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

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 2/DEF/DGSIC portant sur le système d'annuaires du ministère de la défense.

Du 9 mars 2007

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

Référence :

Ordonnance n° 2005-1516 du 8 décembre 2005 (JO du 9, texte n° 9 ; BOEM 120-0.3.1).

Pièce(s) Jointe(s) :

Deux annexes.

Classement dans l'édition méthodique : BOEM 160.1.

Référence de publication : BOC N°17 du 19 juillet 2007, texte 1.

SOMMAIRE

4.2. Règles organisationnelles.

4.3. Règles sémantiques.

ANNEXE(S)

ANNEXE I. GLOSSAIRE ET ACRONYMES.

ANNEXE II. RÉFÉRENCES.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

Cette directive définit les règles du ministère de la défense et donne des critères de décision pour l'acquisition, la réalisation et la mise en œuvre du système d'annuaires.

Elle s'applique à tous les composants, projets, programmes, opérations incluant des logiciels.

Cette directive s'inspire du [CCI] et du projet de [RGI] 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.

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. **Gestion du document.**

Le présent document est actualisé annuellement par la direction générale des systèmes d'information et de communication (DGSIC) après avis de la commission ministérielle technique des systèmes d'information et de communication (CMTSIC), par :

- une publication de la version en cours d'application sur le [site DGSIC] ;

- la possibilité pour toute personne du ministère de la défense de proposer une évolution du document via le [site DGSIC] en postant un commentaire sur la page de publication ;

- une mise à jour régulière pour prendre en compte les évolutions techniques ainsi que les propositions d'évolution ou de modification validées par la DGSIC.

1.4. **Modalités d'application.**

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure. La trajectoire pour rejoindre la cible reste de la responsabilité des organismes, à échéance fin 2009, ou de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense (DIRISI) pour les organismes dont les attributions correspondantes lui ont été confiées.

1.5. **Gestion des exceptions pour les projets.**

Un directeur de projet doit présenter les points suivants auprès de l'instance ministérielle qui autorise le lancement du projet (1) :

- les circonstances et justifications du non respect d'une règle «Recommandé» ;

- les circonstances et justifications du non respect d'une règle «Déconseillé» ;

- 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.**

[CCI] - Recommandations nationales du cadre commun d'interopérabilité.

[RGI] - Référentiel général d'interopérabilité et [RGS] référentiel général de sécurité.

[PRIS] - Politique de référencement intersectoriel de sécurité.

[DGSIC001] - Directive sur les logiciels.

[Schéma] - Schéma d'annuaire.

[CatOID] - Catalogue des OID.

2.2. **Normes et standards applicables.**

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

[RFC 4510] - LDAP v3.

[RFC 4346] - TLS v1.1.

[RFC 4366] - TLS extensions.

[RFC 4422] - SASL.

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

[Site DGSIC] - Site intranet défense DGSIC.

[CMTSIC001] - Compte rendu de la 1re CMTSIC.

[CMTSIC002] - Compte rendu de la 2e CMTSIC.

[CMTSIC003] - Compte rendu de la 3e CMTSIC.

[CGAT] - Recommandations du CGAT.

3. DOMAINE COUVERT ET EMPLOI.

Un annuaire d'entreprise est une base de données hiérarchique permettant de stocker, classer et mettre à disposition des données de référence, notamment en terme d'identités des utilisateurs du système d'information ou d'organisation au sein duquel exercent ces utilisateurs. Il est accessible de manière sécurisée et offre des services avancés d'accès, de recherche, de navigation, de déploiement et de réplication. Il n'a pas vocation à être utilisé pour de la gestion fine de ressources humaines ou matérielles, ni d'être un annuaire technique. L'agrégat de plusieurs annuaires d'entreprises et de mécanismes associés, s'appuyant sur des doctrines et des procédures organisationnelles, est nommé Système d'annuaires.

