Conforme à l'original produit,
Début du texte, page suivante.

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 3/DEF/DGSIC/SDAI définissant les règles de la messagerie électronique (1).

Du 8 janvier 2008

NOR D E F M 0 8 5 0 0 0 8 X

Références :

Ordonnance n° 2005-1516 du 8 décembre 2005 (JO n° 286 du 9 décembre 2005, texte n° 9 ; BOC, p. 8645. ; BOEM 120-0.3.1).
Décret n° 2006-497 du 2 mai 2006 (n.i. BO ; JO n° 103 du 3 mai 2006, texte n° 9 ; JO/135/2006. ; BOEM 160.1).

Pièce(s) Jointe(s) :

Six annexes.

Classement dans l'édition méthodique : BOEM 160.1.

Référence de publication : BOC N°06 du 15 février 2008, texte 1.

---

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La directive vise à définir des mécanismes permettant la mise en oeuvre d'une messagerie électronique.
Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.
Elle s'inspire du cadre commun d'interopérabilité [CCI] du 4 décembre 2002, du projet de [RGI] dans sa version provisoire V0.98 de juin 2007 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.
Elle décline la directive n°1/DEF/DGSIC du 17 octobre 2006 sur les logiciels [DGSIC001] du ministère de la défense.

1.2. **Niveaux de préconisation.**

Les règles définies 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.**

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure de projet de messagerie électronique mis en oeuvre sur un réseau utilisant le protocole IP* y compris les réseaux classifié de défense. Pour ces derniers, certaines préconisations seront adaptées pour tenir compte de la réglementation en matière de sécurité.
Les systèmes de messagerie électronique existant à la date de publication de la présente directive sont mis en conformité avec celle-ci dans un délai de trois ans à compter de cette date.
Les directions et services référencent la présente directive dans les cahiers des charges portant sur des marchés publics relatifs à la messagerie.

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

Elles sont instruites par la CMTSIC* et font l'objet d'une approbation par le directeur général de la DGSIC.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

[ORD] - Ordonnance n° 2005-1516 du 8 décembre 2005.
[CCI] - Cadre commun d'intéropérabilité.
[PRIS] - Politique de référencement intersectoriel de sécurité.
[DGSIC001] - Directive n° 1 sur les logiciels.
[DGSIC002] - Directive n° 2 sur les systèmes d'annuaire.
[DIRMESS] - Directives messagerie des armées et organismes interarmées.
[MOFI] - Messagerie officielle de l'intradef.

2.2. **Normes et standards applicables.**

2.2.1. ***Définitions.***

[RFC 2119] - Mots-clés pour niveaux d'obligation.

2.2.2. ***SMTP*.***

[RFC 2156] - Mime* internet X.400 enhanced relay.
[RFC 2821] - SMTP*.
[RFC 2822] - Internet message format.
[RFC 4409] - Message submission for mail.

2.2.3. ***ESMTP*.***

[RFC 1652] - SMTP* service extension for 8bit-MIME* transport.
[RFC 1870] - SMTP* service extension for message size declaration.
[RFC 2554] - SMTP* service extension for authentification.
[RFC 2920] - SMTP* service extension for command pipelining.
[RFC 3461] - SMTP* service extension for delivery status notifications (DSN*).
[RFC 3462] - The multipart/report content type for the reporting of mail system administrative messages.
[RFC 3463] - Enhanced mail system status code.
[RFC 3464] - An extensible message format for delivery status notifications.
[RFC 3798] - Message disposition notification.

[RFC 3885] - SMTP* service extension for message tracking.
[RFC 3886] - An extensible message format for message tracking responses.

2.2.4. ***POP*/IMAP*.***

[RFC1939] - POP*.
[RFC 2449] - POP* extension mechanism.
[RFC 2595] - Utilisation de TLS* avec POP3* et IMAP4*.
[RFC 3501] - IMAP*.

2.2.5. ***MIME*.***

[RFC 2045] - MIME* part one.
[RFC 2046] - MIME* part two.
[RFC 2047] - MIME* part three.
[RFC 2048] - MIME* part four.
[RFC 2049] - MIME* part five.

2.2.6. ***XSMTP*.***

[XSMTP].

2.2.7. ***S/MIME*.***

[RFC 2634] - Enhanced security services for S/MIME*.
[RFC 3370] - CMS algorithms.
[RFC 3850] - S/MIME* extensions.
[RFC 3851] - S/MIME* extensions.
[RFC 3852] - CMS.

2.2.8. ***SSL*/TLS*.***

[RFC 3207] - SMTP* service extension for secure SMTP* over TLS*.
[RFC 4346] - TLS*.
[RFC 4366] - TLS* extensions.

2.2.9. ***SASL*.***

[RFC 4422] - SASL*.

2.2.10. ***DKIM*.***

[RFC 4686] - DKIM* analyse of threats.
[RFC 4871] DKIM* signatures.
[DKIM] - Site du groupe de standardisation.

2.2.11. ***DIVERS.***

[RFC 3629] - UTF8*, a transformation format of ISO10646*.
[RFC 2428] - vCard*, MIME* directory profile.
[RFC 2560] - OCSP*.
[RFC3977] - NNTP*.
[RFC4287] - Atom* syndication format.

