CEA/DAM/DCG/SAPI
DO 1405 18/12/15
15SSJD002413
diffusé le : 18/12/15

Date : 28/03/17

DIF/UPN			
	A/I		A/I
FRL	I	ODR	I
EHL	I	GVR	I
BGA	I	FMI	I
SCH	I	CNL	I
EOB	I	DLA	I
TDA	I	XPT	I
JBT	I	ERO	I
ACL	I	CTi	I
GBT	I	GJO	I
		FVX	I
Cit	1-07		

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information

Diffusion Restreinte

–

Déclinaison en règles de sécurité informatique

CEA/DAM/DCG/SAPI
DO 1405 18/12/15
17PPPL000722
Diffusé le 28/03/17

SYM A000D SJD DIR 15002413 A

	Rédacteur	Vérificateurs		Approbateur	Émetteur
Nom	J.J. FILLET	G. FICINI-DORN	E. DELAVAULT	J. AUTHESSERRE	J. CARDONNA
Fonction ou Unité	DCG/SAPI	DCG/SAPI	DAM/DQSCG	DAM/DQSCG	DCG/SAPI
Date	18/12/15	18/12/15	18/12/15	6/1/2016	18/12/15
Visa					

Commissariat à l'énergie atomique et aux énergies alternatives
Centre DAM-Ile de France - DAM/DCG/SAPI/BPAM – Bâtiment U
Bruyères-le-Châtel – 91297 Arpajon cedex
Etablissement public à caractère industriel et commercial – RCS Paris B 775 685 019

Direction des applications militaires

TABLEAU DES EVOLUTIONS

Edition	Motif et nature des évolutions	Date
Indice A	Edition initiale	15/12/2014

Sommaire

OBJET

Le présent document a pour objet de définir les prescriptions de sécurité informatiques du CEA/DAM pour les systèmes d'informations traitant des informations sensibles non classifiés de défense.

Il se décompose en trois chapitres et une annexe :

1. Un premier chapitre didactique ayant pour vocation de rappeler les grands principes qui permettent au titulaire d'un marché de la Direction des Applications Militaires du CEA de comprendre clairement le contexte du marché et les obligations afférentes en matière de Sécurité des Systèmes d'Information (SSI),
2. Un deuxième chapitre qui définit les prescriptions de sécurité informatique du CEA/DAM pour les systèmes d'informations du Titulaire devant accueillir des données « Diffusion restreinte »,
3. Un troisième chapitre qui définit les prescriptions de sécurité informatique pour les échanges d'informations de Diffusion Restreinte entre le CEA/DAM et le Titulaire ou avec ses éventuels sous-traitants ou cotraitants,
4. Une annexe qui constitue la convention d'utilisation du logiciel ACID Cryptofiler si celui-ci est retenu dans le cadre de l'exécution du marché.

Ces chapitres, et notamment les chapitres 2 et 3, sont autoporteurs et peuvent être utilisés indépendamment les uns des autres.

DOCUMENTS DE REFERENCE

IGI 1300	Instruction Générale Interministérielle n°1300 sur la protection du secret de la défense nationale
II 920	Instruction Interministérielle n°920 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel Défense
II 901	Instruction Interministérielle n° 901 relative à la protection des systèmes d'information sensibles (réf. PRMD1503279J du 28/01/2015)
Guide ANSSI	Maitriser la SSI pour les systèmes industriels – juillet 2013
	Hygiène Informatique - janvier 2013

CHAPITRE 1 : PRINCIPES DE SECURITE DES SYSTEMES D'INFORMATION – CONDITIONS D'USAGE

1 Nature des marchés impliquant la détention d'informations classifiées ou sensibles

Les marchés mettant en œuvre des informations classifiées ou sensibles passés par le CEA/DAM sont qualifiés :

- de Marché classifié avec détention d'informations lorsque le Titulaire a accès à des informations ou supports classifiés dans ses locaux,
- de Marché classifié sans détention d'informations lorsque le Titulaire a accès à des informations ou supports classifiés dans les locaux du CEA sans détention de ces informations ou supports classifiés,
- de Marché sensible lorsque le Titulaire a accès à et peut détenir des informations sensibles,
- de Marché sans mention de protection dans les autres cas.

En application des dispositions de l'IGI 1300, ces marchés intègrent les clauses de protection du secret adéquates.

Toutes les dispositions applicables au Titulaire d'un marché sensible sont applicables à ses sous-traitants dans le cadre de l'exécution du marché dans la mesure où les prestations sous-traitées sont sensibles.

2 Le classement des informations

Le CEA/DAM applique les définitions réglementaires nationales relatives à la protection de l'information, par sensibilité décroissante :

- Les **informations classifiées** : Confidentiel Défense ou Secret Défense.

- les **informations sensibles non classifiées** dont la divulgation est susceptible d'induire une perte, une nuisance ou une gêne au CEA :

  Elles portent une mention : en général Diffusion Restreinte, voire Confidentiel CEA, Confidentiel Industrie ou spécifique.

  Le CEA/DAM distingue pour ses besoins propres, des informations « sensibles » et « très sensibles », mais y applique l'unique mention de Diffusion Restreinte.

