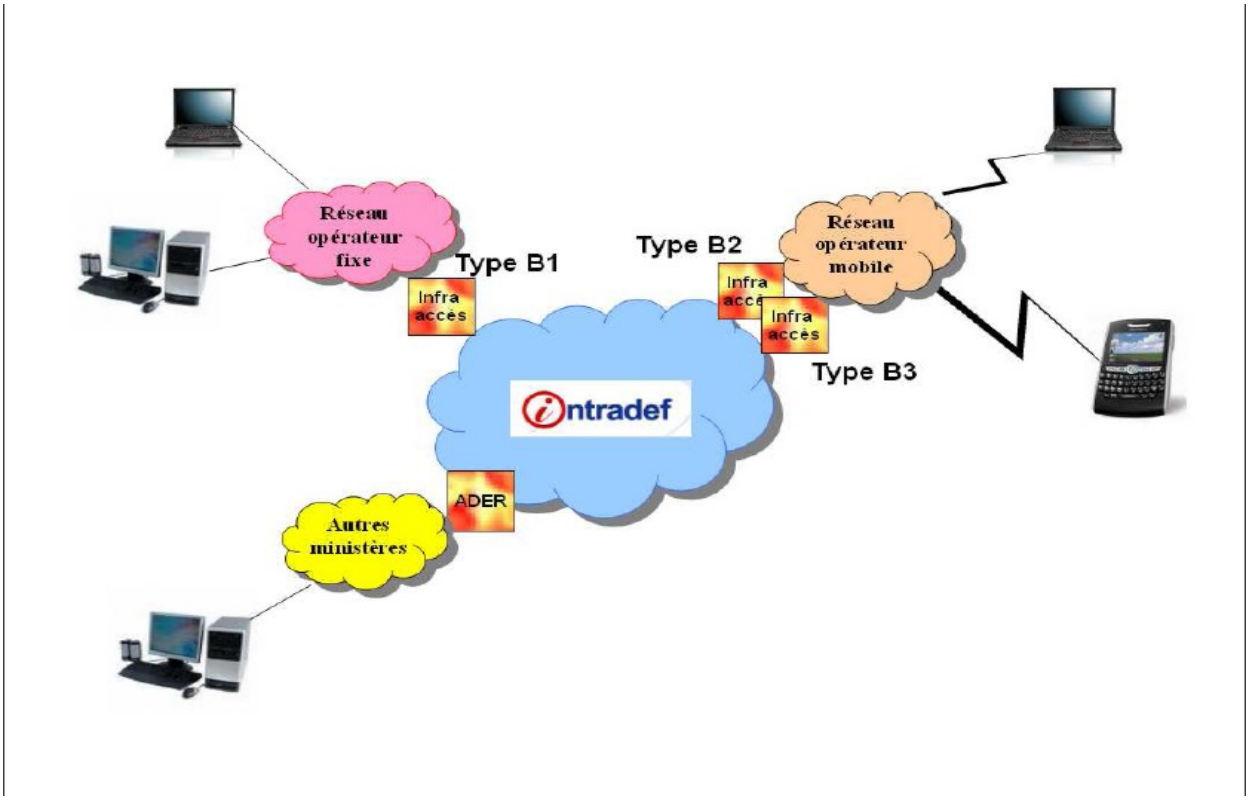
- Type B1 : accès filaire par un fournisseur d'accès internet (accès filaire) ;

- Type B2 : accès sans fil pour ordinateurs portables ;

- Type B3 : accès sans fil pour PDA (3) et ordiphones (3).

L'accès à l'intradef depuis l'extérieur du ministère, *via* des réseaux d'opérateurs de télécommunications fixes ou de téléphonie mobile s'effectue *via* des passerelles d'interconnexion maîtrisées sous la responsabilité de la DIRISI.

La présente directive s'applique au ministère de la défense et ne prévoit pas l'accès en situation de mobilité depuis un poste fixe d'un autre ministère : la passerelle ADER est hors périmètre de la présente directive.




Une ou plusieurs infrastructures d'accès pourront être déployées par type d'accès. La mutualisation des équipements des passerelles d'interconnexion devra être recherchée en respectant les exigences de sécurité et de disponibilité.