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Services attendus.**

La messagerie doit permettre l'envoi de courriel d'une personne agissant en son nom, au titre d'une délégation de pouvoir ou de signature à une ou plusieurs personnes ou machines.
L'émetteur du courriel doit pouvoir être identifié et authentifié, l'intégrité du courriel garantie et la non répudiation* à l'émission et à la réception assurée. La confidentialité des messages doit pouvoir être assurée.

3.2. **Périmètre et limites.**

Les règles définies ci-dessous autorisent la mise en oeuvre de la messagerie de niveau bas, moyenne voire haute telle que définie dans la directive messagerie de l'état-major des armées [DIRMESS].
Elles concernent la transmission de courriels de machine à machine, de machine à personne et de personne à personne ainsi que les mécanismes de sécurité afférents.
Cette directive couvre également l'interopérabilité avec les messagerie non SMTP*.
Les mécanismes concourant à l'élaboration d'un courriel (circuit visa), et ceux régissant la gestion du courrier (enregistrement, archivage et distribution) ne sont pas pris en compte.

3.3. **Interopérabilité avec les messageries non SMTP*.**

L'utilisation des extensions XSMTP* permet, au moyen de passerelle (automatique ou non), une interopérabilité entre les systèmes de messagerie au standard SMTP* et les systèmes de messagerie de type MUSE* ou MMHS* de l'OTAN*.

4. LES RÈGLES.

La directive est déclinée sous 3 angles : technique (RT), organisationnel (RO) et sémantique (RS) ; les règles sont numérotées séquentiellement par catégorie.

4.1. **Règles techniques.**

4.1.1. ***Transport.***

RT 01 : il est OBLIGATOIRE d'utiliser le protocole SMTP* pour l'échange de messages électroniques.
RT 02 : il est RECOMMANDÉ d'utiliser les extensions ESMTP* pour implémenter les fonctionnalités supplémentaires au protocole SMTP*.
RT 03 : il est OBLIGATOIRE d'être en mesure d'utiliser le protocole POP3* ou IMAP4* pour relever les messages électroniques déposés dans les boîtes aux lettres.
RT 04 : il est RECOMMANDÉ d'utiliser le protocole POP3* ou IMAP4* pour relever les messages électroniques contenus dans les boîtes aux lettres.
RT 05 : il est RECOMMANDÉ d'utiliser comme serveur de messagerie le MTA* PostFix.
RT 06 : il est OBLIGATOIRE que les MTA* exploitent l'extension XSMTP* relative à l'urgence afin de gérer la préemption et la priorité.
RT 07 : il est OBLIGATOIRE que le MTA* gère le support des notifications de statut de livraison (DSN*).

4.1.2. ***Formatage.***

RT 08 : il est OBLIGATOIRE d'utiliser le format MIME* pour la représentation des messages électroniques et des pièces jointes.
RT 09 : il est RECOMMANDÉ d'utiliser le format XSMTP* pour la gestion des entêtes militaires.

4.1.3. ***Sécurité.***

RT 10 : il est OBLIGATOIRE d'utiliser l'extension S/MIME* pour sécuriser les envois de messages électroniques.
RT 11 : il est RECOMMANDÉ d'utiliser les protocoles TLS* et SSL* pour sécuriser les échanges utilisant les protocoles HTTP*, SMTP*, IMAP* et POP*.

RT 12 : il est OBLIGATOIRE de renseigner le champ Sender* s'il diffère du champ From*.
RT 13 : il est OBLIGATOIRE de vérifier la cohérence au niveau du serveur SMTP* (MTA*) entre le « Mail From » et le « Sender* », et si le « Sender* » n'est pas positionné de vérifier la cohérence avec le « From ».
RT 14 : il est OBLIGATOIRE de mettre en oeuvre DKIM* pour sécuriser les entêtes et corps de message sur les réseaux de niveau non protégé ou diffusion restreinte en absence de solution alternative standardisée.
RT 15 : il est OBLIGATOIRE que le serveur de messagerie utilise l'heure et la date de référence du ministère.
RT 16 : il est OBLIGATOIRE que le client de messagerie utilise l'heure et la date de référence du ministère

4.1.4. ***Routage.***

RT 17 : il est OBLIGATOIRE de publier dans l'annuaire « LDAP* » du ministère de la défense les relais SMTP* (MTA*) capables de router les messages au plus près des boîtes aux lettres.
RT 18 : il est OBLIGATOIRE que les relais SMTP* (MTA*) soient en mesure d'utiliser les informations issues du système d'annuaires, au protocole « LDAP* », du ministère de la défense pour router les messages électroniques.

4.1.5. ***Nommage.***

RT 19 : il est OBLIGATOIRE de se conformer aux règles de gestion des homonymies définies dans la « Charte de nommage Internet » v1.2 du [CCI], règles rappelées en annexe.

