CEA/DAM/DSID/SEAS
DO 1 16/01/26
26SSBD000001
diffusé le : 16/01/26

RAPPORT

CCTG

EXIGENCES SPECIFIQUES APPLICABLES AUX MARCHES INCLUANT UNE FOURNITURE OU UN SERVICE EN LIEN AVEC DE L'INFORMATIQUE, DU LOGICIEL OU DU CONTRÔLE-COMMANDE

Nombre de pages : 20

Le Chef de service EAS

Le 16/01/2026 à 14:04:23
SIGNOL Franck

Franck SIGNOL

CEA
Centre DAM Île-de-France – DSID
Bruyères-le-Châtel I 91297 Arpajon cedex
T. +33(0)1 69 26 79 50
Franck.signol@cea.fr
Établissement public à caractère industriel et commercial I RCS Paris B 775 685 019

Direction des applications militaires
Direction des Systèmes d'Information de la DAM
Service Exploitation et Architecture des Systèmes informatiques

FICHE DOCUMENTAIRE DAM

Identification du document				
Origine (affiliation) : **CEA/DSID/SEAS**			**Type de document** : **Rapport**	
Classif. : DO	**Sous-classif** : N/A	**N° réf.** : 01	**Date** : 16/01/2026	**CB GCAO (affixe)** : 26SSBD000001
Référence enregistrement :				
Auteur(s) : D'AGIER DE RUFOSSE Artus, SCHMIDT Gabrielle				
Objet : Rapport CCTG **EXIGENCES SPECIFIQUES APPLICABLES AUX MARCHES INCLUANT UNE FOURNITURE OU UN SERVICE EN LIEN AVEC DE L'INFORMATIQUE, DU LOGICIEL OU DU CONTRÔLE-COMMANDE**				
Résumé : Ce document décrit le **référentiel d'exigences informatiques de base** que le Titulaire doit respecter pour tout marché passé avec le CEA DAM, dès lors que le périmètre du marché inclut de la fourniture ou du service en lien avec de **l'informatique de quelque nature qu'elle soit (entreprise, industrielle, scientifique)**, du **logiciel**, de **l'automatisme** ou du **contrôle-commande**.				
Mots clés : **CCTG, Exigences informatiques, Référentiel, marchés informatiques**				

Transmission des connaissances		
Nom du projet : N/A	**Intérêt mémoire projet** : N/A	**Arborescence / classement mémoire projet** : N/A

Gestion du document	
Unité responsable de l'archivage DAM : CEA/DSID	**Exemplaire à conserver** : OUI
Rubrique du plan de classement (à remplir par le destinataire en cas de document papier) :	
Durée de conservation dans l'unité :	**Sort à l'issue de ce délai** *(une seule case à cocher)* : ☐ Transfert au BCA ☐ Élimination

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

TABLEAU DES EVOLUTIONS		
Version	**Motif et nature des évolutions**	**Date**
A	Création.	16/01/2026

ELABORATION DU DOCUMENT	
Rédacteur(s)	Artus D'AGIER DE RUFOSSE
Vérificateur(s) technique(s)	Franck SIGNOL
Vérificateur qualité	Anne-Laure GUELIN HOARAU

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

SOMMAIRE

1. OBJET DU DOCUMENT ET STRUCTURE 5
2. TERMINOLOGIE 5
2.1. Définitions 5
2.2. Glossaire 6
3. DOCUMENTS DE REFERENCES 6
4. EXIGENCES 7
4.1. Forme de la réponse aux exigences 7
4.2. Interlocuteur technique informatique 7
4.3. Gestion documentaire 8
4.4. Cartographie 8
4.5. Label et qualification de sécurité 9
4.6. Matériel informatique et approvisionnement 9
4.7. Socle informatique des postes et serveurs 10
4.8. Architecture et administration 10
4.9. Gestion des matériels embarquant des micrologiciels 11
4.10. Gestion des logiciels 13
4.11. Gestion des comptes et mots de passe 15
4.12. Sauvegarde et restauration 16
4.13. Processus de développement, déploiement et cycle de vie 16
4.14. Solutions de chiffrement 16
5. Annexe 1 : Synthèse des exigences et des livrables 18
6. DIFFUSION 20

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

1. OBJET DU DOCUMENT ET STRUCTURE

Ce document décrit le **référentiel d'exigences informatiques de base** que le Titulaire doit respecter pour tout marché passé avec le CEA DAM, dès lors que le périmètre du marché inclut de la fourniture ou du service en lien avec de **l'informatique de quelque nature qu'elle soit (entreprise, industrielle, scientifique)**, du **logiciel**, de **l'automatisme** ou du **contrôle-commande**.