3.1. **Services attendus du système.**

Au ministère de la défense, le système d'annuaires est notamment utilisé pour :

identification et authentification :

- identifiant unique ;

- support des certificats à tous les niveaux organisationnels du ministère (Infrastructure de Gestion de Clés, Automate de Chiffrement des Informations de la Défense) ;

- SSO (notamment applications web) ;

couplage avec messagerie :

- support de l'adresse de routage ;

- fourniture du nom pour complétion automatique ;

- aide à la constitution de listes de diffusion ;

stockage de droits macroscopiques :

- intra organisme (profils, groupes...) ;

- transverses ;

pages blanches ;

pages jaunes ;

restitution du référentiel d'organisation et des organigrammes.

Cette liste, non exhaustive, est susceptible d'évolutions résultant de nécessaires analyses et spécifications complémentaires.

3.2. **Périmètre et limites.**

Le système d'annuaires défense inclut toutes les procédures et tous les composants nécessaires à la mise en œuvre des fonctions remplies par le système pour apporter les services attendus.

Ces procédures (mode d'alimentation, gestion des mouvements...) et ces composants (annuaires, bases de données relationnelles, programmes, mécanismes de synchronisation et de supervision...) sont de niveau ministère ou à défaut organisme.

Le système d'annuaires défense n'inclut pas les composants et bases de données techniques ou de services, spécifiques à un organisme, une application ou un système d'exploitation. A titre d'exemple, les ressources matérielles et logicielles d'un réseau local ne sauraient faire l'objet de standardisation ou de gestion par le système d'annuaires.

Toutefois, tout annuaire externe doit faire appel au système d'annuaires défense, tel que défini et standardisé au cœur ou en interface dans la suite du document, pour des services de référence tels que l'identification - authentification.

3.3. **Interopérabilité et interfaçage inter-annuaires.**

Les règles garantissent l'interopérabilité du système d'annuaires défense avec les systèmes interfacés.

4. LES RÈGLES.

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

4.1. **Règles techniques.**

RT 01 : il est Obligatoire d'implémenter le schéma d'annuaire défini par l'ADISIC C.

RT 02 : il est Obligatoire de prévoir un mode d'accès conforme à LDAP v3 pour les organismes participant au système d'annuaires de la défense. [RFC 4510]

RT 03 : il est Recommandé d'utiliser *OpenLDAP*, produit sous licence libre.

RT 04 : il est Obligatoire d'utiliser LDAP v3 pour interfacer le système d'annuaires défense avec un annuaire externe. [RFC 4510]

RT 05 : il est Recommandé de disposer au minimum du format LDIF pour échanger tout ou partie d'un annuaire de données LDAP ou, en fonction des nature et fréquence de mise à jour, des mécanismes plus évolués. À ce titre, DSML est un format candidat.

RT 06 : il est Recommandé d'utiliser les extensions de sécurisation LDAP pour sécuriser les services d'un annuaire de données LDAP. [RFC 4346][RFC 4366] [RFC 4422]

RT 07 : lorsque le besoin est de mettre en relation des informations ou de répondre à des requêtes complexes, il est Recommandé d'utiliser une base de données relationnelle.

RT 08 : lorsque le besoin est de refléter une organisation, il est Recommandé d'envisager une solution d'annuaire pour stocker les informations.

RT 09 : lorsque le besoin consiste à gérer des transactions, il est Recommandé d'utiliser une base de données relationnelle.

RT 10 : lorsque le besoin est de modifier fréquemment ou de gérer un volume important d'informations, il est Recommandé d'utiliser une base de données relationnelle. Pour une fréquence moyenne et un volume modéré, un annuaire convient.

RT 11 : il est Recommandé de prévoir un mécanisme de redondance du service d'annuaire (DSA).

RT 12 : il est Recommandé d'utiliser une architecture centralisée pour assurer la cohérence des données du système d'annuaires. Cette architecture peut se baser sur un annuaire fédérateur.

RT 13 : il est Déconseillé de mettre en œuvre un mécanisme de réplication sans faire une étude d'impact sur le réseau.