- les **informations de diffusion ordinaire**, destinées à une diffusion large sans jamais être publique. Elles peuvent prendre le statut d'information ouverte après autorisation de publication.

  Elles ne portent pas de mention.

Il est du ressort exclusif de l'unité prescriptrice du CEA/DAM d'identifier et de définir le périmètre des informations sensibles non classifiées qui sont traitées par le Titulaire et de bien définir les SI qui seront concernés par les prescriptions de sécurité et d'échange.

Les documents techniques relatifs aux marchés sensibles de la DAM portent généralement la mention Diffusion Restreinte, voire Confidentiel CEA.

3 Principes de sécurité des SI pour les marchés classifies ou sensibles

Du point de vue des systèmes d'informations du Titulaire, les contraintes de sécurité ne sont liées qu'aux informations détenues par le Titulaire. Les marchés qualifiés de « Marché classifié sans détention d'informations » mettant en œuvre uniquement des données sensibles non classifiées de défense sur le SI du Titulaire, les dispositions relatives aux marchés sensibles doivent leur être appliquées.

3.1 – Dans le cas du traitement sur le SI de l'entreprise titulaire du marché, d'informations classifiées de niveau Confidentiel Défense ou Secret Défense, le marché établi avec l'entreprise est un contrat classifié du niveau de confidentialité adapté avec détention d'information. La responsabilité du Titulaire de respecter les obligations portées par l'IGI1300 et l'II920 lui est propre. Le Titulaire fait intervenir des personnels habilités et fera valoir, sinon fait procéder à l'homologation du système d'information concerné. Pour cela, il dispose de locaux dont une aptitude physique aura été délivrée par l'autorité de sécurité compétente. Aucune exigence complémentaire n'est demandée par le CEA/DAM sur le SI homologué. La présentation des attestations d'aptitude physique des locaux et d'homologation des systèmes d'information est un préalable à la signature du marché.

3.2 – Dans le cas du traitement par le Titulaire d'informations sensibles non classifiées, identifiées par la mention Diffusion Restreinte ou Confidentiel CEA, le marché établi avec l'entreprise est au minimum[1] un marché sensible. La responsabilité de l'entreprise de respecter les obligations exprimées par l'II901 pour son SI lui est propre. L'II901 exige alors que le SI du Titulaire soit de classe 2 (isolé de l'Internet) ou de classe 1 (communicant avec l'Internet par une passerelle filtrante dotée d'un dispositif de traçabilité et d'alerte, de surcroît qualifiée par l'ANSSI ou un organisme agréé). La nouveauté de l'instruction, la difficulté de se prémunir des risques issus de l'Internet et l'indisponibilité à court ou moyen terme de solutions de classe 1, amène le CEA/DAM à

[1] Il peut également s'agir d'un marché classé sans détention.

exiger certaines dispositions pratiques et à préconiser des solutions pragmatiques issues de l'II901 dans la mesure où le Titulaire ne dispose pas d'un SI conforme aux exigences de l'II901 pour le traitement des informations « Diffusion Restreinte ». Les prescriptions de sécurité relatives aux SI abritant des données sensibles non classifiées (Chapitre 2) sont applicables.

Les grands principes sont les suivants :

3.2.1 En général, conséquence du principe du besoin d'en connaître, le Titulaire est amené à dédier un système d'information à l'exécution du marché. Il doit alors être un système de classe 2 isolé de l'Internet.

3.2.2 Dans le cas d'entreprises possédant un SI adapté à l'exécution de marchés sensibles ou classifiés, il est possible que la sécurité soit conforme aux objectifs des SI de classe 1 : dans ce cas, le Titulaire fournit la description précise du système et des conditions de traitement sur ce réseau des informations sensibles du marché.

3.2.3 Dans le cas où le Titulaire ne manipule pas ou très peu d'informations très sensibles au sens défini au §2, des solutions pragmatiques et de compromis qui maintiennent l'isolement de l'Internet de ces informations sont prises en accord avec le CEA/DAM. Elles ne peuvent être appliquées qu'après accord écrit du CEA.

3.2.4 Enfin il est des informations, en général créées par le Titulaire, qui ne bénéficient pas de mention protection pour des raisons techniques (codes automate, fichiers techniques ou de paramétrage, etc.). De même que précédemment, le Titulaire y applique des règles de protection adaptées prises en accord avec le CEA/DAM.

4 Les échanges d'informations entre le Titulaire et le CEA/DAM

L'exécution du marché implique des échanges d'informations entre le Titulaire du marché et le CEA/DAM. L'échange d'informations classifiées se fait en respectant les règles d'acheminement, marquage et traçabilité prescrites par l'IGI1300. L'échange de documents électroniques ne peut se faire que sur des supports classifiés dûment enregistrés ou éventuellement via des supports agréés (Globull).

Néanmoins, le suivi régulier du contrat peut impliquer l'échange d'informations non classifiées, et ce indépendamment de la classification générale du marché.

Sous réserve que le cumul des informations échangées au cours du temps ne relève pas de l'information classifiée, il est possible d'échanger de l'information en conteneur chiffré dans des conditions conformes à l'II901. Pour cela, le CEA/DAM exige l'utilisation de solutions de conteneurs chiffrés agréés dont la sécurité repose sur des conditions d'utilisation qui doivent être respectées.