Les clés USB et dispositifs équivalents permettant le transport d'un environnement de travail complet (système d'exploitation, clients lourds, données utilisateurs, ...) ne seront pris en considération dans la présente directive que lorsque le processus d'évaluation auprès de l'ANSSI (3) sera terminé.

3.2. **Périmètre et limites.**

La présente directive comprend le périmètre suivant :

- pour la mobilité interne :
  - les briques de l'architecture de l'Intradef concernées par la mobilité ;
  - les terminaux mobiles (ordinateurs portables, ...) ;
- pour la mobilité externe :
  - les passerelles d'interconnexion mises en œuvre permettant aux terminaux mobiles de se connecter au système d'information du ministère ;
  - l'administration de ces passerelles d'accès ;
  - le canal (mais pas le support) de communication entre le terminal et la passerelle d'accès ;
  - les terminaux mobiles (ordinateurs portables, ordiphones,...).

Les réseaux accessibles en situation de mobilité externe sont des réseaux de niveau sensible non classifiés de défense au sens du point 6.3.3. de l'instruction ministérielle n° 900 (n.i. BO), notamment l'intradef. La présente directive ne s'applique pas aux réseaux classifiés.

- seule l'utilisation des terminaux professionnels fournis par le ministère est autorisée. L'utilisation de terminaux personnels pour se connecter aux réseaux sensibles est interdite.
L'usage d'un terminal personnel dans le cadre du télétravail ne sera autorisé que lorsque les mesures techniques et organisationnelles permettant cet usage dans des conditions de sécurité seront arrêtées et approuvées par l'autorité compétente.

- les connexions aux réseaux sensibles depuis un poste non maîtrisé par le ministère (exemple cybercafé) sont interdites.

- l'accès des implantations isolées du ministère à l'intradef (cas de certaines DMD (3), de certains CIRFA (3), des sémaphores, de certains bateaux, ...), *via* des réseaux non maîtrisés ne rentre pas dans le périmètre de la présente directive.

Conformément à l'IM900, le poste de travail mobile et ses supports protégés sont gérés comme des documents de même niveau de classification que de la documentation papier du niveau considéré.

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 technique.**

*4.1.1.* ***Règles techniques liées à la mobilité interne.***

RT MOBI1 : il est obligatoire que l'intradef permette la mobilité d'un utilisateur dans le réseau.

Lorsque la DIRISI proposera un service de mobilité interne à l'ensemble des organismes du ministère, les organismes désirant disposer de ce service devront le demander et identifier les sites sous leur responsabilité offrant cet accès (voir point 4.2.2. pour l'aspect organisationnel).

*4.1.2.* ***Règles techniques liées à la mobilité externe.***

*4.1.2.1. Administration.*

RT ADM1 : il est obligatoire d'administrer et de superviser les passerelles d'interconnexion.

RT ADM2 : il est recommandé que les terminaux de type 2 soient administrés par des mécanismes sécurisés au moyen d'un système d'administration centralisé installé dans une DMZ (3). À partir d'une console d'administration, le système doit permettre de déployer en mode OTA (3) (Over The Air) (6), des applications ou des paramètres à l'ensemble des terminaux mobiles concernés.

Le service d'administration des terminaux doit pouvoir supporter diverses plates-formes et proposer, dans la mesure des possibilités des terminaux, les fonctionnalités suivantes :

- inventaire des ressources matérielles et logicielles ;

- gestion des licences ;

- télédistribution de logiciels, de mises à jour ou de correctifs de sécurité ;

- télédistribution de règles de sécurité ;

- contrôle des règles de sécurité (contrôle d'accès, authentification, mots de passe) ;

- contrôle de la politique de sécurité mise en œuvre par les dispositifs de sécurité (VPN [3], pare-feu, antivirus, antimalware, antispam, etc.) ;

- effacement à distance des données utilisateur et remise à zéro constructeur en cas de perte ou de vol ;

- contrôle des applications (usage, accès, téléchargements, etc.) ;

- contrôle des ports de communications (infrarouge, Bluetooth, 3G, WiFi ou autre) ;

- contrôle d'usage des dispositifs tels que micro, caméra, webcam, appareil photo, et média amovible ;

- blocage des services et terminaux non autorisés ;

- chiffrement des communications entre le terminal et la passerelle d'interconnexion ;

- optimisation des communications (gestion des déconnexions, compression des flux, transferts intelligents, etc.) ;

- sauvegarde automatisée des données utilisateurs.