Le prescripteur CEA peut compléter ce référentiel par des exigences informatiques et/ou cybersécurité liées à la classe de sensibilité, à la classification du système ou à une contrainte particulière.

Dans la suite du document les exigences que le Titulaire doit respecter sont numérotées E-XXXX et son présentées sous la forme suivante :

[E-ARCH0] Exemple d'exigence. Le Titulaire doit faire …

Ces exigences encadrées de bleu ne redétaillent pas forcément l'ensemble des attendus, le cas échéant elles se rapportent au(x) paragraphe(s) explicatifs positionnés avant ou après dans le chapitre.

Note : **Certaines exigences sont sur fond rouge**, comme ce présent paragraphe. Il s'agit des exigences plus structurantes, pour lesquelles **le Titulaire doit valider avec le CEA les choix retenus** par rapport à l'item précis.

2. TERMINOLOGIE

2.1. DÉFINITIONS

Titulaire : la personne morale à laquelle le CEA confie les prestations objet du marché.

Prescripteur (CEA) : point de contact CEA pour les aspects techniques du marché.

Système : on appelle le Système (avec une majuscule) l'ensemble technique et technologique qui constitue la solution informatisée dans son ensemble. Le Système peut être constitué de sous-ensembles. Le Système est un des produits livrables du marché.

Système industriel : Un système est dit « industriel » s'il regroupe tout ou partie des éléments suivants :

- Capteurs et élément d'acquisition ;
- Automates ;
- Supervision métier (*PCVue, Panorama*, etc.) ;
- Contrôle-commande ;
- Tous types d'équipements connectés par des protocoles informatiques (USB, Bluetooth, Wifi, Ethernet, etc.) ; par exemple, il peut s'agir de caméra, d'équipements de téléphonie ou de sonorisation ;
- Tout appareil de mesure embarquant un système d'exploitation.

Logiciel Métier : Logiciel spécialisé dans un ou plusieurs domaines précis : supervision, pilotage, acquisition, calcul, gestion, etc.

Micrologiciel : Logiciel intégré dans un composant matériel. Le Micrologiciel (firmware) se situe entre le matériel (hardware) et les logiciels « haut niveau » (software).

Station blanche CEA : poste informatique CEA dédié au transfert sécurisé et à l'analyse de supports de stockages amovibles.

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

2.2. GLOSSAIRE

C	
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CPE	Common Plateform Enumeration
CPU	Central Processing Unit
G	
GMSA	Group managed service account – compte de service administré dans Windows
L	
LOG	Journal
M	
MCO	Maintien en Conditions Opérationnelles
R	
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
S	
SSI	Sécurité des systèmes d'information

3. DOCUMENTS DE REFERENCES

Les documents suivants sont appelés au cours du document.

	Intitulé	Référence
[DR1]	Conditions générales d'achat du CEA	Edition de Janvier 2022 (téléchargeable sur le site web du CEA cea.fr)

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

4. EXIGENCES

Les exigences informatiques et SSI sont regroupées par thématique au sein des paragraphes suivants du présent chapitre. Les thématiques sont les suivantes :

- Forme de la réponse aux exigences (E-FORM)
- Interlocuteur technique informatique (E-INT)
- Gestion documentaire (E-DOC)
- Cartographie (E-CART)
- Label et qualification de sécurité (E-QUAL)
- Matériel informatique et approvisionnement (E-MAT)
- Socle informatique des postes et serveurs (E-PDT)
- Architecture et administration (E-ARCH)
- Gestion des matériels embarquant un micrologiciel (firmware) (E-FIRM)
- Gestion des logiciels (E-LOGI)
- Gestion des comptes et mots de passe (E-MDP)
- Sauvegarde et restauration (E-SVG)
- Processus de développement, déploiement et cycle de vie (E-DVP)
- Solutions de chiffrement (E-CHIF)

4.1. FORME DE LA RÉPONSE AUX EXIGENCES

Le Titulaire fournit la **Matrice de réponse aux exigences**, document sous forme de tableau qui décrit pour chacune des exigences du présent document la prise en compte ou non, et le cas échéant la manière ou les mesures compensatoires proposées.