Parmi les solutions agrées par l'ANSSI pour le transport de données sensibles, le CEA/DAM en a déployé deux sur ses postes de travail : ACID Cryptofiler et ZoneCentral et ses conteneurs associés Zed. Pour les échanges avec le CEA, le choix de la solution sera nécessairement entre ces deux possibilités. Pour les besoins propres du Titulaire, le choix de la solution devra se faire prioritairement entre ces deux possibilités, en concertation avec le CEA. L'adoption de toute autre solution agréée ANSSI nécessite un accord préalable du CEA.

Dans le cas de choix du logiciel ACID Cryptofiler comme solution pour le transport des données sensibles, une convention d'usage doit être établie. Celle-ci fait l'objet de l'annexe au présent document.

Les prescriptions pour les échanges d'informations sensibles non classifiées (Chapitre 3) sont applicables à tous les marchés sensibles ou classifiés dès lors que ceux-ci mettent en œuvre l'échange d'information de Diffusion Restreinte ou Confidentiel CEA.

5 Synthèse des principes applicables

Le tableau ci-dessous synthétise pour les différentes natures d'informations les règles applicables en termes de gestion sur le système d'information du Titulaire ou d'échange avec le CEA ou ses sous-traitants.

	Nature des informations		
	CD/SD	DR, Confidentiel CEA	Diffusion Ordinaire
SI du Titulaire	Selon IGI 1300	Chapitre 2(*)	Pas de dispositions particulières
Échange électronique des informations	Interdit	Chapitre 3(*)	Pas de dispositions particulières

(*) Dans la mesure où l'exécution du marché ne met en œuvre que quelques informations sensibles non classifiées, sur décision du CEA/DAM, les dispositions minimales suivantes peuvent être appliquées :

- Sur le SI du Titulaire, les données sont stockées sous forme chiffrée. Elles ne sont manipulées en clair que lorsque le SI est déconnecté physiquement de l'Internet.
- Les échanges d'informations sensibles sont réalisés sous forme chiffrée dans les conditions prescrites par ce document.

CHAPITRE 2 : PRESCRIPTIONS DE SECURITE DES SYSTEMES D'INFORMATION SENSIBLES

1 Objet

Le présent chapitre précise les exigences du CEA liées à la sécurité informatique dans les projets du CEA/DAM réalisés avec des partenaires industriels. Il précise les dispositions nécessaires à la protection des informations Diffusion Restreinte en application de l'IGI 1300 et de l'II 901. Il vient en application des obligations déclinées dans l'annexe de sécurité du marché, qui définit le niveau de classification du marché et la sensibilité de ses composantes informationnelles.

2 Terminologie

ACID	Logiciel de chiffrement de conteneurs
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASSI-C	Agent de Sécurité des Systèmes d'Information du Centre
ASSI-U	Agent de Sécurité des Systèmes d'Information d'Unité
CCEA	Confidentiel CEA (mention)
CD	Confidentiel Défense (mention)
CEA	Commissariat à l'Energie Atomique et aux énergies alternatives
DAM	Direction des Applications Militaires du CEA
DCS	Direction Centrale de la Sécurité du CEA
DO	Diffusion Ordinaire
DR	Diffusion Restreinte (mention)
GSM	Global System for Mobile communications (connexion téléphonie mobile)
PDA	Personal Digital Assistant (Assistant Personnel ou Ordinateur de Poche)
SD	Secret Défense
SSI	Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
USB	Universal Serial Bus
WIFI	Wireless Protocol Access (Accès réseau sans fil)
ZoneCentral	Logiciel de chiffrement de poste de travail
Zed	Conteneurs chiffrés
Zedle	Logiciel d'utilisation de conteneurs chiffrés, associé à ZoneCentral

3 Documents de référence

IGI 1300	Instruction Générale Interministérielle n°1300 sur la protection du secret de la défense nationale
II 920	Instruction Interministérielle n°920 relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel-défense
II 901	Instruction Interministérielle n° 901relative à la protection des systèmes d'information sensibles (réf. PRMD1503279J du 28/01/2015)
Guide ANSSI	Maitriser la SSI pour les systèmes industriels – juillet 2013
	Hygiène Informatique - janvier 2013

4 Intervenants & fonctions

Lors du début de l'exécution du marché, le Titulaire désignera un responsable d'exploitation du ou des SI concernés ainsi que le RSSI pertinent de l'entreprise. Le CEA indiquera l'ASSI du centre ainsi que l'ASSI d'Unité désigné pour encadrer l'application des prescriptions de sécurité informatique.

C'est cet ASSI de centre qui est à même de prescrire d'éventuelles dispositions particulières ; pour la délivrance de certificats nécessaires aux systèmes de chiffrement, il est autorité de certification du centre, il gère les certificats de chiffrement.

Le Titulaire désignera officiellement, au plus tard à la réunion de lancement ou d'enclenchement du marché, un RSSI.