RT ADM3 : il est obligatoire que la console de supervision dispose d'une interface de supervision permettant de contrôler toute l'activité du (des) serveur(s) du service de mobilité externe et des connexions distantes (échecs d'authentification, anomalies, etc.). Elle doit être capable de visualiser de manière détaillée tous les évènements (système, session, sécurité...).

RT ADM4 : pour les terminaux de type 2a, il est obligatoire de mettre en place des mécanismes interdisant à l'utilisateur d'installer, d'exécuter (ou de faire exécuter) ou de supprimer des applications ou des logiciels du poste nomade qui lui a été attribué à moins que cette opération s'effectue sous le contrôle d'un administrateur du système.

RT ADM5 : pour les terminaux de type 2b, il est recommandé de mettre en place des mécanismes interdisant à l'utilisateur d'installer, d'exécuter (ou de faire exécuter) ou de supprimer des applications ou des logiciels du poste nomade qui lui a été attribué à moins que cette opération s'effectue sous le contrôle d'un administrateur du système.

RT ADM6 : il est obligatoire que le service de connexion à distance des terminaux mobiles soit configuré pour imposer que toute connexion internet passe par la plate-forme ad hoc du ministère de la défense ; cette règle ne s'applique pas lors de l'utilisation de postes homologués multi-niveaux.

RT ADM7 : il est obligatoire que le terminal de type 2a soit doté de la dernière version de la configuration logicielle de référence approuvée dans le cadre du concept d'emploi et de l'homologation du système de mobilité. Il doit être notamment doté :

- d'une fonction de chiffrement des données ayant fait l'objet d'une qualification au niveau standard, conformément aux exigences réglementaires applicables à la sensibilité des données traitées ou transmises ;

- d'un pare-feu ;

- d'un client VPN ;

- la connexion Bluetooth, Wifi, ou infrarouge du terminal mobile doit pouvoir être désactivée ;

- les fonctions « modem sans-fil » doivent être arrêtées ou désactivées lorsque les connexions sans-fil ne sont pas utilisées.

RT ADM8 : il est obligatoire que le terminal de type 2b soit doté de la dernière version du logiciel de sécurisation du terminal.

RT ADM9 : le partage de connexion physique entre deux réseaux (split tunneling) est interdit. Le terminal ne peut pas être connecté en même temps au réseau intradef et à un autre réseau informatique, sauf s'il existe un dispositif multi-niveaux autorisé.

*4.1.2.2. Sécurisation du canal de communication.*

RT CC1 : il est obligatoire que les équipements (terminal mobile et passerelle de chiffrement) aux extrémités du canal de communication s'authentifient mutuellement.

RT CC2 : il est obligatoire d'utiliser un tunnel chiffré afin de transporter l'information de façon sécurisée entre le terminal mobile et la passerelle d'interconnexion.

Le type d'algorithme et les longueurs de clef doivent être conformes à l'annexe B du RGS (2).

*4.1.2.3. Configuration des ports de communication.*

RT CPC : il est obligatoire de pouvoir contrôler les ports de communication des terminaux de type 2. Seuls les ports strictement nécessaires à la satisfaction des services doivent rester fonctionnels. Cette mesure vise à empêcher toute interconnexion accidentelle ou intentionnelle entre deux ou plusieurs réseaux.

*4.1.2.4. Cloisonnement des services.*

RT CS : il est recommandé de cloisonner les différents services applicatifs accessibles au niveau applicatif.

*4.1.2.5. Accès.*

4.1.2.5.1. Infrastructure d'accès au service.

RT IAS 1 : il est recommandé que l'infrastructure d'accès déployée permette les opérations d'administration à distance :

- effacement des données utilisateurs sur les terminaux de type 2b ;

- remise à zéro constructeur des terminaux de type 2b ;

- mise à jour de sécurité ;

- verrouillage et déverrouillage du poste.

