CEA/DAM/DCG/SAPI
DO 54 27/03/23
23SSJD000187
diffusé le : 27/03/23

Engagement du Soumissionnaire en matière de protection de l'information protégée par la mention *Diffusion Restreinte*

–

Déclinaison en règles de sécurité informatique

SOMMAIRE

TERMINOLOGIE

ACID	Logiciel de chiffrement (générant des conteneurs chiffrés)
ANSSI	Agence nationale de la sécurité des systèmes d'information
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CEA/DAM	Direction des applications militaires du CEA
DO	Diffusion Ordinaire (informations non protégées mais réservées à une diffusion interne au sein de l'entreprise)
DR	*Diffusion Restreinte* (définition de l'IGI 1300)
GSM	Global System for Mobile communications (connexion téléphonie mobile)
S	***Secret*** (définition de l'IGI 1300), anciennement Confidentiel Défense
SF	Spécial France (définition de l'IGI 1300)
SI	Système(s) d'Information
TS	***Très Secret*** (définition de l'IGI 1300), anciennement Secret Défense
USB	Universal Serial Bus
Wi-Fi	Accès réseau sans fil (différents protocoles utilisés : WPA soit Wi-Fi Protected Access, WPA2 (préconisé), WPA3)
Zed	Logiciel de chiffrement de conteneurs
ZoneCentral	Logiciel de chiffrement (générant aussi des conteneurs chiffrés Zed)

ARTICLE 1 - OBJET

Le présent document précise les règles de sécurité informatique qui doivent être respectées par les candidats ou soumissionnaires (ci-après dénommés « Soumissionnaire(s) ») aux consultations menées par la Direction des applications militaires du Commissariat à l'Energie Atomique et aux énergies alternatives (CEA/DAM) et donnant lieu à l'échange d'informations à caractère sensible, faisant l'objet d'une mention de protection particulière *Diffusion Restreinte* (DR) visant à garantir leur confidentialité.

Ce document doit être signé par un représentant du Soumissionnaire ayant tout pouvoir à cet effet et être retourné au CEA/DAM dans les conditions définies par les documents de consultation ou par l'avis de marché.

En cas de candidature en groupement momentané d'entreprises, un exemplaire de ce document doit être établi et retourné par le mandataire ainsi que par chaque membre du groupement (cotraitant) concerné par l'échange d'information à caractère sensible.

De même, un exemplaire de ce document doit être rempli et retourné pour chaque sous-traitant auquel il est envisagé de faire appel dans la phase d'élaboration de l'offre et concerné par l'échange d'information à caractère sensible.

Rappel : Le présent document traite des systèmes d'information (SI) utilisés par le Soumissionnaire pour sa réponse à la consultation. Le Soumissionnaire doit impérativement mentionner dans son offre, les SI qui lui sont propres ou qu'il entend créer spécifiquement et utiliser dans le cadre de l'exécution du marché. Ces SI doivent être conformes aux règles citées à l'article 2 auxquelles s'ajoutent les BONNES PRATIQUES ANSSI[1] et les prescriptions spécifiques au marché.

ARTICLE 2 - EXIGENCES DE SECURITE INFORMATIQUE

La réponse à la consultation implique le traitement d'informations ou supports sensibles DR.

Le Soumissionnaire s'engage à traiter ces informations ou supports, portant la mention de protection DR, dans le respect des règles édictées par les dispositions légales et réglementaires en vigueur suivantes, dans leur version applicable :

- l'Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale (IGI 1300),
- l'Instruction interministérielle relative à la protection des systèmes d'informations sensibles n°901/SGDSN/ANSSI (II 901),
- l'arrêté du ministère des Armées portant approbation de l'Instruction ministérielle n° 900 sur la protection du secret et des informations *diffusion restreinte* et sensibles (IM 900) et
- le guide ANSSI « Guide d'hygiène Informatique »[2] dans sa dernière version. Ces règles sont déclinées par ce qui suit.

L'annexe n°1 de l'IGI 1300 prévoit que les SI aptes à traiter des informations DR doivent faire l'objet d'une homologation de sécurité (§ 5). En conséquence, les SI utilisés par le Soumissionnaire et ses éventuels cotraitants et sous-traitants pour traiter et élaborer les documents DR dans le cadre de la consultation doivent être :

- des SI homologués par l'Autorité Qualifiée de l'entreprise, aptes à traiter des informations classifiées ;
- ou des SI homologués par l'Autorité Qualifiée de l'entreprise conformément aux dispositions de l'II 901, aptes à traiter des informations DR ;
- ou, dans l'attente d'une homologation, des SI constitués d'un ordinateur ou d'un réseau qui obéissent aux règles suivantes :
    - Le système est dédié aux applications bureautiques propres à l'entreprise ;
    - Le système ne possède aucune connexion avec l'Internet[3] ;
    - Le système est conforme aux règles de configuration et d'utilisation de l'article 3.

Les exigences pour l'homologation de sécurité d'un SI ne peuvent être inférieures à celles indiquées dans ce document pour la réponse à la consultation.