5 Domaine d'application – Obligation de transfert

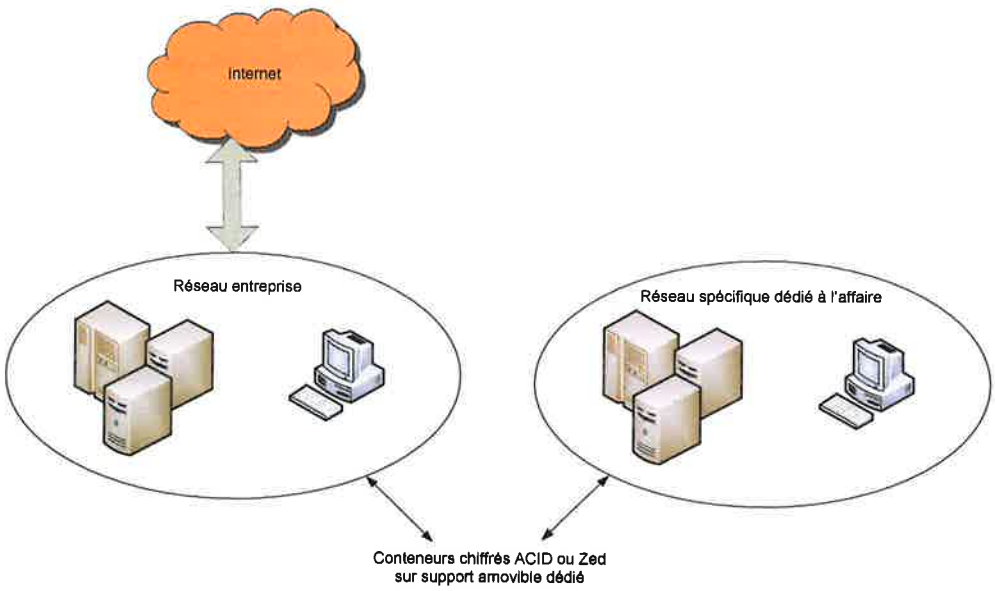
Ces dispositions s'appliquent aux informations sensibles telles que définies au chapitre I. Elles s'appliquent au Titulaire ainsi qu'à l'ensemble de son personnel amené à travailler sur l'affaire. Si le Titulaire a recours à des sous-traitants, il s'oblige à transférer l'ensemble des présentes dispositions à ses sous-traitants dans la mesure où ceux-ci ont connaissance et/ou transmission d'informations sensibles.

6 Réseau informatique spécifique

Dans le cas où le Titulaire possède un réseau d'entreprise qui lui est propre et qui est conforme aux exigences de l'II901 pour le traitement des informations « Diffusion Restreinte », les exigences du chapitre 6 ne s'appliquent pas, notamment l'isolement de l'Internet. Le Titulaire fournira, une description précise de ce système et des conditions de traitement sur ce réseau des informations sensibles qui font l'objet du marché. Cette description sera fournie de manière préliminaire dans l'offre du candidat puis de manière définitive dans ou en accompagnement des documents de gestion de projet (Plan d'Assurance Qualité, Plan de Management, ...).

Il est convenu entre le CEA et le Titulaire qu'aucun fichier sensible relatif à l'affaire ne sera implanté sur une machine (serveur, ordinateur portable, ordinateur individuel, PDA...) directement connectée avec internet et ce, quelle que soit la connexion (filaire, WIFI, GSM...). De ce fait, l'intégralité des fichiers correspondants sera implantée sur un système[2] physiquement déconnecté de l'Internet (directement et indirectement). Par la suite, ce système informatique dédié[3] à l'affaire sera dénommé « réseau spécifique ».

Le schéma ci-dessous représente la configuration autorisée par le CEA :



Le réseau spécifique du Titulaire est a minima de niveau Diffusion Restreinte, mais il est possible que, dans des cas exceptionnels, le Titulaire utilise un réseau classifié de défense qui lui est propre.

Quel que soit son statut et en complément des dispositions réglementaires applicables (IGI1300, II920, II901), le système informatique obéit aux règles suivantes :

---

[2] Dans certains cas, il peut s'agir d'une machine unique.
[3] Le réseau peut être utilisé pour d'autres affaires du CEA, sous réserve d'accord du CEA/DAM et des responsables CEA des affaires concernées.

- Toute connexion directe ou indirecte du réseau spécifique avec internet est strictement interdite.
- Toute connexion directe ou indirecte d'une ou plusieurs des stations de travail du réseau spécifique avec internet est strictement interdite.
- Les technologies de transmission sans fil sont interdites, de ce fait le réseau spécifique est constitué uniquement de liaisons filaires.
- Toute connexion d'un téléphone portable au réseau spécifique est interdite ; le raccordement d'équipements mobiles particuliers nécessaires à l'exécution du marché doit faire l'objet d'une analyse de sécurité.
- Le réseau spécifique doit être protégé par un antivirus et un anti-malware mis à jour régulièrement, au minimum de manière hebdomadaire.
- Une traçabilité des connexions, déconnexions (réussies et en échec) est mise en place, couvrant la durée de vie du système. Les traces système seront paramétrées (localement sur les postes de travail et/ou sur serveur d'authentification s'il y en a un) pour couvrir cette durée. L'intégrité des traces est confiée à la responsabilité de l'administrateur local.