RT IAS2 : il est obligatoire que l'ensemble des équipements bénéficient d'un maintien en configuration de sécurité (terminal, firmware du point d'accès,...).

4.1.2.5.2. Point d'accès dédié.

Un point d'accès est un équipement d'extrémité de réseau d'un opérateur de téléphonie mobile vers lequel sont routés les appels *data* (échange de données) des terminaux mobiles d'une société pour accéder au réseau de l'entreprise. Ce point d'accès peut être mutualisé avec d'autres entreprises ou être dédié à une seule entreprise.

RT PA1 : depuis l'extérieur du ministère, il est obligatoire d'accéder à l'infrastructure d'accès par un point d'accès dédié (APN (3) Acces Point Name) au ministère de la défense ;

RT PA2 : il est obligatoire de mettre en place une authentification forte pour s'authentifier au point d'accès.

4.1.2.5.3. Accès au réseau et systèmes d'information.

RT ARSO1 : un dispositif d'authentification forte (à deux facteurs) doit obligatoirement être mis en œuvre sur tout terminal mobile afin d'identifier et d'authentifier l'utilisateur avant toute connexion à un réseau du ministère de la défense. Aucune clé ou mot de passe stocké dans le terminal mobile ne doit être utilisé en tant qu'un des facteurs requis par le mécanisme d'authentification forte.

RT ARSO2 : il est obligatoire que l'authentification des utilisateurs soit effectuée à l'aide de certificats électroniques délivrés par l'IGC (3) en service au ministère.

RT ARSO3 : il est obligatoire que la connexion d'un utilisateur soit immédiatement routée vers la passerelle d'interconnexion adéquate du ministère de la défense.

RT ARSO4 : il est obligatoire que la politique de sécurité applicable soit vérifiée avant d'autoriser le poste terminal à se connecter au réseau et systèmes d'information du ministère (authentification forte de l'utilisateur, contrôle de conformité du poste, etc.).

Les paramètres de connexion ne doivent pas être modifiables par l'utilisateur. Si besoin, un choix pourra être proposé à l'utilisateur en fonction du type d'accès.

*4.1.2.6. Sécurité.*

4.1.2.6.1. Stockage de l'information.

RT SECU1 : en dehors des dispositifs de journalisation, tout stockage d'information transitant au sein de l'infrastructure d'accès est interdit.

4.1.2.6.2. Protection locale.

RT SECU2 : il est recommandé que des pare-feu matériels soient utilisés en coupure au sein de la passerelle d'interconnexion.

RT SECU3 : dans le cadre de la défense en profondeur, il est obligatoire que des dispositifs locaux de sécurisation soient mis en œuvre sur tout terminal mobile (type 2a et 2b).

4.1.2.6.3. Utilisation de client « virtual private network (réseau privé virtuel) ».

RT SECU4 : il est obligatoire que tout terminal mobile utilise un « client VPN » IPSEC qualifié au niveau standard (7) par l'ANSSI pour chiffrer tous les flux échangés avec le ministère de la défense.

4.1.2.6.4. Dispositifs de chiffrement.

RT SECU5 : il est obligatoire de doter les terminaux mobiles de dispositif de chiffrement de mémoire de masse qualifié au niveau standard.

RT SECU6 : il est obligatoire que les données stockées sur un terminal de type 2b soient chiffrées par ce dispositif.

4.1.2.6.5. Journalisation des évènements.

RT SECU7 : il est obligatoire de journaliser les événements des équipements de la passerelle d'interconnexion.

Une directive (à paraître) sur la gestion des traces précisera la typologie des évènements à journaliser.

4.1.2.6.6. Synchronisation.

RT SECU8 : il est obligatoire que tout terminal mobile doté de fonctionnalités de synchronisation (ex : ActiveSync, SyncML, etc.) respecte les exigences suivantes :

- mettre en œuvre une fonction de contrôle d'accès (ex : exiger l'entrée d'un mot de passe par l'utilisateur) ;

- désactiver toute connexion sans-fil lors des synchronisations au moyen d'un câble du terminal mobile avec un équipement du ministère de la défense.