4.1.6. ***Client de messagerie.***

RT 20 : il est RECOMMANDÉ d'utiliser le client de messagerie Mozilla Thunderbird.
RT 21 : il est OBLIGATOIRE d'utiliser un client de messagerie qui renseigne conformément à la norme les entêtes (« From », « To », « Subject », « Date », « Mime-Version », « Content-Type »).
RT 22 : il est RECOMMANDÉ d'utiliser l'encodage UTF8*.
RT 23 : il est OBLIGATOIRE que le client de messagerie supporte le protocole SMTP* pour l'envoi de message.
RT 24 : il est OBLIGATOIRE que le client de messagerie supporte les protocoles POP3*(S) et IMAP4*(S) pour relever les boîtes aux lettres.
RT 25 : il est OBLIGATOIRE que le client de messagerie supporte la consultation des listes de révocation de certificats électroniques* X509 via l'utilisation du protocole LDAP*.
RT 26 : il est OBLIGATOIRE que le client de messagerie supporte le protocole OCSP* pour la vérification de validité des certificats électronique*.
RT 27 : il est OBLIGATOIRE que le client de messagerie permette la consultation de plusieurs comptes de messagerie.
RT 28 : il est OBLIGATOIRE que le client de messagerie supporte l'encodage UTF8* et 8859-15.
RT 29 : il est OBLIGATOIRE que le client de messagerie autorise l'ajout d'attache de signature.
RT 30 : il est OBLIGATOIRE que le client de messagerie permette l'ajout de carte de visite au format vCard*.
RT 31 : il est OBLIGATOIRE que le client de messagerie dispose d'une fonction d'auto-complétion des adresses par interrogation d'un ou plusieurs annuaires LDAP*.
RT 32 : il est RECOMMANDÉ que le client de messagerie supporte le protocole NNTP*.
RT 33 : il est OBLIGATOIRE que le client de messagerie dispose d'une fonction de notification de message supprimé sans être lu. Cette notification est à destination de l'émetteur. La fonction doit pouvoir être désactivée.
RT 34 : il est RECOMMANDÉ que le client de messagerie supporte le protocole Atom* de syndication de contenu.
RT 35 : il est OBLIGATOIRE que le client de messagerie gère les demandes de notification de statut de livraison (DSN*).

4.2. **Règles organisationnelles.**

4.2.1. ***Adressage.***

RO 01 : Il est OBLIGATOIRE que toute personne disposant d'une boîte aux lettres sur les systèmes d'information du ministère de la défense dispose d'un alias de la forme *prénomX.nom@nom_de_domaine* X correspondant aux caractères supplémentaires permettant de gérer l'homonymie conformément à la charte définie par la règle RT 19, sauf application des règles RO 02 et RO 04.
RO 02 : il est OBLIGATOIRE que toute personne n'appartenant pas à un ministère français et travaillant sur les systèmes d'information du ministère de la défense dispose d'une adresse de la forme de celle des personnels du ministère de la défense (RO 01) complétée d'un signe distinctif unique « *.ext* » soit une adresse de la forme *prénomX.nom.ext@nom_de_domaine*.
RO 03 : il est OBLIGATOIRE d'utiliser le nom d'usage stocké dans le système d'annuaire du ministère de la défense pour l'adresse de messagerie personnelle.
RO 04 : il est RECOMMANDÉ que les personnes dont la mission requiert l'anonymat soient dotées d'une identité artificielle attribuée par leur organisme de rattachement et permettant de leur affecter une adresse personnelle conforme aux règles techniques précédentes, ainsi qu'un identifiant de connexion.
RO 05 : il est RECOMMANDÉ que les adresses d'organisme soient de la forme : *Organisme@Organisme.nom_de_domaine*. La définition du champ Organisme est donnée en annexe.
RO 06 : il est RECOMMANDÉ que les adresses d'autorité ou organisationnelle soient de la forme : *Structure_organisationnelle(-Lieu)(+Dossier)@Organisme.nom_de_domaine*. La définition des champs Structure_organisationnelle, lieu (optionnel) et dossier (optionnel) est donnée en annexe.
RO 07 : il est RECOMMANDÉ que les adresses fonctionnelles soient de la forme : *Fonction.Structure_organisationnelle(-lieu)(+dossier)@Organisme.nom_de_domaine* et Fonction.Organisme@Organi
La définition des champs Fonction, Structure_organisationnelle, lieu (optionnel) et dossier (optionnel) est donnée en annexe.

Nota : le champ *nom_de_domaine* correspond à *defense.gouv.fr* pour l'intranet défense sensible. Les règles RO 01 à 07 s'appliquent aux réseaux classifiés en utilisant à la place de *nom de domaine* l'intitulé du domaine défini pour le réseau concerné.

4.2.2. ***Identité.***

RO 08 : il est OBLIGATOIRE de construire l'identifiant unique à partir des éléments constituant l'adresse de messagerie INTRADEF. La partie *prénomX.nom* constitue la base de cet identifiant (*prénomX.nom.ext* pour les extérieurs).
RO 09 : il est OBLIGATOIRE que l'identifiant de connexion (« login ») corresponde à la partie gauche de l'adresse de messagerie : *prénomX.nom* ou *prénomX.nom.ext* pour les extérieurs.

4.2.3. ***Sécurité.***

RO 10 : il est INTERDIT de faire circuler en clair les mots de passe d'authentification*.
RO 11 : il est OBLIGATOIRE de s'identifier et s'authentifier* avec son identité personnelle (identifiant/mot de passe ou certificat) pour envoyer des messages électroniques.
RO 12 : il est OBLIGATOIRE de s'identifier et s'authentifier* avec son identité personnelle (identifiant/mot de passe ou certificat) pour accéder aux boîtes aux lettres sur lesquelles on possède des droits.
RO 13 : il est RECOMMANDÉ de signer avec un certificat personnel que l'on agisse en son nom, ou au titre d'une délégation de pouvoir ou de signature.
RO 14 : il est RECOMMANDÉ de s'authentifier* au moyen d'un certificat électronique délivré par une infrastructure de gestion des clefs cautionnée par le ministère de la défense.