L'utilisation de systèmes d'informations mobiles (téléphone portable, PDA, etc..) présente des risques (communication sans fil, capacité de stockage et traitement d'information, prises de vue), il revient au RSSI du Titulaire de sensibiliser ses utilisateurs, voire de mettre à disposition des consignes pour déposer ces appareils en dehors de la zone de travail du réseau spécifique.

6.1 Réseau spécifique diffusion restreinte

Pour la gestion d'informations sensibles non classifiées de défense (DR maximum), le Titulaire (personne morale) et son personnel participant à l'exécution du marché doivent avoir fait l'objet d'un contrôle élémentaire à la demande du CEA.

Le Titulaire met en place un réseau informatique spécifique DR.

Il est convenu entre les parties que le Titulaire est en charge dès le début de l'affaire de la conception, la fourniture et la mise en place du réseau spécifique, que cela concerne le software, le hardware, tous les périphériques (tels qu'imprimantes, traceurs, scanner, lecteurs divers, baies de brassage, switch, câbles, écrans...). Les conditions de réutilisation d'un SI préexistant sont soumises à la validation du CEA/DAM.

Le Titulaire est par ailleurs averti que l'intégralité des mémoires rémanentes qui auront été connectées au réseau spécifique (serveurs, stations de travail, imprimantes...) devra être remise au CEA en fin d'affaire. Dans certains cas, une attestation sur l'honneur d'effacement sécurisé des données de l'affaire peut être acceptée après accord du CEA sur la procédure d'effacement. La date de fin d'affaire est définie par le responsable CEA du contrat, en général quand les obligations de garantie ou de maintenance n'imposent pas au Titulaire une obligation de conservation des informations.

Une description conforme de l'organisation du réseau spécifique et la liste des serveurs, postes informatiques sur lesquels sont implantés les documents du projet et le logiciel de chiffrement sera remise par le Titulaire au démarrage de l'affaire. Le document est mis à jour lors de toute évolution significative du système (évolution matérielle ou changement dans les principes d'exploitation).

6.2 *Réseau spécifique classifié de défense (cas exceptionnel)*

Pour l'exploitation et l'utilisation de ce SI classifié de défense (CD ou SD), et conformément à l'IGI 1300, le Titulaire fait intervenir des personnels habilités, dispose de locaux dont une aptitude physique aura été délivrée par l'autorité compétente, et le SI aura fait l'objet d'une homologation.

Le réseau spécifique utilisé dans le cadre de l'affaire pourra être le réseau classifié du Titulaire suivant un accord explicite du CEA. Dans ce cas, le Titulaire s'organisera pour regrouper les données liées à l'affaire afin de pouvoir s'engager à les détruire[4] en fin d'affaire, sur demande explicite du responsable CEA du marché et de respecter le besoin d'en connaitre au sein du personnel du Titulaire. Dans tout autre cas, les exigences du paragraphe 6.1 sont applicables.

7 Les systèmes industriels

Les systèmes industriels (automates programmables industriels, déports d'entrées et sorties, réseaux de terrain, etc.) sont exposés à des risques de malveillance, à plus forte raison s'ils sont déployés sur des installations sensibles.

Dans le cadre de ses prestations, pendant les phases de conception, d'intégration et de maintenance des systèmes industriels, le Titulaire doit mettre en œuvre les bonnes pratiques[5] suivantes :

- Les développements doivent se faire sur le réseau spécifique.
- Le raccordement d'une machine (PC portable de maintenance) non dédiée à l'affaire (ou au CEA) est à proscrire. En cas de nécessité incontournable, les conditions d'utilisation d'un PC mutualisé sont précisées et validées par le CEA/DAM.
- Maîtriser les points d'accès physique qui permettraient de s'introduire dans le système. Les équipements concernés sont les serveurs, postes opérateurs, équipements réseau, automates, capteurs/actionneurs, écrans tactiles.
- Séparer les flux réseaux par des équipements dédiés ou des VLAN.
- Réduire les risques liés à l'utilisation de médias amovibles. Installer des machines dédiées aux transferts de données, désactiver les ports USB sur

[4] La procédure d'effacement sécurisé ainsi que les éventuels résidus dans les systèmes de sauvegarde sont soumis à l'acceptation du CEA.
[5] Se référer aux guides de l'ANSSI « Maitriser la SSI pour les systèmes industriels » et « Hygiène informatique ».

les systèmes, définir une politique d'utilisation des médias amovibles.