*4.1.3.* ***Accès au terminal mobile (concerne la mobilité interne et la mobilité externe).***

RT ATM1 : tout terminal mobile (PC portable, PDA, ordiphone, etc.) doit obligatoirement être protégé par un code PIN (3) ou un mot de passe pour déverrouiller le système. En outre :

- le code PIN ou le mot de passe doit être systématiquement requis pour déverrouiller le terminal mobile et autoriser l'accès aux données et aux applications ;

- la protection par code PIN ou mot de passe doit être active en permanence.

RT ATM2 : le mécanisme de déverrouillage utilisé pour accéder à un terminal de type 2b doit obligatoirement respecter les exigences suivantes :

- un dispositif spécifique doit provoquer l'effacement sécurisé des données utilisateur et une remise à zéro constructeur du terminal ;

- le code de déverrouillage par défaut doit être changé.

RT ATM3 : il est obligatoire qu'un terminal mobile de type 2b dispose d'une fonction verrouillage de session après une période d'inactivité en fonction des exigences de la politique de sécurité applicable.

RT ATM 4 : Il est recommandé que la période d'inactivité d'un terminal mobile de type 2b soit fixée à 5 minutes.

4.2. **Règles organisationnelles.**

*4.2.1.* ***Sécurité.***

RO SECU1 : il est obligatoire que les solutions de mobilité déployées au sein du ministère utilisent des produits de sécurité (notamment le logiciel de sécurisation des terminaux mobiles de type 2b) qualifiés au niveau standard.

La liste des produits qualifiés, la démarche de qualification des produits sont disponibles en ligne sur le site www.ssi.gouv.fr.

RO SECU2 : il est obligatoire que les solutions de mobilité déployées au sein du ministère soient qualifiées au niveau standard (l'évaluation (8) du système comprendra la passerelle d'interconnexion et le moyen d'accès distant).

RO SECU3 : il est obligatoire que les solutions de mobilité déployées au sein du ministère fassent l'objet d'une procédure d'homologation du système composé de la passerelle d'interconnexion et du terminal mobile.

RO SECU4 : il est obligatoire que les solutions de mobilité fassent l'objet d'une évaluation des risques et d'une gestion continue des risques.

RO SECU5 : il est obligatoire que l'accès aux services autorisés de l'internet depuis un poste de type 2 (2a comme 2b) soit réalisé *via* une passerelle d'interconnexion homologuée. Cette règle ne s'applique pas lors de l'utilisation de postes multi-niveaux.

RO SECU6 : les solutions de mobilité externe doivent obligatoirement s'appuyer sur l'IGC en service sur le réseau intradef (pour la signature et l'authentification).

RO SECU7 : les numéros d'identification des terminaux mobiles (ex : numéro de la carte mère d'un PC portable, code IMEI (3) , adresse MAC (3) des cartes réseau, etc.) doivent obligatoirement être relevés, conservés et gérés par les autorités compétentes afin de faciliter la recherche des matériels volés.

RO SECU8 : il est obligatoire que la politique de sécurité détermine une durée limite/maximale d'absence de connexion au réseau pour les terminaux mobiles au-delà de laquelle le terminal devra être contrôlé par le service informatique de proximité avant reconnexion.

RO SECU9 : il est interdit aux utilisateurs de traiter des informations sensibles dans les SMS et MMS échangés à partir d'un terminal mobile de type 2b.

RO SECU10 : il est obligatoire de sensibiliser les personnels utilisant un service de mobilité externe.

La sensibilisation préalable à toute ouverture de droits à la mobilité comprendra notamment :

- un rappel du code de bon usage des systèmes d'information et de communication du ministère de la défense ;

- le rappel de la politique de sécurité, des PES et des conditions d'emploi du service de mobilité ;

- une présentation des menaces liées à l'utilisation d'un poste nomade, des attaques les plus courantes ;

- les réactions à tenir en cas de constatation d'un incident de sécurité.

RO SECU11 : Il est obligatoire qu'il y ait une politique de sécurité harmonisée du ministère relative à la gestion et l'utilisation des terminaux mobiles.

L'évaluation est conduite sous la responsabilité d'un ou de plusieurs centres d'évaluation agréés par l'ANSSI. Elle a lieu en vue de la qualification du système ou du produit.

