BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°06 du 3 février 2012

PARTIE PERMANENTE
Administration Centrale

Texte n°3

DIRECTIVE N° 21/DEF/DGSIC
portant sur les certificats électroniques employés au sein du ministère de la défense et des anciens combattants.

Du *20 décembre 2011*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION : *sous-direction de la sécurité des systèmes d'information.*

DIRECTIVE N° 21/DEF/DGSIC portant sur les certificats électroniques employés au sein du ministère de la défense et des anciens combattants.

Du 20 décembre 2011

NOR D E F E 1 1 5 2 4 3 0 X

Pièce(s) Jointe(s) :

Une annexe.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°06 du 3 février 2012, texte 3.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit la politique à mettre en œuvre par les organismes du ministère de la défense et des anciens combattants en matière de production, d'acquisition et d'emploi des certificats électroniques.

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

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'interopérabilité (RGI) et à la request for comments (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.**

Ce document est maintenu et mis à jour par la sous-direction sécurité des systèmes d'information de la DGSIC. Les modifications sont soumises pour approbation au directeur général des systèmes d'information et de communication.

Ce document est disponible sur le site DGSIC.

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

Ces règles définissent la cible et sont applicables aux certificats produits et/ou utilisés au sein du ministère. La trajectoire pour rejoindre la cible, dans les trois ans à partir de la date de parution de la directive (1), 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.

1.5. **Gestion des dérogations.**

Les dérogations concernent :

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

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

- les circonstances et justifications des exceptions à toute règle absolue (obligatoire ou interdit).

Un dossier de dérogation est présenté à la DGSIC. Il fait l'objet d'une approbation par le directeur de la DGSIC lorsqu'il comporte des exceptions à une règle absolue.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

Loi n° 2004-1343 du 9 décembre 2004 (A) de simplification du droit.

Ordonnance 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 (B) pris pour l'application des articles 9., 10. et 12. de l'ordonnance du 8 décembre 2005 .

Arrêté du 6 mai 2010 (C) portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

Référentiel général de sécurité version 1.0 du 6 mai 2010 (2).

Note n° 748/DEF/DGSIC/FSSI du 26 juin 2011 (2) relative à l'application des référentiels généraux de sécurité (RGS) et d'interopérabilité (RGI) au sein du ministère de la défense et des anciens combattants.

Cette directive prend par ailleurs en compte les travaux réglementaires de refonte de l'instruction ministérielle n° 900/DEF/CAB/DR du 18 juin 2007 (2) relative à la protection du secret de la défense nationale au sein du ministère de la défense (2) et de protection des informations diffusion restreinte.

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

Site de la direction générale des systèmes d'information et de communication (DGSIC) à l'adresse intradef (www.dgsic.defense.gouv.fr) ;

Site de la sécurité des systèmes d'informations (SSI) du ministère à l'adresse intradef (www.ssi.defense.gouv.fr) ;

Site SSI de l'agence nationale de la sécurité nationale des systèmes d'information (ANSSI) à l'adresse internet (www.ssi.gouv.fr) ;

Site du *Journal officiel* de la République française (www.legifrance.gouv.fr) ;

http://www.ssi.defense.gouv.fr/_dirsic/textes/mis_sec_dir_sic/secur_sys_info/textes_base/ref_regl/ref_regl.htm ;

Référentiel général d'interopérabilité, version 1.0 du 12 juin 2009 ;

Référentiel général d'accessibilité à l'administration, version 1.0 du 14 mai 2009 ;

Request for comments (RFC 2119) relative aux mots clés pour les niveaux d'obligation (mars 1997).

3. SYNTHÈSE.

3.1. **Objectifs.**

L'emploi des certificats électroniques conforme à la norme X509 version 3 a pour objectifs de fiabiliser les échanges et d'augmenter la confiance (authentification, signature), de renforcer la confidentialité des données (chiffrement), en s'appuyant sur des méthodes éprouvées et robustes.

Le recours systématique aux certificats électroniques pour les besoins de sécurité permet de réduire le coût de possession de ces systèmes (uniformisation des services de sécurité) et d'améliorer l'ergonomie des systèmes d'information.

3.2. **Périmètre et limites.**

La directive est applicable aux systèmes utilisés par le ministère de la défense et des anciens combattants, ainsi que par les établissements ou organismes sous tutelle. Elle fait partie du référentiel documentaire sur lequel s'appuie la politique de sécurité de leurs systèmes d'information (SI).

La directive vise donc à définir les besoins du ministère en termes de prestation interne de services de confiance, ainsi que la qualité, les modalités de délivrance et le concept d'emploi des certificats électroniques au sein du ministère.