4.3. **Règles sémantiques.**

Sans objet.

Pour le ministre de la défense et par délégation :

L'ingénieur général des télécommunications,
directeur général des systèmes d'information et de communication,

Henri SERRES.

---

(1) Approuvée par note n° 9/DEF/DGSIC/SDAI en date du 8 janvier 2008.

ANNEXE I.

GLOSSAIRE ET ACRONYMES*.

ASCII : american standard code for information interchange : norme utilisée pour le codage de caractères. Elle consiste à coder un caractère sur un seul octet.

Atom : atom syndication format est un format de document basé sur XML conçu pour la syndication de contenu périodique.

Authentification/identification : 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 reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

Autorité de Certification (AC) : au sein d'un prestataire de services de certification électronique (PSCE), une autorité de certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification.

Certificat électronique : fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification*. En signant le certificat, l'AC* valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat électronique de signature : certificat disposant des caractéristiques nécessaires à la réalisation d'une signature électronique. Son utilisation permet d'assurer l'intégrité du document signé, la non répudiation à l'émission du document et l'authentification du signataire du document.

Certificat électronique de chiffrement : certificat disposant des caractéristiques nécessaires pour chiffrer un document. Son utilisation permet de garantir un droit d'en connaître de l'information chiffrée. Et de s'assurer de la non répudiation à la réception dans le cas de l'émission en automatique d'un accusé de réception.

Certificat électronique d'authentification : certificat disposant des caractéristiques nécessaires à la réalisation d'une authentification. Son utilisation permet de réaliser une identification et une authentification forte de son détenteur.

CMTSIC : commission ministérielle technique des SIC. Commission ministérielle spécialisée instaurée par l'arrêté DEFD0600690A du 6 juin 2006.

CSIAG : commission des systèmes d'information d'administration et de gestion, régie par l'arrêté du 6 juin 2006 portant création et organisation d'instances relatives aux systèmes d'information et de communication du ministère de la défense.

CSIOC : commission des systèmes d'information opérationnels et de communication, régie par l'arrêté du 6 juin 2006 portant création et organisation d'instances relatives aux systèmes d'information et de communication du ministère de la défense.

DKIM : domain keys identified mail, permet de sécuriser les entêtes du message, ainsi que le corps de celui-ci en réalisant une opération cryptographique s'appuyant sur des certificats X509 et le DNS. Pensée pour lutter contre le pourriel, ce protocole permet de vérifier simplement l'intégrité des entêtes et du corps du message.

DSN : delivery status notification : notification d'état de remise.

ESMTP : extended SMTP est la définition de protocoles d'extension à SMTP*.

From : champ du message qui contient l'identité de l'expéditeur (la personne qui a souhaité que le message soit envoyé) placée par le MUA* de l'émetteur.

GS : groupe de standardisation. Instance de gouvernance technique placée sous l'égide de la CMTSIC*.

HTTP : hypertext transfer protocol, protocole utilisé par un butineur (navigateur Web) pour accéder à un serveur Web.

IETF : internet engineering task force : groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour l'Internet. Produit les RFC.*

IGC : infrastructure de gestion de clefs. Elle permet la délivrance de certificats électroniques et offre la confiance nécessaire pour l'usage des certificats électroniques.

IMAP : internet message access protocol Version 4, c'est un protocole utilisé pour récupérer les messages sur le serveur de messagerie. Il permet de conserver ses messages sur le serveur et offre des fonctionnalités avancées comme les boîtes aux lettres multiples, la possibilité de créer des dossiers pour trier ses courriels.

Intranet : utilisation des technologies de l'Internet à des fins internes à une entreprise. L'Intranet permet de bénéficier de l'économie d'échelle acquise par les logiciels sur l'Internet et d'outils de développement orientés objet. On peut réaliser maintenant sur l'Intranet la totalité des applications métiers et services communs. L'Intranet nécessite une administration soigneuse des droits d'accès.

Interopérabilité technique : l'interopérabilité des services correspond à la possibilité de fonctionner indifféremment sur des réseaux différents. En informatique, l'interopérabilité signifie l'aptitude de deux ou plusieurs systèmes (logiciels ou matériels) à fonctionner ensemble en utilisant des standards communs.

ISO : international organization standardization, organisation non gouvernementale qui constitue un réseau d'instituts nationaux de normalisation de 157 pays, selon le principe d'un membre par pays.

ISO/CEI 10646:2003 : normalise le jeu universel de caractères codés sur plusieurs octets. Elle s'applique à la représentation, à la transmission, à l'échange, au traitement, au stockage, à la saisie et à la présentation des langues du monde sous forme écrite et de symboles complémentaires.

IP : internet protocol : protocole de communication correspondant globalement au niveau 3 du modèle OSI. Protocole utilisé par le réseau Internet et sur les réseaux intranet et extranet.

