BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°28 du 29 juin 2012

PARTIE PERMANENTE
Administration Centrale

Texte n°2

DIRECTIVE N° 26/DEF/DGSIC

modifiant la directive n° 21/DEF/DGSIC du 20 décembre 2011 portant sur les certificats électroniques employés au sein du ministère de la défense et des anciens combattants.

Du *12 juin 2012*

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

DIRECTIVE N° 26/DEF/DGSIC modifiant la directive n° 21/DEF/DGSIC du 20 décembre 2011 portant sur les certificats électroniques employés au sein du ministère de la défense et des anciens combattants.

Du 12 juin 2012

NOR D E F E 1 2 5 0 8 7 1 X

Texte modifié :

Directive n° 21/DEF/DGSIC du 20 décembre 2011 (BOC N° 06 du 3 février 2012, texte 3 ; BOEM 160.1).

Référence de publication : BOC N°28 du 29 juin 2012, texte 2.

La directive n° 21/DEF/DGSIC du 20 décembre 2011 est modifiée comme suit :

1. Au point 1.5. « Gestion des dérogations ».

Remplacer :

« 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. » ;

Par :

« Les dérogations concernent les circonstances et justifications des exceptions à toute règle absolue (obligatoire ou interdit).

Un dossier de dérogation est présenté et fait l'objet d'une approbation par le DGSIC. ».

2. Au point 2.1. « Documents applicables ».

Septième alinéa.

Remplacer :

« 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 et de protection des informations diffusion restreinte. » ;

Par :

« Instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (2) relative à la protection du secret de la défense nationale au sein du ministère de la défense. ».

3. Au point 4.1.1. « Règles relatives à l'emploi des certificats électroniques ».

Avant le premier alinéa, insérer les deux alinéas suivants :

« RG 0 : il est recommandé d'utiliser des certificats au format X.509 version 3.

Cette recommandation découle de la recommandation du référentiel général d'interopérabilité de se conformer au « WS-I Basic Profile version1.1 ». Lorsqu'elle n'est pas respectée, les autres règles de la présente directive demeurent applicables. ».

4. Au point 4.3.1. « Règles relatives aux certificats porteurs ».

4.1. Remplacer :

« 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. » ;

Par :

« RC 2 : il est obligatoire que les certificats porteurs de signature respectent les prescriptions du RGS.

RC 2 *bis* : il est recommandé que les certificats porteurs d'authentification et de chiffrement 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 la signature, ce qui contreviendrait aux dispositions relatives à la signature électronique, notamment l'article 1316-4. du code civil. On notera que si la validation éventuelle des certificats par l'IGC/A est fonctionnellement requise, celle-ci suppose le respect des prescriptions du RGS, conférant alors à cette règle un caractère obligatoire. ».

4.2. Remplacer :

« 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. » ;

Par :

« RC 3 : il est obligatoire que les certificats porteurs fonctionnels soient délivrés sous une procédure assurant la traçabilité de l'utilisateur.

RC4 : il est recommandé que les certificats porteurs fonctionnels soient délivrés sous la forme d'un support matériel ACSSI (articles contrôlés de la sécurité des systèmes d'information).

L'emploi de certificats fonctionnels ne permet pas de gérer le besoin d'en connaître, ni d'imputer directement des actions à une personne. La traçabilité requise doit donc être faite par des moyens organisationnels. La prise en compte du support du certificat fonctionnel, si c'est un ACSSI, permet d'assurer cette traçabilité par un moyen juridiquement décrit et réglementaire, désignant les responsabilités. L'autorité prenant en compte ce support est ensuite libre de mettre en place les moyens de traçabilité de l'usage de ce support qu'elle juge pertinents. ».

Pour le ministre de la défense et par délégation :

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

Christian PÉNILLARD.