La directive établit des règles communes et particulières à tous les systèmes indépendamment de leur niveau de confidentialité. Elle s'applique à la mise en œuvre des algorithmes définis par le référentiel général de sécurité (RGS) et non aux algorithmes gouvernementaux.

Chaque autorité qualifiée en sécurité des systèmes d'information (SSI) sera responsable de l'application de cette directive au sein de son organisme et des organismes ou établissements rattachés.

4. LES RÈGLES.

La directive est déclinée sous l'angle organisationnel principalement, et se décompose en trois parties traitant d'une part des règles globales (RG), puis des systèmes non classifiés (RN), et enfin des systèmes classifiés (RC).

La mise en œuvre technique de la directive et les choix qu'elle implique relèvent de l'opérateur ministériel.

4.1. **Règles générales.**

4.1.1. ***Règles relatives à l'emploi des certificats électroniques.***

RG 1 : il est interdit d'utiliser des certificats multi-usages (exemple : authentification et chiffrement).

Rappel du RGS : l'authentification et la signature sont fondées sur le même procédé. Par exemple, l'authentification est obtenue en « signant » électroniquement un fichier transmis par le correspondant (défi). Si le même certificat sert aux deux fonctions, on ne fera pas la différence entre un défi et un document authentique signé.

RG 2 : un certificat est obligatoirement générique et ne doit pas être porteur de droits.

Afin de ne pas avoir à les renouveler au gré des changements de droits, les certificats doivent être génériques. Les extensions des certificats ne servent pas à gérer des droits applicatifs.

RG 3 : il est recommandé que les utilisateurs aient suivi une sensibilisation sur l'emploi des certificats électroniques et disposent des moyens et/ou des connaissances leur permettant de contrôler la validité des certificats et la chaîne de certification.

C'est nécessaire dans la mesure où il est probable que des autorités de certification racine hors ministère de la défense (MINDEF) seront nativement reconnues par les postes informatiques. Cette règle implique des mesures techniques et/ou organisationnelles.

RG 4 : l'utilisation dans le cadre privé de certificats délivrés par une infrastructure de gestion de clé ministérielle est interdite.

Ils sont destinés à un usage professionnel.

4.1.2. ***Règles relatives aux infrastructures.***

RG 5 : il est obligatoire que les dispositifs porteur (exemple : cartes à puce), support de bi-clés et des certificats, respectent les spécifications du socle commun cartes IAS ECC (identification-authentification-signature european-citizen-card).

Cette règle permet de se prémunir contre le choix d'un type de carte propriétaire. De plus, ce socle commun garantit la prise en compte des exigences de sécurité minimales imposées par le RGS.

RG 6 : il est obligatoire que les dispositifs porteurs d'authentification, de protection de clés privées, de création de signature et de chiffrement mis en œuvre respectent les exigences du niveau 3 étoiles.

Le RGS impose l'emploi de dispositifs matériels pour du 3 étoiles et le recommande pour du 2 étoiles.

Remarque : la carte d'identité multi-services (CIMS) sera au standard IAS ECC évaluée au niveau elevation assurance level 4+ (EAL4+) qualifié renforcé 3 étoiles.

RG 7 : il est recommandé que les dispositifs matériels serveur d'authentification, de cachet, de protection des clés privées, de chiffrement et de création de signature mis en œuvre respectent les exigences du niveau 3 étoiles.

RG 8 : il est obligatoire qu'une application utilisant le certificat électronique détermine automatiquement quel certificat doit être utilisé, à partir de paramètres définis par l'utilisateur.

Cette règle apporte du confort à l'utilisateur et évite qu'une opération soit effectuée avec le mauvais certificat en forçant l'application à contrôler la cohérence entre l'opération souhaitée et le certificat utilisé. L'utilisateur devra par exemple choisir dans un premier temps entre « authentifier, signer, chiffrer » (choix non exclusif), puis choisir l'infrastructure de gestion de clés (IGC) utilisée (donc implicitement le niveau).

L'application devra en particulier exploiter les champs keyUsage, Certificate policy et QCstatements des certificats.

Remarque : l'emploi du champ QCstatements est prévu dans l'annexe A14 du RGS.

RG 9 : il est recommandé que les fonctions de sécurité des systèmes d'information et de communication s'appuient sur l'utilisation de certificats électroniques délivrés par le ministère.

Dans un souci de cohérence et d'économie, les systèmes actuels disposant d'une infrastructure de gestion de clés (IGC) propre et les systèmes futurs devront rallier l'IGC ministérielle de référence ou s'appuyer sur les services de la carte CIMS.

Les systèmes hébergés sur l'internet doivent utiliser les services de CIMS.

Les systèmes hébergés sur l'intraced doivent utiliser l'IGC-G.