LDAP : (lightweight directory access protocol). Protocole permettant l'accès des annuaires. LDAP est initialement un frontal d'accès à des bases d'annuaires respectant la norme X.500 édictée par l'UIT. Il est devenu un annuaire natif (standalone LDAP) utilisant sa propre base de données, sous l'impulsion d'une équipe de l'université du Michigan. DAP est un protocole défini à l'IETF* pour simplifier l'accès (consultation, modification) aux annuaires supportant les modèles d'information X.500, pour favoriser les implémentations et l'usage des annuaires. Sa version courante est LDAP* v3, définie dans la [RFC 4510]. LDAP* définit un protocole réseau pour accéder à l'information contenue dans l'annuaire, un modèle d'information définissant la forme et le type de l'information contenue dans l'annuaire, un espace de nommage définissant comment l'information est organisée et référencée, un modèle fonctionnel définissant comment on accède et met à jour l'information, un modèle de distribution permettant de répartir les données (à partir de la v3), un protocole et un modèle de données extensible, des API pour développer des applications clientes.

MMHS : military message handling system : messagerie militaire de l'OTAN*.

MTA : mail transfert agent, c'est le service qui s'occupe de l'acheminement des messages. Il utilise le protocole SMTP*. C'est le service postal et ses centres de tri.

MDA : mail delivery agent, c'est le programme qui transmet le courrier du serveur (MTA*) au client (MUA*). C'est le facteur qui dépose le courrier dans votre boîte aux lettres.

MUA : mail user agent, c'est le programme qui tourne sur le poste client et permet de lire, écrire et consulter ses messages. Il communique avec le MTA* pour l'envoi des messages et le MDA* pour la récupération des messages. C'est lui qui récupère votre courrier dans la boîte aux lettres.

MIME : multipurpose internet mail extension est un format de données permettant d'introduire dans les messages SMTP* différents types de fichiers multimédias.

MUSE : messagerie universelle sécurisée, système de messagerie permettant l'échange d'information de niveau confidentiel de défense dans un environnement sécurisé offrant un haut niveau de disponibilité.

Non répudiation : impossibilité pour un utilisateur de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'information (imputabilité) que sur son contenu (intégrité).

NNTP : network news transfert protocol : protocole de « news » ou forums.

OCSP : online certificate status srotocol est un service de vérification de la validité d'un certificat*.

OTAN : organisation du traité de l'Atlantique Nord.

POP : post office protocol version 3, c'est le protocole qui permet de récupérer les messages sur le serveur de messagerie.

RFC : request for comment : série de documents et normes concernant l'Internet. Peu de RFC sont des standards mais tous les standards de l'Internet sont enregistrés en tant que RFC.

SASL : simple authentication and security layer, c'est une couche de sécurité permettant de découpler les mécanismes d'authentification de n'importe quel protocole d'application. Les protocoles supportant SASL sont IMAP*, LDAP*, POP*, SMTP* et XMPP*.

Sender : champ de l'entête du message qui contient l'identité de l'expéditeur réel. Ce champ n'est utile que s'il diffère du From*, c'est le cas lorsque le From* est par exemple une adresse organisationnelle, dans ce cas le champ Sender* contient l'adresse de l'expéditeur réel.

S/MIME : secure/multipurpose internet mail extension est un standard pour le chiffrement et la signature à clef publique de courriel encapsulé dans MIME*.

SMTP : simple mail transfer protocol, c'est un protocole de communication utilisé pour transférer les messages vers le serveur de messagerie (MTA*), entre serveurs de messagerie (MTA*).

SSL : secure sockets layer : prédécesseur de TLS*.

TLS : transport layer security, norme de sécurisation du transport de l'information. Elle offre des mécanismes d'authentification du serveur, du client en option, ainsi que des mécanismes d'intégrité et de confidentialité du transport. Nécessite l'utilisation de certificats électroniques d'authentification de type X509V3.

UCS : universal character set, jeu de caractères abstraits définis par la norme ISO/CEI 10646*.

UNICODE : norme développée par le consortium unicode qui vise à donner à tout caractère de n'importe quel système d'écriture de langue un nom et un identifiant numérique, et ce de manière unifiée, quelle que soit la plate-forme informatique ou le logiciel. La norme ISO/CEI 10646:2003* est un sous-ensemble d'UNICODE.

UTF8 : UCS* transformation format 8 bits, format de codage de caractères défini pour les caractères UNICODE*. Chaque caractère est codé sur une suite d'un à quatre octets. UTF8* a été conçu pour être compatible avec certains logiciels originellement prévus pour traiter des caractères sur un seul octet (ASCII*).

vCard : est un format standard d'échange de données personnelles (visit card soit carte de visite).

Web Mail : interface WEB permettant l'émission, la consultation et la manipulation de courriers électroniques directement à partir d'un butineur.

XMPP : extensible messaging and presence protocol, c'est un protocole de messagerie instantannée.

XSMTP : format définissant les entêtes permettant de véhiculer des informations militaires dans des messages SMTP afin de répondre aux différents besoins d'interopérabilité : ACP127, MUSE*, Messagerie OTAN*.

ANNEXE II.
RÉFÉRENCES.