RT 14 : il est Déconseillé de stocker dans l'annuaire des informations volumineuses telles que des photos par exemple.

RT 15 : dans une optique de réduction des coûts (acquisition, possession, administration et maintenance), il est Recommandé de choisir des solutions matérielles et logicielles interopérables et d'hétérogénéité maîtrisée, au niveau du ministère de la défense et de ses organismes.

RT 16 : il est Obligatoire que chacun des systèmes participant à la fédération, y compris le système d'annuaires fédérateur, mette à disposition les informations à publier dans les zones démilitarisées, lorsque ces dernières existent.

4.2. **Règles organisationnelles.**

RO 01 : Il est Obligatoire que l'identifiant d'une personne du ministère, au sens agent, soit construit depuis le SIRH de sa structure d'appartenance.

RO 02 : Il est Obligatoire que l'identifiant d'une personne du ministère soit de la forme prenom(x).nom où x permet de gérer les homonymies selon les règles du [RGI]. [CMTSIC002]

RO 03 : Il est Obligatoire que l'identifiant d'une personne externe au ministère soit invariant. L'appartenance d'une personne externe au ministère à un SIREN, SIRET, ... n'étant pas pérenne, l'utilisation de ces données est donc prohibée.

RO 04 : Il est Obligatoire de définir l'identifiant d'une personne externe au ministère selon la RO 02, complété d'un signe distinctif unique. [CMTSIC002]

RO 05 : Il est Obligatoire de soumettre toute demande d'évolution du schéma ou du catalogue des OID à l'ADISIC C. [Schéma][CatOID]

RO 06 : Il est Recommandé que les mises à jour intra et inter organismes soient assurées par un réseau de correspondants des entités participant au système d'annuaires défense.

RO 07 : Il est Obligatoire d'estimer l'impact d'un arrêt du service, en particulier vis-à-vis des systèmes interfacés avec l'annuaire et de définir un plan de reprise sur incident adapté.

4.3. **Règles sémantiques.**

RS 01 : Il est Obligatoire de se conformer aux définitions ou références de l'ADISIC C en terme de syntaxe et de sémantique associées aux objets du schéma d'annuaire.

(1) Par exemple le groupe de travail spécialisé dans l’examen des projets (GTEP) de la CSIAG ou de la CSIOC.

ANNEXE I.
GLOSSAIRE ET ACRONYMES.

ADISIC-C : Agence de doctrine et d'interopérabilité des systèmes d'information et de communication placée sous l'égide de la CSIOC, sous-groupe application opérationnelle des normes.

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.

CGAT : Cadre général d'architecture technique.

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 intrinsèquement.

CMTSIC : Commission ministérielle technique des SIC. Commission ministérielle spécialisée instaurée par l'arrêté du 6 juin 2006 (JO du 21, texte n° 11).

DIT : (Directory information tree). LDAP présente les informations sous forme d'une arborescence d'informations hiérarchique appelée DIT, dans laquelle les informations, appelées entrées (ou encore DSE, « Directory service entry »), sont représentées sous forme de branches.

DSA : (Directory service agent). Service d'annuaire « serveur » gérant cette base et ses accès. DIB, DSA et DUA communiquent entre eux à l'aide d'un protocole dédié (DAP ou LDAP).

DSML : (Directory service markup language). Représentation au format XML des informations de services d'annuaire. La première version du DSML a été publiée en juillet 1999. Parmi les supporters de cette initiative, figurent AOL-Netscape, Sun Microsystems, Oracle, Novell, Microsoft et IBM. Dans sa version 1, le DSML résulte en une définition de document type (DTD en anglais) permettant de formaliser en XML les entrées du modèle de données LDAP de manière similaire à un fichier LDIF. La deuxième version du DSML est parue au sein d'OASIS. Il s'agit de décrire la formalisation XML des opérations LDAP d'accès à l'annuaire pouvant être encapsulées dans des paquets SOAP.