[E-FORM1] Le Titulaire rédige et fournit la Matrice de réponse aux exigences

4.2. INTERLOCUTEUR TECHNIQUE INFORMATIQUE

Le Titulaire **désigne un interlocuteur** dédié aux échanges avec le correspondant informatique du CEA, qui possède les compétences requises en système d'information au sens large. Selon le périmètre technique du marché et des choix technologiques proposés par le Titulaire, des compétences avancées complémentaires sont nécessaires pour un dialogue efficace avec le CEA. Le Titulaire s'engage par ailleurs à assurer la suppléance et la continuité de la fonction sur la durée du marché.

[E-INT1] Le Titulaire désigne un interlocuteur dédié aux échanges informatiques avec le CEA, et assure la continuité de la fonction sur la durée du marché.

[E-INT2] Le Titulaire s'assure de la compétence technique de l'interlocuteur au regard des technologies objet du marché

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

4.3. GESTION DOCUMENTAIRE

De manière générale toute la **documentation du Système doit être tenue à jour** lors d'évolution, et ce sur toute la durée du marché. La documentation englobe la cartographie complète (cf. §4.4 suivant), le catalogue méthodique, mais aussi tout document demandé à travers les exigences du présent document et dans le cadre du marché (les cahiers de recette, procédures d'installation, procédures de sauvegarde, etc.).

[E-DOC1] Le Titulaire tient à jour la documentation du Système tout au long du marché.

4.4. CARTOGRAPHIE

Le Titulaire fournit une **cartographie complète** du système. Le Titulaire doit fournir un inventaire précis des matériels, logiciels ainsi que la cartographie de tous les éléments informatiques du système (tout élément contenant une mémoire informatique y compris amovible).

La cartographie comprend à minima :

- La vision de **l'infrastructure technique** :
  - Le schéma physique représentant le positionnement des dispositifs (automates, systèmes de gestion, etc.) ;
  - Le schéma réseau physique (équipements réseau, types d'interconnexions)
  - Le schéma réseau logique (représentant les sous-réseaux logiques, les fonctions de routage et de filtrage, le cloisonnement logique opéré) ;
  - Le plan d'adressage IP (Les adresses IP de chaque équipement)
  - La matrice de flux (représentant les flux réseau) :
    - Source : nom d'hôte et/ou adresse IP / rôle fonctionnel ;
    - Destination : nom d'hôte et/ou adresse IP / rôle fonctionnel ;
    - Protocole : Protocole de transport (niveau 4) et port associé + nom du protocole de niveau 7 le cas échéant ;
    - Description : Identification de la fonction associée au flux.
  - Le document décrivant la liste complète des équipements physiques utilisés, incluant leur code CPE.
- La vision **applicative** :
  - Le schéma de principe des interactions au niveau applicatif ;
  - Le document décrivant les composants logiciels, incluant leur code CPE, ainsi que les flux de données entre ces composants (base de données comprises);
  - Document répertoriant les périmètres et niveaux de privilèges des comptes utilisateurs et des comptes administrateurs.
- La vision pour **l'exploitation et le MCO** du système :
  - Liste des différents scénarios possibles d'interaction entre les intervenants et les équipements informatiques du système
    - **Exemple :** fiche d'exploitation ou maintenance qui décriront les opérations effectuées sur les éléments informatiques (gammes de maintenances)
    - **Exemple :** traçabilité des logiciels ou équipements informatiques mis à jour/remplacés lors d'une maintenance sur un équipement.

[E-CART1] Le Titulaire fournit la cartographie complète du système

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

4.5. LABEL ET QUALIFICATION DE SÉCURITÉ

Le Titulaire **privilégie l'utilisation de produits qualifiés par l'ANSSI** (visas ou certifications), dans le respect d'un compromis raisonnable entre coût et performance par rapport au besoin technique.

[E-QUAL1] **Le Titulaire privilégie des produits qualifiés ANSSI**

4.6. MATÉRIEL INFORMATIQUE ET APPROVISIONNEMENT

Tout poste informatique physique (y compris portable pour la maintenance), matériel d'affichage (écran, vidéoprojecteur, …) et élément constituant l'informatique (commutateur réseau, etc. - hors matériel très spécifique) est **soit fourni par le CEA**, **soit validé par le CEA**. Si l'acquisition du matériel est réalisée par le Titulaire, le CEA sera indiqué comme propriétaire du matériel et des licences associées, ainsi que comme organisme couvert par la garantie et la maintenance. Si le matériel est fourni par le CEA, le Titulaire fournit la liste complète des prérequis matériels minimaux (CPU, RAM, etc.), ainsi que les procédures nécessaires à l'installation, le paramétrage, l'exploitation et la maintenance du système.