- Définir une politique de gestion des comptes utilisateurs et des comptes d'application. Ne pas laisser de compte par défaut (admin/admin par exemple), ne pas utiliser de compte générique, définir une robustesse et durée de vie des mots de passe éventuellement en accord avec les règles du CEA/DAM.
- N'installer que les logiciels, protocoles et services nécessaires. Désactiver les modes de configuration et de programmation à distance.
- Tracer les actions et les interventions de maintenance (journaux d'évènements et d'alarmes) afin de permettre de détecter des intrusions.
- S'assurer que les versions actives dans les équipements (version N) n'ont pas été modifiées, identifier et analyser les écarts des versions N et N-1 avant la mise en service de nouvelles versions.
- Définir et mettre en œuvre une politique de sauvegarde des données[6] (y compris les données des systèmes).
- Maitriser la documentation pour disposer d'une image exacte des installations et maitriser sa diffusion pour gérer le besoin d'en connaître.
- Protéger les équipements et applications contre les virus et malware. Définir et mettre en œuvre une politique antivirale.
- Définir et mettre en œuvre une politique de gestion des correctifs des systèmes d'exploitation, des applications, des firmwares (systématique, périodique ou ponctuelle, adaptée aux contraintes fonctionnelles et aux risques identifiés).
- Sécuriser l'accès aux automates. Les équipements sont dans des baies fermées à clef, les accès au code source et au code embarqué dans les automates sont protégés.
- Sécuriser les postes de développement et les consoles de programmation automates. Appliquer les correctifs, activer un antivirus. Dédier les machines au système concerné et tracer leur utilisation – à défaut, expliciter les conditions de mutualisation avec d'autres affaires ou projets.
- Maintenir à jour (et fournir à la livraison) le dossier du système : cartographie physique et réseau adressé, descriptif système, dossiers de fichiers et programmes applicatifs, liste des comptes, des services, des protocoles, des temps caractéristiques.

8 Gestion des supports amovibles

Dans le cadre de l'affaire, il s'agit de clefs USB[7], de CD-ROM ou de disques amovibles, a minima de niveau DR. Tous ces supports sont neufs, distincts des autres affaires et acceptés par le CEA avant usage. L'utilisation des supports amovibles DR est autorisée suivant les conditions suivantes :

- les supports sont parfaitement identifiés et tracés dans un registre,

[6] il peut s'agir par exemple des codes sources des applications, des bases de données, des journaux de supervision, des programmes des automates, des fichiers de configuration des équipements réseau, etc.
[7] Les clefs USB peuvent être interdites sur certains systèmes du CEA

- ils sont dédiés à l'affaire en cours,
- l'utilisation de clefs USB ne sert qu'à faire du transfert de fichiers DR chiffrés entre le réseau spécifique et le CEA via internet,
- les clefs USB ne sont pas utilisées pour faire du stockage ou de l'archivage de données,
- tous les fichiers de l'affaire contenant des informations sensibles, déposés sur ces supports, sont chiffrés avec le logiciel de chiffrement ACID ou ZoneCentral[8],
- il est toléré que des fichiers non sensibles (DO), tels que des fichiers constructeurs, soient non chiffrés,
- il est recommandé de procéder régulièrement à un effacement sécurisé[9] des clefs USB (par exemple, avec l'exécutable cipher fourni avec Windows),
- à la fin de la prestation et au plus tard à la fin des obligations du Titulaire, la totalité des supports amovibles est remise au CEA ; un procès-verbal sera alors adressé à l'ASSI-U de l'unité,
- l'utilisation de tout autre support amovible sur un poste informatique du réseau spécifique est strictement interdite.

La copie d'un fichier sensible de l'affaire sur un support amovible ne s'effectuera qu'après son chiffrement par ACID Cryptofiler ou Zed. Aucun fichier sensible de l'affaire non chiffré ne devra être placé sur un support amovible.

En fin d'affaire, les supports amovibles devenus inutiles ou périmés, seront détruits par le CEA ou le Titulaire selon les recommandations de l'IGI 1300. Un procès-verbal de destruction sera dressé par le CEA ou le Titulaire.

9 Gestion des comptes

Le RSSI du Titulaire assure que l'administration du SI est conforme aux bonnes pratiques de sécurité. A ce titre, il est notamment responsable de la gestion des comptes informatiques créés pour l'accès aux SI ou réseaux spécifiques.

En particulier : toute action sur le SI doit pouvoir être imputée à une personne. L'ouverture d'une session sur un réseau spécifique est donc impérativement nominative.

Les utilisateurs standards du SI ne doivent pas être en mesure de mettre en défaut l'intégrité système du SI ; ils ne doivent donc posséder aucun privilège administrateur.

Le RSSI du Titulaire tient à jour un registre listant les utilisateurs du SI, leurs profils d'accès (utilisateur standard, administrateur système, maintenancier…) et la justification du besoin d'accès privilégiés.

Au cas où le réseau spécifique se résume à une unique machine, le CEA préconise :
- que le système et les données soient placés dans deux partitions distinctes,
- que les utilisateurs standards ne puissent pas modifier le système,
- que les données soient accessibles aux seuls utilisateurs autorisés.

[8] Le CEA peut créer des conteneurs chiffrés avec le logiciel de chiffrement ZoneCentral (conteneurs Zed). Dans le cadre d'un marché, l'utilisation de conteneurs ACID est bien adaptée.
[9] Pour réellement supprimer les fichiers, il faut réécrire des données sur l'espace mémoire ou disque qu'ils occupaient, par « surcharge » de cet espace.

10 Sauvegardes

Les parties conviennent que, dans le cas d'un système dédié à la réalisation du contrat, une sauvegarde des données sera réalisée par le Titulaire et sous sa responsabilité. Le support de sauvegarde pourra être :

- des CD ROM ou DVD ROM : Ceux-ci devront alors être stockés dans une armoire fermée à clefs.
- des disques durs amovibles : Ceux-ci devront alors être stockés dans une armoire fermée à clefs.
- une ou plusieurs machines du réseau spécifique.