[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 (n.i.BO).
[CMTSIC] - Commission ministérielle des SIC : arrêté du 6 juin 2006 portant création et organisation d'instances relatives aux systèmes d'information et de communication du ministère de la défense.
[DGSIC001] - Directive sur les logiciels n° 1/DEF/DGSIC du 17 octobre 2006.
[DGSIC002] - Directive système d'annuaire n° 2/DEF/DGSIC du 9 mars 2007.
[DIRMESS] - Directives générales en matière de messagerie des armées et organismes interarmées. Note n°1620/DEF/EMA/PI/SI/NP du 26 juin 2006 (n.i.BO).
[DKIM] - Le groupe de travail de l'IETF* relatif à DKIM* : www.dkim.org/ietf-dkim.htm.
[MOFI] - Messagerie officielle de l'intradef et guide de mise en oeuvre de la messagerie officielle de l'intradef. Note n°3789/DEF/EMA/EPI/SI/NP du 18 décembre 2006 (n.i.BO).
[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.
[PRIS] - Politique de référencement intersectoriel de sécurité v2.1 du 6 novembre 2006 (ADAE et DCSSI).
[RFC1652] - SMTP service extension for 8bit-MIME transport (Draft Standard 07/1994).
[RFC1870] - SMTP service extension for message size declaration (Standard 11/1995).
[RFC1939] - Post office protocol version 3 (Standard 05/1996).
[RFC2045] - Multipurpose internet mail extensions (MIME) : format of internet message bodies (draft standard 11/1996).
[RFC2046] - Multipurpose internet mail extensions (MIME) : media types (Draft Standard 11/1996).
[RFC2047] - Multipurpose internet mail extensions (MIME) : message header extensions for Non-ASCII Text (draft standard 11/1996).
[RFC2048] - Multipurpose internet mail extensions (MIME) : registration procedures (best current practice 11/1996).
[RFC2049] - Multipurpose internet mail extensions (MIME) : conformance criteria and examples (draft standard 11/1996).
[RFC2119] - Key words for use in RFCs to indicate requirement levels (Best Current Practice 03/1997).
RFC2156] - MIXER (mime internet X.400 enhanced relay): mapping between X.400 and RFC 822/MIME (proposed standard 01/1998).
[RFC2428] - vCard, MIME directory profile (proposed standard Sept 1998).
[RFC2449] - POP extension mechanism (proposed standard 11/1998).
[RFC2554] - SMTP service extension for authentication (proposed standard 03/1999).
[RFC2560] - X509 intranet public key infrastructure online certificate status protocol (proposed standard 06/99).
[RFC2595] - Using TLS with IMAP, POP3 and ACAP (proposed standard 06/1999).
[RFC2634] - Enhanced security services for S/MIME (proposed standard 06/1999).
[RFC2821] - Simple mail transfer protocol (proposed standard 04/2001).
[RFC2822] - Internet message format (proposed standard 04/2001).
[RFC2920] - SMTP service extension for command pipelining (standard 09/2000).
[RFC3207] - SMTP service extension for secure SMTP over TLS (proposed standard 02/2002).
[RFC3370] - Cryptographic message syntax (CMS) algorithms (proposed standard 08/2002).
[RFC3461] - SMTP service extension for delivery status notifications (draft standard 01/2003).
[RFC3462] - The multipart/report content type for the reporting of mail system administrative messages (draft standard 01/2003).
[RFC3463] - Enhanced mail system status code (draft standard 01/2003).
[RFC3464] - An extensible message format for delivery status notifications (Draft Standard 01/2003).[RFC3501] - Internet message access protocol version 4 revision 1 (proposed standard 03/2003).
[RFC3629] - UTF8, a transformation format of ISO* 10646 (standard 11/2003).
[RFC3798] - Message disposition notification (draft standard 05/2004).
[RFC3850] - Secure/multipurpose internet mail extensions (S/MIME) Version 3.1 certificate handling (proposed standard 007/2004).
[RFC3851] - Secure/multipurpose internet mail extensions (S/MIME) version 3.1 message specification

(proposed standard 07/2004).
[RFC3852] - Cryptographic message syntax (CMS) (proposed standard 07/2004).
[RFC3885] - SMTP service extension for message tracking (proposed standard 09/2004).
[RFC3886] - An extensible message format for message tracking responses (proposed standard 09/ 2004).
[RFC3977] - Network news transfert protocol (proposed standard 10/2006).
[RFC4287] - Atom syndication format (proposed standard 12/2005).
[RFC4346] - The transport layer security (TLS) protocol V1.1 (proposed standard 04/2006).
[RFC4366] - Transport layer security (TLS) extensions (proposed standard 04/2006).
[RFC4409] - Message submission for mail (draft standard 04/2006).
[RFC4422] - Simple authentication ans security layer (SASL) (proposed standard 06/2006).
[RFC4686] - Analysis of threats motivating domainkeys identified mail (informationnal 09/2006).
[RFC4871] - Domainkeys identified mail signatures (proposed standard 05/2007).
[RGI] - Référentiel général d'interopérabilité, dans sa version V0.98 de juin 2007, défini par 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.
[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.
[XSMTP] - Recommandation du format XSMTP n°2005/101978/CELAR/ASC/Ap/03875/NC - version 1.1 du 24 juin 2005 disponible à l'adresse www.milimail.org.

ANNEXE III.

RÈGLES DE GESTION DES HOMONYMIES ISSUES DU CADRE COMMUN D'INTEROPÉRABILITÉ.

La forme canonique prenom.nom@nom-de-domaine doit être utilisée.