---

[1] Documents disponibles sur le site de l'ANSSI (https://www.ssi.gouv.fr), catégorie 'UNE ENTREPRISE'
[2] BONNES PRATIQUES de l'ANSSI, thème : Poste de travail et serveurs
[3] Filaire, Wi-Fi, GSM, etc.

ARTICLE 3 - REGLES DE CONFIGURATION ET D'UTILISATION

3.1 PROTECTION DU SYSTEME INFORMATIQUE

Le SI (postes de travail informatiques, applications bureautiques) est propre à l'entreprise et ne peut être externalisé ou hébergé par un tiers (pas de solution bureautique en nuage). Le Soumissionnaire atteste que l'administration de ces SI est confiée à des administrateurs respectant les règles élémentaires d'hygiène informatique définies par l'ANSSI et celles du présent article 3. Il doit préciser (à l'article 7 du présent engagement) si ces administrateurs sont des salariés de l'entreprise ou si cette activité est sous-traitée. Conformément à l'II 901 - Annexe 2, à défaut de passerelle d'interconnexion homologuée, le réseau utilisé doit être un réseau de classe 2, « isolé c'est-à-dire non connecté même indirectement à Internet ». Les transferts à destination de ce type de réseau doivent être réalisés de préférence par le biais de supports amovibles contenant les informations chiffrées transmises par le CEA/DAM ou au travers d'une interconnexion directe unidirectionnelle par le biais d'une passerelle montante (diode).

Le SI est protégé par un antivirus efficace mis à jour régulièrement, au minimum de manière hebdomadaire et l'accès aux informations sensibles est restreint aux seules personnes ayant à les consulter et les traiter, via un compte nominatif et un mot de passe de niveau de sensibilité moyen à fort (au sens de l'ANSSI) a minima.

3.2 SAUVEGARDES

Le Soumissionnaire souhaitant sauvegarder des informations portant la mention de protection DR, s'engage à mettre en œuvre, sous sa responsabilité, une sauvegarde de ces informations dans des conditions telles que l'on puisse localiser et identifier le ou les supports de sauvegarde. Le support de sauvegarde peut être :

- des CD ROM ou DVD ROM : Ceux-ci doivent alors porter la mention « Diffusion Restreinte » et être stockés dans une armoire fermée à clefs.
- des disques durs externes : Ceux-ci doivent alors porter la mention « Diffusion Restreinte » et être stockés dans une armoire fermée à clefs.
- une ou plusieurs machines du réseau spécifique.

A l'issue de la consultation, les supports de sauvegarde devront être remis au CEA/DAM ou faire l'objet d'une destruction conformément aux dispositions de l'article 5 du présent engagement.

3.3 SUPPORTS AMOVIBLES

Si le Soumissionnaire souhaite utiliser des supports informatiques amovibles dans le cadre de la consultation, ces derniers doivent être des clés USB, des CD-ROM ou des disques amovibles. Le Soumissionnaire s'engage à ce que ces supports répondent aux conditions mentionnées ci-dessous :

- les supports sont neufs ou ont été reformatés par un outil approuvé par l'ANSSI,
- ils sont parfaitement identifiés,
- ils sont dédiés à l'affaire en cours.

Tous les fichiers relatifs à la consultation contenant des informations DR, déposés sur ces supports, doivent être chiffrés suivant les dispositions de l'article 4.2 du présent engagement.

Nota : Les fichiers n'ayant pas de caractère sensible tels que des documents administratifs, plaquettes d'entreprise, etc., qui sont de Diffusion Ordinaire ou publics, peuvent être non chiffrés.

A l'issue de la consultation, les fichiers et supports amovibles devront être remis au CEA/DAM ou faire l'objet d'une destruction ou d'un effacement sécurisé conformément aux dispositions de l'article 5 infra.

ARTICLE 4 - COMMUNICATIONS PAR VOIE ELECTRONIQUE

4.1 PRINCIPES GENERAUX

Le Soumissionnaire s'engage à appliquer les règles suivantes pour toute communication par voie électronique réalisée dans le cadre de la consultation (et notamment toute communication entre les membres de son personnel, avec ses cotraitants et sous-traitants ou avec le CEA/DAM) :

1. Aucun message de niveau DR (corps du message et pièce jointe) n'est transmis en clair sur Internet.

2. Tout document de niveau DR, y compris lorsqu'il est échangé au moyen de la plateforme de dématérialisation des achats utilisée par le CEA/DAM, doit être transmis dans des conteneurs chiffrés suivant les dispositions des articles 4.2 et 4.3 du présent engagement.

4.2 MANIPULATION DES CONTENEURS CHIFFRES

Les Soumissionnaires disposant préalablement du logiciel de chiffrement ACID Cryptofiler peuvent échanger avec le CEA/DAM par ce moyen. Pour ce faire, les clés publiques ACID des correspondants/interlocuteurs peuvent être échangées sur l'Internet.