Les supports utilisés pour les sauvegardes sont identifiés et tracés dans un registre. Les supports de sauvegarde devront être remis au CEA en fin d'affaire.

11 Audits du CEA

Le CEA/DAM et son autorité de sécurité se réservent le droit de procéder ou de faire procéder à un ou plusieurs audits pour vérifier la bonne application des spécifications de la présente convention.

CHAPITRE 3 : PRESCRIPTIONS POUR LES ECHANGES D'INFORMATIONS SENSIBLES NON CLASSIFIEES

1 Objet

Le présent chapitre précise les exigences du CEA liées à la sécurité des échanges d'information dans les projets du CEA/DAM réalisés avec des partenaires industriels. Le présent document vient en application des obligations déclinées dans l'annexe de sécurité du marché, qui définit le niveau de classification du marché et la sensibilité de ses composantes informationnelles.

2 Terminologie

ACID	Logiciel de chiffrement de conteneurs
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASSI-C	Agent de Sécurité des Systèmes d'Information du Centre
ASSI-U	Agent de Sécurité des Systèmes d'Information d'Unité
CCEA	Confidentiel CEA (mention)
CD	Confidentiel Défense (mention)
CEA	Commissariat à l'Energie Atomique et aux énergies alternatives
DAM	Direction des Applications Militaires du CEA
DCS	Direction Centrale de la Sécurité du CEA
DO	Diffusion Ordinaire
DR	Diffusion Restreinte (mention)
GSM	Global System for Mobile communications (connexion téléphonie mobile)
PDA	Personal Digital Assistant (Assistant Personnel ou Ordinateur de Poche)
SD	Secret Défense
SSI	Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
USB	Universal Serial Bus
WIFI	Wireless Protocol Access (Accès réseau sans fil)
ZoneCentral	Logiciel de chiffrement de poste de travail
Zed	Conteneurs chiffrés
Zedle	Logiciel d'utilisation de conteneurs chiffrés, associé à ZoneCentral

3 Echanges avec le CEA

3.1 Messagerie électronique

Dans le cadre de l'exécution de l'affaire, les personnels du Titulaire et de ses sous-traitant éventuels sont amenés à communiquer par messagerie électronique entre eux, et avec les acteurs CEA du projet, des pièces jointes de niveau DR (sensible non classifié de défense). Ces pièces jointes doivent être transmises dans des conteneurs chiffrés avec le logiciel de chiffrement ACID Cryptofiler ou avec le logiciel de chiffrement ZoneCentral (conteneurs Zed).

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

La communication par messagerie électronique de pièces jointes de niveau classifiées de défense est interdite, même après chiffrement avec le logiciel ACID-Cryptofiler.

3.2 Réunion

Dans le cadre des réunions liées à l'affaire, la connexion d'un support amovible ou d'un ordinateur portable non CEA/DAM sur un réseau CEA/DAM est strictement interdite.

Pour les présentations en salles de réunion du CEA, le Titulaire peut venir avec son ordinateur portable professionnel[10] qui peut être connecté directement sur un vidéoprojecteur. A défaut, l'organisateur CEA de la réunion doit utiliser son ordinateur portable CEA pour projeter un document déposé sur le support amovible du Titulaire[11].

Les téléphones portables sont interdits dans les bâtiments du CEA/DAM[11]. Si la réunion a lieu en dehors du CEA/DAM et traite d'informations sensibles ou classifiées, le responsable CEA de la réunion peut interdire la présence de téléphone portable dans la salle ainsi que la prise de note sur support informatique ou papier.

3.3 Intervention

Dans le cadre des interventions liées à l'affaire, la connexion d'un support amovible ou d'un ordinateur portable non CEA/DAM sur un réseau CEA/DAM est interdite sauf nécessité impérieuse approuvée par le CEA/DAM.

Pour les opérations sur site en phase d'intégration des systèmes informatiques et industriels de l'affaire, le Titulaire doit prévoir les moyens matériels et logiciels qui devront rester sur site pendant la

[10] Pour rentrer du matériel (ordinateur ou support amovible) sur un centre CEA, une demande doit être faite auprès du responsable CEA du marché et validée par l'Officier de Sécurité du centre.
[11] Les téléphones doivent être déposés dans des casiers consigne à l'entrée des centres ou des bâtiments des centres CEA/DAM

durée des travaux. Il est admis qu'un support amovible[12] dédié à cette activité, jamais connecté à Internet et vérifié sain en usine, soit utilisé comme navette entre le réseau spécifique et l'installation sur site.

En prévision des activités MCO (Maintien en Condition Opérationnelle), le Titulaire doit définir la configuration informatique nécessaire pour disposer des moyens in-situ afin d'assurer la maintenance des systèmes informatiques et industriels livrés, sans devoir faire rentrer du matériel informatique non maitrisé par le CEA.