#### *4.2.2.* ***Mobilité interne.***

L'ensemble des implantations du ministère n'accueille pas constamment des personnels de la défense extérieurs au site. Il est important de distinguer les états-majors ou directions, plus susceptibles d'accueillir des personnels d'organismes ou d'entités extérieurs que des régiments, des bases aériennes. Il s'agit de sélectionner les implantations sur lesquelles une infrastructure plus ou moins légère devra être mise en place pour permettre la mobilité interne.

L'accès en mobilité interne s'effectue à partir de son poste professionnel connecté sur le réseau local de l'organisme accueil ou par un poste d'accès contrôlé à partir de ses identifiants de connexion.

RO MOBI1 : il est obligatoire que chaque organisme identifie les implantations offrant un service de mobilité interne pour tout utilisateur bénéficiant du service de mobilité interne.

RO MOBI2 : pour chaque implantation, il est recommandé que les accès physiques au réseau soient privilégiés sur les lieux de passage fréquents des personnels extérieurs à l'entité (salle de réunion, un espace d'accueil, ...).

Ces lieux doivent faire l'objet d'une surveillance particulière (mesures organisationnelles ou techniques) visant à interdire l'accès aux personnels non autorisés.

RO MOBI3 : il est obligatoire que les points d'accès permettant la connexion d'un ordinateur professionnel en mobilité interne soient clairement identifiés.

RO MOBI4 : il est recommandé que les points d'accès permettant la connexion d'un ordinateur professionnel en mobilité interne soient identifiés de manière uniforme au sein du ministère. La DIRISI est chargée de définir le modèle.

RO MOBI5 : il est obligatoire d'offrir un service de mobilité interne au sein d'une implantation pour les utilisateurs affectés sur cette implantation (permettant par exemple l'accès depuis une salle de réunion).

#### *4.2.3.* ***Utilisation des applications en mode déconnecté.***

Le mode déconnecté permet l'utilisation hors connexion d'une application qui se synchronise lors de la reconnexion physique du poste terminal sur sa base de retour au bureau (par une synchronisation de base de données, *via* un formulaire,...).

RO DEC : dans le cadre de l'expression du besoin de chaque nouvelle application, il est obligatoire de stipuler si l'application doit ou non inclure la possibilité de travailler en mode déconnecté.

#### *4.2.4.* ***Infrastructures d'accès à la mobilité externe.***

RO ACC1 : pour un même type d'accès, il est recommandé que la ou les passerelles d'interconnexion soient basées sur la même architecture.

RO ACC2 : il est obligatoire que les passerelles d'interconnexion permanentes déployées pour le fonctionnement courant du ministère soient sous la responsabilité de l'opérateur ministériel DIRISI.

#### *4.2.5.* ***Rationalisation des achats.***

RO RAT1 : il est obligatoire de mettre en place une procédure d'achat centralisée des terminaux mobiles et des dispositifs amovibles de connexion (cartes 3G,...) conforme à la politique d'achat définie par la mission achat du ministère.

RO RAT2 : il est obligatoire que les organismes du ministère utilisent la procédure d'achat centralisée pour acquérir leurs terminaux.

RO RAT3 : pour les terminaux où le stockage de l'information n'est pas fait sur support amovible ou extractible, il est obligatoire d'acheter les terminaux mobiles de type ordiphones plutôt que de les louer.

RO RAT4 : pour les terminaux loués, il est obligatoire que la mémoire de masse reste la propriété de l'administration.

RO RAT5 : il est recommendé de privilégier l'utilisation de dispositifs amovibles de connexion maîtrisables par les applications de sécurité (de type PCMCIA, ExpressCard, clé USB...) plutôt que des dispositifs embarqués.

Cette règle vise à :

- rationaliser les dispositifs amovibles ;

- répondre à un cadencement différent du renouvellement des dispositifs de communications et des connectiques embarquées.

4.3. **Règles sémantiques.**

Sans objet.

Pour le ministre de la défense et par délégation :

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

Christian PÉNILLARD.

---

(1) Pour la mobilité interne (voir définition au point 3).

(2) Voir annexe III.

(3) Voir annexe II.

(4) n.i. BO.