A défaut, le logiciel de chiffrement ZoneCentral ou Zed sont utilisés. Pour ce faire, dans le cadre d'un dossier de consultation des entreprises, un conteneur Zed vide est mis à disposition des Soumissionnaires par le CEA/DAM. Le mot de passe d'accès est transmis aux personnes concernées par une voie spécifique (courrier papier, appel téléphonique uniquement). Le mot de passe, qu'il est conseillé de noter dans un document protégé de niveau DR, n'est écrit sur aucun SI ni téléphone mobile. Les conteneurs Zed doivent être utilisés uniquement à l'aide du logiciel ZoneCentral ou la version qualifiée gratuite du logiciel Zed[4] disponible sur le site de l'éditeur Prim'x : https://client.primx.eu/PublicSoftware/zedlimitededition/.

Une fois le code obtenu **et le dossier de consultation des entreprises (DCE) décompressé**, le fichier xxx_DR.zed pourra être décrypté à l'aide du logiciel téléchargeable à l'adresse ci-dessus. Un guide d'utilisation de cette version à date est disponible en Annexe 1.

Les conteneurs chiffrés, Zed ou ACID, sont transférés sur le SI sécurisé du Soumissionnaire tel que défini à l'article 2 du présent engagement préalablement au traitement des documents qu'ils contiennent. Symétriquement, les documents à expédier sont mis en conteneur sur le SI sécurisé, avant expédition en pièce jointe de messagerie ou dépôt sur la plateforme d'échange avec le CEA/DAM.

4.3 POLITIQUE DES MOTS DE PASSE

Les règles minimales pour la composition des mots de passe sont décrites ci-après :

- Longueur minimale : 12 caractères ;
- Composition - nombre de jeux de caractères différents = 3 ;
- Durée de vie : le temps de la consultation.

EXIGENCES DE COMPOSITION

Les exigences de composition sont les suivantes :

- Ne pas contenir 5 caractères consécutifs du nom, prénom, numéro de badge du salarié ou dernier mot de passe ;
- Ne pas contenir un mot issu d'un dictionnaire (français, anglais) ni, autant que possible, des combinaisons triviales (1234, azerty, etc.) ;
- Ne pas contenir plus de 2 fois consécutives le même symbole.

[4] A date, la version Q.2020.1 pour Windows certifiée le 22/08/2022

ARTICLE 5 - FIN DE PROCEDURE - RESTITUTION

A la fin de la consultation, si votre entreprise n'est pas retenue pour le marché, objet de la consultation du CEA/DAM, l'intégralité des informations ou supports sensibles portant la mention *Diffusion Restreinte* mis à votre disposition dans le cadre de la procédure/consultation devront être retournés ou détruits. Tous les fichiers DR traités, ainsi que les dossiers de travail et les sauvegardes de niveau DR devront être supprimés selon une procédure d'effacement sécurisé[5]. Les supports amovibles seront détruits ou remis au CEA/DAM. Une attestation sur l'honneur de destruction ou d'effacement des informations DR et supports amovibles sera alors adressée au CEA/DAM.

Nous vous rappelons que la conservation, la copie, la diffusion de ces informations ou supports sensibles, sans autorisation écrite et préalable du CEA/DAM, est susceptible d'engager votre responsabilité.

En cas d'attribution du marché, le -désormais- Titulaire s'engage à respecter les dispositions de restitution figurant dans les documents applicables au marché.

ARTICLE 6 - AUDIT ET CONTROLE

Le CEA/DAM ou son autorité de sécurité peuvent être amenés à auditer ou faire auditer les conditions de protection par le Soumissionnaire (ses cotraitants et sous-traitants éventuels) des informations de *Diffusion Restreinte* du CEA.

[5] La suppression effective des fichiers exige de réécrire des données sur l'espace mémoire ou disque qu'ils occupaient, par « surcharge » de cet espace.

ARTICLE 7 - ENGAGEMENT DU SOUMISSIONNAIRE

La société (1)....., immatriculée au Registre du Commerce et des Sociétés sous le numéro (2)....., représentée par (3)....., s'engage par les présentes à respecter l'ensemble des règles fixées dans le présent document.

Les administrateurs des SI de l'article 2 sont :

□ des salariés de la société Soumissionnaire

□ des salariés d'un sous-traitant (préciser sa dénomination sociale) .....

.....

Sous réserve de l'accord préalable de l'acheteur concerné, le présent engagement peut être valable (et donc ne pas être transmis de nouveau par le Soumissionnaire) pendant une durée d'un an à compter de sa date de signature, pour toutes les consultations **d'une même unité achats du CEA/DAM**.

(1) Indiquer la raison sociale de l'entreprise
(2) Préciser au format : RCS + ville + « B » + numéro
(3) Mentionner le nom et la fonction du représentant

Date :

Signature :

Cachet de l'entreprise :

Annexe 1

Guide d'utilisation de la version Zed Limited Edition à date

Une fois que vous avez cliqué sur le lien https://client.primx.eu/PublicSoftware/zedlimitededition/, sélectionnez la version correspondante à votre système d'exploitation et à la version souhaitée :

Une fois le téléchargement terminé ouvrez le fichier et lancez le fichier téléchargé, soit dans l'exemple ci-dessus zedle Q.2020.1 x64.exe

Dans le logiciel ouvert sélectionnez votre fichier xxx _DR.zed puis insérez le mot de passe.