4 Logiciels de chiffrement de conteneur

Le CEA choisit le logiciel de chiffrement de conteneurs utilisé pour les échanges sensibles non classifiés entre le Titulaire et le CEA. Le choix de technologie est entre :

- Zed : ce sont des conteneurs chiffrés produits par les logiciels ZoneCentral et Zed dans leurs versions qualifiées par l'ANSSI. Si le Titulaire ne possède pas ces logiciels, le logiciel Zedle est mis à disposition gratuitement au Titulaire via un site Internet d'accès libre, avec un document du CEA qui en indique les modalités d'emploi. Le CEA choisit d'utiliser des clés délivrées gratuitement par l'infrastructure de gestion de clés du CEA ou un code d'accès par mot de passe défini en concertation avec le Titulaire et respectant les règles de constitution du CEA.

- ACID : ce sont des conteneurs chiffrés produits par le logiciel ACID Cryptofiler qui est un produit qualifié par l'ANSSI et de distribution contrôlée. Les clés sont fournies par le CEA ou, éventuellement par un organisme agréé pour la distribution de clés ACID du domaine cryptographique 'INDUS'. Si le Titulaire ne possède pas ce logiciel, il est mis à disposition du Titulaire par le CEA. Les prescriptions d'emploi qui en restreignent l'usage et la rétrodiffusion imposent l'établissement d'une convention cosignée entre le Titulaire[13] et le CEA.

Le Globull est un produit unique[14] agréé pour le transport d'information classifiée de défense de niveau CD ; il est donc apte à transporter des informations sensibles non classifiées. Le CEA ne fournit pas de Globull au Titulaire mais si celui-ci en dispose, il peut être utilisé comme support de transport pour des échanges. Le raccordement d'un Globull sur les SI du CEA se fait alors en accord avec les règles de cybersécurité en vigueur au CEA.

5 Audits du cea

Le CEA/DAM et l'autorité de sécurité du CEA se réservent le droit de procéder ou de faire procéder à un ou plusieurs audits pour vérifier la bonne application des spécifications de la présente prescription.

---

[12] Utiliser de préférence un CD ROM
[13] Si le Titulaire choisit d'utiliser la technologie ACID pour communiquer avec ses sous-traitants, une convention entre le CEA et chacun des sous-traitants du Titulaire devra être établie.
[14] Disque USB chiffré, produit par la société Bull.

CONVENTION D'USAGE DU LOGICIEL CE CHIFFREMENT ACID CRYPTOFILER

Le présent document constitue le protocole d'utilisation du logiciel de chiffrement ACID Cryptofiler, qui est la propriété de l'Etat et dont l'utilisation doit être limitée strictement aux échanges d'informations dans le cadre de la prestation. La duplication du programme d'installation et l'installation d'ACID doivent être limités aux besoins du Titulaire. La diffusion du programme d'installation est interdite et une extension du périmètre d'installation ne peut se faire qu'avec l'autorisation expresse de l'ASSI-C.

Pour le cadre de la présente convention, les intervenants désignés officiellement sont les suivants :

- pour le Titulaire :
  - Représentant de la société : M. _____
  - RSSI de la société : M. _____
- pour le CEA :
  - ASSI-C[15] du Centre CEA/DAM de M. _____
  - AAS-U de l'unité du Responsable CEA du marché M. _____
  - Responsable CEA du marché : M. _____

Le logiciel est mis à la disposition du Titulaire par le CEA dans le cadre strict de la prestation demandée. Il est installé sur les postes de travail informatiques du réseau spécifique à partir d'un CD-ROM d'installation fourni par l'ASSI-C du CEA. Ce support contient des prescriptions obligatoires d'installation et d'emploi.

Le RSSI du Titulaire assure la gestion du logiciel et des certificats, mis à disposition par le CEA. L'ASSI-U est son interlocuteur concernant toute question relative à la sécurité informatique.

Le Titulaire demande la création de certificats de clé privée/publique ACID[16] pour les personnes suivantes:

- M _____ M _____
- M _____ M _____
- M _____ M _____

Tout besoin supplémentaire est adressé à l'ASSI-C. La durée de vie des certificats étant limitée à un an, le renouvellement est aussi demandé autant que de besoin, à l'ASSI-C.

Un accusé de réception de certificats ACID est adressé à l'ASSI-C en retour.

---

[15] Le donneur d'ordre (responsable CEA du marché) est une unité hébergée sur le Centre DAM désigné au chapitre 5 ; c'est donc l'ASSI de ce centre qui est autorité de certification du Centre ; il gère les certificats nécessaires aux systèmes de chiffrement.

[16] Limiter le nombre de licences au juste besoin

Les certificats publics des différents acteurs CEA du projet seront mis à votre disposition afin de permettre d'envoyer les fichiers chiffrés :

- M _____
- M _____
- M _____

Les certificats privés sont confiés au personnel du Titulaire sous leur responsabilité. Ils ne doivent en aucun cas être archivés sur le poste de travail, mais sur un support amovible. L'ASSI-C doit être informé sans délai de toute compromission ou suspicion de compromission.

A la fin de la prestation et au plus tard à l'échéance du contrat, les différents certificats (privés et publics) sont détruits ; un procès-verbal est adressé l'ASSI-C. Le CD-ROM d'installation devra être restitué au CEA à la fin de l'affaire et tous les exemplaires existants, quel que soit leur support, devront être détruits.

Pour le CEA, le responsable CEA du marché Mme / M. _____ Le	Pour la société _____ Mme / M. _____ Le