(5) Sous réserve que le site ait été développé avec les technologies adéquates.

(6) Les terminaux se connectent par voie radio avec le serveur d'administration par GSM, 3G, WiFi,...

(7) La qualification au niveau standard est délivrée par l'ANSSI après évaluation du dispositif conformément à une cible de sécurité validée.

(8) Estimation de la sécurité d'un produit ou d'un système par rapport à des critères d'évaluation définis, annoncées dans la cible de sécurité.

ANNEXE I.

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

| | POSTE TYPE 2A BANALISÉ MOBILE QUI S'APPUIE SUR UN RÉSEAU FIXE MAÎTRISÉ (ORDINNATEUR PORTABLES, TABLETTES PC, ULTRAPORTABLES). | POSTE TYPE 2B BANALISÉ MOBILE QUI S'APPUIE SUR UN RÉSEAU FIXE MAÎTRISÉ (PDA, SMARTPHONE, UMPC). | MOBILITÉ INTERNE. | MOBILITÉ EXTERNE. |
|---|---|---|---|---|
| RT MOB1 | O | - | O | - |
| RT ADM1 | - | - | - | O |
| RT ADM2 | R | R | - | R |
| RT ADM3 | - | - | - | O |
| RT ADM4 | O | - | - | O |
| RT ADM5 | - | R | - | R |
| RT ADM6 | O | O | - | O |
| RT ADM7 | O | - | - | O |
| RT ADM8 | - | O | - | O |
| RT ADM9 | I | I | - | I |
| RT CC1 | O | O | - | O |
| RT CC2 | O | O | - | O |
| RT CPC | O | O | - | O |
| RT CS | R | R | - | R |
| RT IAS1 | - | - | - | R |
| RT IAS2 | O | O | - | O |
| RT PA1 | - | - | - | O |
| RT PA2 | O | O | - | O |
| RT ARSO1 | O | O | - | O |
| RT ARSO2 | O | O | - | O |
| RT ARSO3 | O | O | - | O |
| RT ARSO4 | O | O | - | O |
| RT SECU1 | - | - | - | I |
| RT SECU2 | - | - | - | R |
| RT SECU3 | O | O | - | O |
| RT SECU4 | O | O | - | O |
| RT SECU5 | O | O | - | O |
| RT SECU6 | - | O | - | O |
| RT SECU7 | - | - | - | O |
| RT SECU8 | O | O | - | O |
| RT ATM1 | O | O | O | O |
| RT ATM2 | - | O | - | O |
| RT ATM3 | - | O | - | O |
| RT ATM4 | - | O | - | O |
| RO SECU1 | O | O | O | O |
| RO SECU2 | O | O | O | O |
| RO SECU3 | O | O | O | O |
| RO SECU4 | O | O | O | O |

| | | | | |
|---|---|---|---|---|
| RO SECU5 | O | O | O | O |
| RO SECU6 | O | O | O | O |
| RO SECU7 | O | O | O | O |
| RO SECU8 | O | O | O | O |
| RO SECU9 | - | I | - | I |
| RO SECU10 | - | - | - | O |
| RO SECU11 | O | O | O | O |
| RO MOBI1 | - | - | O | - |
| RO MOBI2 | - | - | R | - |
| RO MOBI3 | - | - | O | - |
| RO MOBI4 | - | - | R | - |
| RO MOBI5 | - | - | O | - |
| RO DEC | - | - | - | O |
| RO ACC1 | - | - | - | R |
| RO ACC2 | - | - | - | O |
| RO RAT1 | O | O | - | O |
| RO RAT2 | O | O | O | O |
| RO RAT3 | - | O | - | O |
| RO RAT4 | O | O | O | O |
| RO RAT5 | R | - | - | R |

- : ne s'applique pas.

O : obligatoire.

R : recommandé.

D : déconseillé.

I : interdit.

ANNEXE II.

**GLOSSAIRE ET ACRONYMES.**

ANSSI : agence nationale de la sécurité des systèmes d'information.

APN : Acces Point Name (point d'accès dédié).

Application webisée : application utilisant un navigateur comme interface avec l'utilisateur.

Authentification : voir identification.

CGAT : cadre général d'architecture technique.