Les homonymies sont réglées par l'insertion des initiales des prénoms suivants, selon besoin. Ces initiales sont séparées du prénom usuel par un tiret. Cette forme est jugée plus simple que l'habitude anglo-saxonne de séparer les initiales par un point. En cas d'homonymie parfaite entre deux agents, un numéro séquentiel est accolé au(x) prénom(x) en fonction de l'ordre de recensement de ces homonymes. Par exemple :

Pierre.Durand pour Pierre Durand, premier enregistré,
Pierre-m.Durand pour Pierre Michel Durand, seconde occurrence du nom,
Pierre-mj.Durand pour Pierre Marie Joseph Durand, troisième occurrence du nom,
Pierre-mj1.Durand pour le premier agent enregistré en cas d'homonymie parfaite,
Pierre-mj2.Durand pour le second agent enregistré en cas d'homonymie parfaite,
Pierre-mj3.Durand pour le troisième agent enregistré en cas d'homonymie parfaite.

Les prénoms et noms composés sont écrits en entier et raccordés par des tirets, par exemple : Louis.Leprince-Ringuet pour Louis Leprince-Ringuet.

Les blancs sont remplacés par un tiret "-", par exemple : Andre.Dunoyer-de-Segonzac pour André Dunoyer de Segonzac.

Les apostrophes sont conservées, par exemple : Marie-Ange-L'helgouarc'h pour Marie-Ange l'Helgouarc'h.

Les particules suivent l'ordre normal d'élocution, et non la forme littéraire Jean-Marie.de-Lattre-de-Tassigny pour Jean-Marie de Lattre de Tassigny.

ANNEXE IV.

RÈGLES D'ÉLABORATION DES ADRESSES D'ORGANISMES.

1. FORME DES ADRESSES D'ORGANISMES.

Organisme@Organisme.nom_de_domaine

Une adresse de ce type représente à la fois l'organisme dans sa globalité et l'autorité représentant l'organisme.

2. DÉFINITION DU CHAMP ORGANISME.

Les valeurs prises par le champ Organisme sont uniques au sein du ministère et sont identiques à celles utilisées dans le système d'annuaire du ministère de la défense pour décrire la structure organisationnelle du ministère.

Les structures disposant d'une adresse d'organisme sont :

- le ministère : valeur *min*
  ex : *min@min.defense.gouv.fr* (écrire au ministre, au ministère)

- les organismes (ex : air, terre, mer, gendarmerie, DGA, SGA, interarmees, etc.) ;

  ex : *terre@terre.defense.gouv.fr* (écrire à l'armée de terre)

- les états-majors (ex : ema, emaa, emm, etc.) ;

  ex : *ema@ema.defense.gouv.fr* (écrire à l'EMA)

- les directions (ex : DAS, DAJ, DCMAT, DPMM, DGGN, etc.) ;

  ex : *cab@cab.defense.gouv.fr* (écrire au cabinet du ministre)
  ex : *das@das.defense.gouv.fr* (écrire à la délégation aux affaires stratégiques)ex : *drhaa@drhaa.defense.gouv.fr* (écrire à la direction des ressources humaines de l'armée de l'air)
  ex : *dsa@dsa.defense.gouv.fr* (écrire à la direction des systèmes d'armes)
  ex : *daf@daf.defense.gouv.fr* (écrire à la direction des affaires financières)
  ex : *drm@drm.defense.gouv.fr* (écrire à la direction du renseignement militaire)

- les services (ex : SIMMAD, santé, essences, SMG, etc.) ;

  ex : *sante@sante.defense.gouv.fr* (écrire au service de santé)

- les commandements organiques et opérationnels (ex : FAN, CASSIC, COFAT, RT, etc.) ;

  ex : *fan@fan.defense.gouv.fr* (écrire à la force d'action navale)
  ex : *cofat@cofat.defense.gouv.fr* (écrire au COFAT)

- les exercices ou opérations extérieures (ex : EPERVIER, etc.)

  ex : *epervier@epervier.defensecdd* (écrire à l'opération EPERVIER)

3. REMARQUE.

Le responsable de l'organisme définit la ou les personnes pouvant accéder à la boîte aux lettres de cet organisme.

Les labels sont fournis par le système d'annuaire du ministère de la défense. Ceux présentés ci-dessus sont cités à titre d'exemple.

ANNEXE V.

RÈGLES D'ÉLABORATION DES ADRESSES ORGANISATIONNELLES.

1. FORME DES ADRESSES ORGANISATIONNELLES.

Structure_organisationnelle(-Lieu)(+Dossier)@Organisme.nom_de_domaine

Une adresse de ce type représente à la fois une structure dans sa globalité et l'autorité la représentant.

2. DÉFINITION DES DIFFÉRENTS CHAMPS.

Toutes les valeurs prises par les champs Entité, Niv-1, Niv-2, Niv-3 et Lieu constituant le champ Structure_organisationnelle sont identiques à celles utilisées dans le système d'annuaire du ministère de la défense pour décrire la structure organisationnelle de l'entité.

2.1. **Le champ Organisme.**

Il suit les mêmes règles que pour la constitution des adresses d'organismes (cf annexe précédente)

2.2. **Le champ Structure organisationnelle.**

Ce champ a une forme similaire à celle d'un timbre de note ou d'une adresse ACP127 expurgé d'éléments superflus.