Les systèmes hébergés sur l'intradef doivent :

- préparer leur migration vers CIMS lorsqu'ils utilisent l'IGC-G ;

- migrer vers CIMS lorsqu'ils utilisent leur propre IGC ;

- préparer leur ralliement à CIMS, et utiliser éventuellement l'IGC-G de manière transitoire dans les autres cas.

RG 10 : il est recommandé d'utiliser, au sein du ministère, les certificats du MINDEF pour les applications interministérielles imposant un certificat, qu'elles soient interministérielles, internationales ou autres.

La signature de l'autorité de certification racine du MINDEF par l'autorité de certification de l'infrastructure de gestion de la confiance de l'administration (IGC/A) doit permettre au MINDEF d'utiliser ses certificats pour les usages interministériels et de limiter le nombre de certificats manipulés par les agents et gérés par l'administration.

RG 11 : il est recommandé de définir les autorités de certification racine reconnues par le ministère et le périmètre (intraced, intradef, internet) où elles sont reconnues.

Cette liste, validée par la DGSIC [fonctionnaire de la sécurité des systèmes d'information (FSSI)], doit permettre de limiter les autorités de certification racine présentes sur les équipements aux seules autorités de certification racine (ACR) reconnues, et/ou de permettre de vérifier qu'un certificat est bien issu d'une ACR reconnue par le ministère.

4.2. **Réseaux ne relevant pas du secret de la défense nationale (intradef, internet).**

La cible est à atteindre pour les réseaux intradef et internet par le biais du projet CIMS. A terme chaque utilisateur du ministère de la défense devra disposer d'au moins un certificat compatible du RGS, même si cela ne semble pas nécessaire a priori. L'objectif est d'homogénéiser les certificats du ministère.

4.2.1. ***Règles relatives aux certificats porteur.***

RN 1 : il est obligatoire que les certificats porteurs d'authentification, de chiffrement et de signature respectent les prescriptions du RGS.

Cf. l'ordonnance n° 2005-1516 du 8 décembre 2005.

RN 2 : chaque agent du ministère de la défense doit obligatoirement disposer d'un triplet de certificats porteurs (authentification, signature, chiffrement) utilisables sur le réseau sensible non classifié de défense.

Il s'agit de la cible à atteindre par le biais du projet de carte CIMS.

RN 3 : la délivrance de certificats fonctionnels pour l'authentification, le chiffrement et la signature est interdite.

Cette règle constitue un rappel du RGS et interdit en particulier la délivrance de certificats fonctionnels, la correspondance certificat-fonction pouvant être réalisée par ailleurs.

RN 4 : les personnes extérieures au ministère ayant légitimement besoin d'accéder à l'intradef utiliseront obligatoirement les certificats porteurs qui leur seront délivrés par le ministère à cet effet.

Cela permettra d'assurer les mêmes fonctions de sécurité vis-à-vis de ces personnes extérieures. Le besoin sera à formaliser dans un contrat, un partenariat, etc.

RN 5 : il est déconseillé d'utiliser des certificats porteurs logiciels [public key cryptographic standards (PKCS) #12)] pour les fonctions de sécurité de niveau supérieur à 1 étoile tel que défini dans le RGS.

Pour les fonctions de sécurité de niveaux 2 étoiles et 3 étoiles, le ministère privilégie l'utilisation de dispositifs matériels de protection des clés privées qualifié au niveau renforcé.

4.2.2. ***Règles relatives aux certificats serveurs.***

RN 7 : il est obligatoire que les certificats serveurs d'authentification et de cachet respectent les prescriptions du RGS.

Cf. l'ordonnance du 8 décembre 2005.

4.2.3. ***Règles relatives à l'infrastructure.***

RN 7 : l'opérateur du ministère de la défense doit être obligatoirement certifié en tant que prestataire de service de certification électronique de niveau 2 étoiles au moins.

C'est une condition nécessaire pour être en mesure de proposer des services d'identification, authentification et de signature de niveau 2 étoiles, ce qui est la cible à atteindre au MINDEF.

Il faut noter que le projet CIMS remplit cette condition pour les certificats porteurs 3 étoiles.

RN 8 : il est obligatoire que le ministère dispose d'une IGC dont l'ACR est signée par l'IGC/A.

Cela permet de disposer de certificats reconnus par les navigateurs et validés par l'État.

L'IGC/A étant reconnue par défaut par les systèmes récents, cela permettra la reconnaissance des certificats sans avoir à forcer la connaissance de l'autorité de certification racine MINDEF et l'usage en interministériel.

Cette reconnaissance par l'IGC/A est subordonnée au respect des meilleures pratiques en matière de gestion de clés et notamment la règle suivante.