CIRFA : centre d'information et de recrutement des forces armées.

CMSSI : commission ministérielle de la sécurité des systèmes d'information.

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

DIRISI : direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense.

DMD : délégation militaire départementale.

DMZ : De Militarized Zone.

DR/NP : diffusion restreinte/non protégé.

Express Card : format de carte d'extension ultra plat destiné notamment aux ordinateurs portables plus récent que le format PCMCIA.

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).

IGC : infrastructure de gestion des clés.

IMEI : le code IMEI (International Mobile Equipment Identity), composé de 15 à 17 chiffres, est le numéro de série unique propre à tout mobile (téléphone, ordiphone, PDA). Ce code est affiché en tapant « *#06# » sur le clavier du téléphone. Le code IMEI sert à bloquer l'usage du téléphone sur tous les réseaux en cas de vol, ainsi

aucune carte SIM ne pourra être insérée.

IP : Internet Protocol.

MAC : Media Access Control est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison (couche 2 du modèle OSI).

MMS : Multimedia Messaging Service.

Ordiphone : terme français pour « 'smartphone*' ».

OTA : Over The Air. Technologie permettant l'accès, la mise à jour et la configuration à distance d'un terminal mobile par voie radio.

Passerelle d'interconnexion : dispositif mis en coupure entre deux réseaux ayant des architectures différentes ou des protocoles différents, ou offrant des services différents.

PC : Personal Computer.

PCMCIA : Personal Computer Memory Card International Association est un format de carte d'extension ultra plat destiné notamment aux ordinateurs portables.

PDA : Personal Digital Assistant : assistant personnel.

PIN : Personal Identification Number.

RFC : Request for comment.

RGI : référentiel général d'interopérabilité.

SI : système d'information .

Smartphone : téléphone mobile couplé à un assistant personnel.

SMS : Short Messaging Service.

Télétravail : le télétravail désigne toute forme d'organisation du travail dans laquelle un travail, qui aurait également pu être exécuté dans les locaux de l'employeur, est effectué par un salarié hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information dans le cadre d'un contrat de travail ou d'un avenant à celui-ci. Le contrat de travail ou son avenant précise les conditions de passage en télétravail et les conditions de retour à une exécution du contrat de travail sans télétravail. (Définition émanant de la proposition de loi pour faciliter le maintien et la création d'emploi du 9 juin 2009).

UMPC : Ultra Mobile Personal Computer.

VPN : Virtual Private Network (réseau privé virtuel).

Wi-Fi : Wireless Fidelity. Technologie permettant de relier sans fil plusieurs appareils informatiques standardisée par l'IEEE : norme 802.11.

ANNEXE III.

**RÉFÉRENCES.**

ORD : ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

RGI : référentiel général d'interopérabilité 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.

RGAA : référentiel général d'accessibilité des administrations défini par ordonnance [ORD] n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

RGS : référentiel général de sécurité défini par ordonnance [ORD] n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives. Décret n° 2010-112 du 2 février 2010 (1) paru au journal officiel n° 0029 du 4 février 2010.

DGSIC001 : directive n° 8/DEF/DGSIC du 29 juin 2009 définissant les règles à appliquer au système de postes terminaux, insérée au BOC n° 26 du 24 juillet 2009.

DGSIC002 : directive n° 10/DEF/DGSIC du 5 novembre 2009 sur la prévention contre les codes malveillants.

PSSIC : plan stratégique des systèmes d'information et de communication du ministère de la défense version 2 - lettre n° 749/DEF/DGSIC/SDS du 25 août 2008 (1).

CCI : recommandations nationales du cadre commun d'interopérabilité des systèmes d'information publics. Circulaires du premier ministre du 21 janvier 2002 et du 4 décembre 2002 ;

DGSIC004 : note n° 137/DEF/DGSIC du 7 février 2008 (1) - compte-rendu de la sixième commission ministérielle technique des systèmes d'information et de communication (CMTSIC).

DGSIC005 : note n° 851/DEF/DGSIC du 1er octobre 2008 (1)- compte-rendu de la septième commission ministérielle technique des systèmes d'information et de communication (CMTSIC).

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.

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

---

(1) n.i. BO.