GTEP : Groupe de travail spécialisé dans l'examen des projets.

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

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.

LDAP : (Lightweight directory access protocol). Protocole permettant l'accès aux 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. (voir aussi DIT)

LDIF : Lightweight data interchange format. Format d'échange de données qui permet d'importer et d'exporter les données d'un annuaire avec un simple fichier texte.

OID : L'Object identifer permet à un objet (par ex: un attribut d'annuaire ou une classe d'objets, une politique de certification...) d'être référencé de façon unique et universelle pendant toute sa durée de vie. Le nommage des OID qui suit une arborescence, notamment selon la RFC 2256, permet d'assurer une interopérabilité entre logiciels. Les attributs et classes d'objets d'annuaire spécifiques du ministère de la défense font l'objet d'un référentiel ministériel : le catalogue des OID du ministère de la défense.

Sémantique : Ce qui est relatif au sens (d'un mot, d'un texte) ou à une intention (d'une action, d'une organisation).

SASL : Simple authentication and security layer

SSO : (Single sign on) Solution d'authentification unique permettant à l'utilisateur de s'authentifier une fois pour toutes sans avoir à entrer de nouveau son identifiant et son mot de passe, pour chaque application à laquelle il souhaite accéder.

Système : Ensemble de doctrines, de méthodes, de personnes, de procédures, de matériels ou d'installations, organisés de façon à accomplir des fonctions spécifiques. (EMA/EMPLOI 2003)

TLS : (Transport layer security).

ANNEXE II.
RÉFÉRENCES.

(n.i. BO).

[CatOID] Catalogue des OID défense défini par l'ADISIC C (Agence de doctrine et d'interopérabilité des systèmes d'information et de communication) de la CSIOC - Version de référence 1.1a du 29 juin 2006.

[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.

[CGAT] Recommandations du CGAT n° P04 F22 : « Document de référence architecture annuaire » du 24 juillet 2006 V1.3.

[CMTSIC001] Compte rendu de la 1re CMTSIC n° 260/DEF/DGSIC du 19 juin 2006 (mandat GS annuaire).

[CMTSIC002] Compte rendu de la 2e CMTSIC n° 347/DEF/DGSIC du 28 juillet 2006.

[CMTSIC003] Compte rendu de la 3e CMTSIC n° 31/DEF/DGSIC du 22 janvier 2007.

[DGSIC001] Directive sur les logiciels n° 434 du 17 octobre 2006.

[GTEP] Les modalités de présentation des projets de SIAG au GTEP de la CSIAG sont fixées par l'instruction n° 713/DEF/SGA du 24 juin 2004.

[PRIS] Politique de référencement intersectoriel de sécurité v2.0 du 1er juin 2005 (ADAE et DCSSI).

Les RFC sont consultables à l'adresse internet http://www.ietf.org/rfc*numerodeRFC*.txt :

[RFC 2119] : Mots-clés employés dans les « Request for comment » pour définir les niveaux d'obligation.

[RFC 4422] : SASL - Juin 2006.

[RFC 4346] : TLS v1.1 - Avril 2006.

[RFC 4366] : TLS extensions - Avril 2006.

[RFC 4510] : "LDAP Technical Specification Road Map" - Juin 2006.

[RGI] : Référentiel général d'interopérabilité prescrit par l'ordonnance n° 2005-1516 du 8 décembre 2005 (JO du 9, texte n° 9 ; BOEM 120-0.3.1) relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

[RGS] : Référentiel général de sécurité défini par l'ordonnance n° 2005-1516 du 8 décembre 2005 (JO du 9, texte n° 9 ; BOEM 120-0.3.1) relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives.

[Schéma] : Schéma d'annuaire défini par l'ADISIC C - Versions de référence Intradef 1.5 du 17 juillet 2006 et Intraced 1.3 du 17 juillet 2006 disponibles sur [Site DGSIC].

[Site DGSIC] : Site DGSIC à l'adresse intradef www.dgsic.defense.gouv.fr