Il est de la forme *Entité « tiret »(Niv-1) « tiret »(Niv-2) « tiret »(Niv-3)* avec :

- le champ *Entité* qui correspond :

  - pour les organismes de type états-majors , directions, services, régions, exercices ou opération extérieurs, commandement organiques et opérationnels, à un ensemble de niveau -1 dans l'organigramme hiérarchique de l'organisme ;

    ex : *bemp@ema.defense.gouv.fr* (écrire au bureau emploi de l'EMA)
    ex : *bemp@rtnord.defense.gouv.fr* (écrire au bureau emploi de la région terre nord)
    ex : *bemp@fan.defense.gouv.fr* (écrire au bureau emploi de la force d'action navale)

  - aux unités et centres dans les autres cas (ex ESIC, 41RT, Mistral, CELAR..). L'organisme utilisé dans l'adresse est l'organisme hiérarchique de plus haut niveau (Air, DGA, Interarmées, Marine, SGA, Terre, Gendarmerie)

    ex : *celar@dga.defense.gouv.fr* (écrire au CELAR de la DGA)
    ex : *esic1j118@air.defense.gouv.fr* (écrire à l'ESIC 1J118 de l'armée de l'air)
    ex : *53rt@terre.defense.gouv.fr* (écrire au 53e RT de l'armée de terre)
    ex : *mistral@marine.defense.gouv.fr* (écrire au bâtiment « Mistral »)

  - les champs *Niv-1, Niv-2, Niv-3* correspondent aux niveaux hiérarchiques -1, -2 et -3 de l'organigramme de l'Entité. Il y a correspondance entre la valeur Niv -x présente dans l'adresse de messagerie et celle décrivant la hiérarchie de l'Entité dans l'annuaire.

ex : *53RT-3cie@terre.defense.gouv.fr* (écrire à la 3e compagnie du 53e RT)
ex : *esic1j107-cosic@air.defense.gouv.fr* (écrire au COSIC de l'ESIC 1J107)

2.3. **Le champ lieu (optionnel introduit par un « tiret »).**

Il permet de préciser la localisation de la structure dans les cas ou le nom de celle-ci ne permet pas de l'identifier ou lorsque celle-ci est répartie sur plusieurs sites géographiques.

ex : *esic1j107-villacoublay@air.defense.gouv.fr* (écrire à l'ESIC 1J107 de villacoublay)

2.4. **Le champ dossier (optionnel introduit par un « plus »).**

Il permet de créer un sous-découpage d'une boîte à lettre organique sous forme de sous-dossiers. Un message doit pouvoir être envoyé dans un de ses sous-dossiers, sans qu'il soit nécessaire de créer une nouvelle adresse.

ex : *53RT-3cie+sas@terre.defense.gouv.fr* (écrire au sas de la 3e compagnie du 53e RT)

3. REMARQUE.

L'autorité représentant la structure organisationnelle définit la ou les personnes pouvant accéder à la boîte aux lettres organisationnelle.
Les labels sont fournis par le système d'annuaire du ministère de la défense. Ceux présentés ci-dessus sont cités à titre d'exemple.

ANNEXE VI.

RÈGLES D'ÉLABORATION DES ADRESSES FONCTIONNELLES.

1. FORME DES ADRESSES FONCTIONNELLES.

Fonction.Structure_organisationnelle(-Lieu)(+Dossier)@Organisme.nom_de_domaine
et
Fonction.Organisme@Organisme.nom_de_domaine

2. DÉFINITION DES DIFFÉRENTS CHAMPS.

2.1. **Les champs Organisme, Structure_Organisationnelle, Lieu et Dossier.**

Ils suivent les mêmes règles que pour les adresses d'organismes et les adresses organisationnelles (cf annexes précédentes).

2.2. **Le champ Fonction.**

Correspond :

- à la valeur tous pour désigner l'ensemble des membres d'une entité ou d'un organismes ;

ex : *tous.dggn@dggn.defense.gouv.fr* (écrire à toutes les personnes de la DGGN)
ex : *tous.mistral@marine.defense.gouv.fr* (écrire à tout le personnel du bâtiment « Mistral »)

- à la valeur archives pour archiver les messages conformément aux directives du guide [MOFI]

ex : *archives.53RT@terre.defense.gouv.fr* (archiver un courriel au 53ième RT)

- à une valeur décrivant la fonction tenue. Il y a correspondance entre la valeur utilisée par l'adresse fonctionnelle et le champ fonction du système d'annuaire du ministère de la défense.

ex : *al.marine@marine.defense.gouv.fr* (écrire au chef d'état-major de la marine)
ex : *al.emm@emm.defense.gouv.fr* (écrire au chef de l'état-major de la marine)
ex : *dir.celar@dga.defense.gouv.fr* (écrire au directeur du CELAR)
ex : *os.53RT@terre.defense.gouv.fr* (écrire à l'officier de sécurité du 53ième RT)
ex : *ossi.ba107-villacoublay@air.defense.gouv.fr* (écrire à l'officier de sécurité des SI de la base aérienne 107)

3. REMARQUE.

Les labels et les valeurs sont fournis par le système d'annuaire du ministère de la défense et la directive [MOFI]. Ceux présentés ci-dessus sont cités à titre d'exemple.