RN 9 : il est obligatoire que toute demande de certificat porteur auprès de l'opérateur prestataire de services de certification électronique (PSCE) du ministère soit identifiée, authentifiée et archivée pendant la durée de validité du certificat demandé.

4.3. **Réseaux relevant du secret de la défense nationale.**

4.3.1. ***Règles relatives aux certificats porteurs.***

RC 1 : il est déconseillé d'utiliser des certificats porteurs logiciels (PKCS#12).

Cela est cohérent avec le niveau de sécurité attendu d'un réseau relevant du secret de la défense nationale.

RC 2 : il est obligatoire que les certificats porteurs d'authentification et de signature respectent les prescriptions du RGS.

Le RGS constitue un référentiel de règles et de bonnes pratiques qu'il est opportun d'appliquer ici. Cette règle interdit de facto la délivrance de certificats fonctionnels pour l'authentification et la signature. Cela

contribuera en particulier à faciliter l'imputabilité des actions.

RC 3 : il est recommandé que les certificats porteurs de chiffrement soient personnels.

L'interdiction des certificats fonctionnels de chiffrement pour les porteurs ne s'impose pas ici.

RC 4 : il est obligatoire que les certificats porteurs de chiffrement utilisés respectent les prescriptions du RGS lorsqu'ils sont utilisés dans le cadre du respect du besoin d'en connaître.

L'emploi de certificats fonctionnels ne permet pas de gérer le besoin d'en connaître.

L'emploi du certificat pour le chiffrement d'une information classifiée permet de limiter son exploitation aux seuls utilisateurs du fichier électronique. Ce chiffrement ne suffit toutefois pas à assurer la confidentialité de l'information qui doit transiter sur des circuits homologués adéquats.

4.3.2. ***Règles relatives aux certificats serveurs.***

RC 5 : il est recommandé que les certificats serveurs d'authentification et de cachet respectent les prescriptions du RGS.

Le RGS constitue un référentiel de règles et de bonnes pratiques qu'il est opportun d'appliquer ici.

Pour le ministre de la défense et des anciens combattants et par délégation :

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

Christian PÉNILLARD.

---

(1) Pour les SI relevant du RGS, 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 impose une mise en conformité dans les 3 ans à compter de sa parution par l'arrêté du 6 mai 2010 portant approbation du RGS soit le 10 mai 2013.

(A) n.i. BO ; JO n° 287 du 10 décembre 2004, page 20857, texte n°1.

(B) n.i. BO ; JO n° 29 du 4 février 2010, page 2072, texte n°1.

(C) n.i. BO ; JO n° 113 du 18 mai 2010, page 9152, texte n°1.

(2) n.i. BO.

ANNEXE.

GLOSSAIRE ET ACRONYMES.

La plupart des définitions suivantes sont issues du RGS.

Agent : personne physique agissant pour le compte d'une autorité administrative.

Autorité de certification (AC) : au sein d'un prestataire de services de certification électronique (PSCE), une AC a en charge, au nom de et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification (PC). Elle est identifiée en tant qu'émetteur dans les certificats émis selon cette PC.

Autorité de certification racine (ACR) : voir « chaîne de certification ».

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

Chaîne de certification : ensemble d'AC où chaque AC est certifiée par une AC d'échelon supérieur. À titre d'illustration, une AC délivrant des certificats à des utilisateurs peut elle-même être certifiée par une AC, dite « AC intermédiaire », qui à son tour peut être certifiée par une autre AC intermédiaire, ainsi de suite jusqu'à l'AC de plus haut niveau, auto-signée, dite « AC racine ».

Défi : suite de caractères aléatoire (pouvant représenter une question) garantissant une notion de fraîcheur/unicité qui est envoyée chiffrée par une entité (le vérificateur) à une autre entité (le prouveur) pour vérifier son identité. Dans le cas du chiffrement asymétrique, le vérificateur utilise la clé publique du prouveur et le prouveur renvoie sa réponse chiffrée avec sa clé privée.

Infrastructure de gestion de clés (IGC) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés cryptographiques asymétriques et des certificats associés. Une IGC peut être composée d'un service de génération de certificats, d'un service d'enregistrement, d'un service de publication, ...

Infrastructure de gestion de la confiance de l'administration (IGC/A) : infrastructure de gestion des clés cryptographiques (IGC) opérée par l'agence nationale de la sécurité des systèmes d'information, l'autorité de certification racine de l'État français.

Prestataire de services de certification électronique (PSCE) : toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différents types de certificats correspondant à des usages et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres ou liées (AC Racines/AC Filles). Un PSCE est identifié, dans un certificat dont il a la responsabilité, au travers de l'AC qui a émis ce certificat.

Système d'information : tout ensemble de moyens destiné à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.