[E-MAT1] **Les ressources informatiques (ordinateurs, commutateurs, routeurs, etc.) sont soit de fourniture CEA, soit validées par le CEA**

[E-MAT2] **Le CEA doit être indiqué comme propriétaire des matériels au regard des licences, garanties et maintenances**

[E-MAT3] **Si le matériel est de fourniture CEA, le Titulaire indique les prérequis matériels minimaux (RAM, CPU, etc.) et fournit les procédures d'installation.**

Avant toute installation sur site CEA, **tous les équipements doivent être blanchis** suivant un protocole à définir avec le CEA. A minima il faudra réinstaller le micrologiciel des matériels avec la dernière version à jour fournie par le constructeur, en cohérence avec ce qui a été testé sur les différentes plateformes.

[E-MAT4] **Les matériels sont blanchis et réinstallés avant installation sur site CEA**

Une fois le Système sur site CEA, **les périphériques amovibles** (media USB, carte SD, …) **sont de fourniture CEA**, sur besoin avéré et justifié par le Titulaire. Ils sont clairement identifiés par un marquage visible, leur utilisation est tracée et limitée au juste besoin. Ils sont dédiés au système et ne se connecteront à aucun élément extérieur à celui-ci, à l'exception de la station blanche CEA.

[E-MAT5] **Les périphériques amovibles (clef USB, etc.) sont fournis par le CEA et dédiés au Système une fois installé sur site CEA. Le Titulaire ne les connecte pas sur d'autres éléments extérieurs au système.**

Les matériels fournis ne doivent pas contenir de modules ou composants permettant des **communications sans-fil**. Si de tels matériels n'existent pas au regard d'une contrainte opérationnelle dûment justifiée par le Titulaire, les fonctionnalités sans-fil sont démontés, désinstallés ou désactivées sur les matériels concernés, et la procédure de désactivation est fournie.

[E-MAT6] **Le Titulaire doit proposer des équipements ne présentant pas de modules d'émission/réception sans-fil**

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-MAT7] Dans le cas contraire, le Titulaire démontre l'impossibilité de [E-MAT6], désactive les fonctionnalités et fournit la procédure de désactivation.

Les matériels doivent être **doubles-alimentés électriquement**. Cette exigence s'applique aux équipements actifs réseau, serveurs, ordinateurs et automates. Les impossibilités techniques doivent être justifiés. Le cas échéant, le Titulaire propose une mesure compensatoire (commutateur de transfert statique rackable par exemple).

[E-MAT8] Le Titulaire propose des matériels double-alimentés électriquement

4.7. SOCLE INFORMATIQUE DES POSTES ET SERVEURS

Les logiciels métiers du système **doivent pouvoir s'intégrer dans l'écosystème CEA** (socle logiciel) suivant :

- Systèmes d'exploitation Windows (version courante à jour au CEA) ou RHEL (version courante à jour au CEA) pour les postes de travail ou les ordinateurs portables de maintenance, et Windows Server (version courante à jour au CEA) ou RHEL (version courante à jour au CEA) pour les serveurs ;
- Navigateur web Microsoft Edge ou Mozilla Firefox (versions courantes à jour au CEA) ;
- Postes et serveurs munis des fonctions suivantes :
    - Un pare-feu réseau local avec liste blanche
    - Le blocage logique des ports entrée/sortie
    - La remontée des évènements vers un collecteur (Log)
    - Un antivirus qui est géré par le CEA et qui reçoit la politique de sécurité du réseau d'accueil
    - Un logiciel de restriction applicative
    - Un écran de veille transparent si besoin (pour les postes de travail).

[E-PDT1] Le Titulaire conçoit le système pour qu'il s'intègre dans le socle informatique du CEA

Les logiciels métiers **doivent pouvoir supporter la réalisation de mises à jour du système d'exploitation**. Une procédure de mise en maintenance applicative (arrêt éventuel de services applicatifs, …), une procédure de validation de bon fonctionnement après mise à jour, et un bordereau de livraison concernant le contenu des versions évolutives/correctives (changelog) doivent être fournies.

[E-PDT2] Les logiciels métiers doivent supporter les mises à jour du système d'exploitation.

[E-PDT3] Le Titulaire fournit les procédures de mise en maintenance des applications, de validation post-mise à jour et le bordereau de livraison des versions

4.8. ARCHITECTURE ET ADMINISTRATION

L'architecture générale du système, en particulier de toute la composante informatique, **doit être validée par le CEA**. Le Titulaire produit pour cela en amont un schéma d'architecture générale.

[E-ARCH1] Le Titulaire fournit un schéma d'architecture informatique générale du système pour validation par le CEA

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

L'administration des équipements du système doit pouvoir se faire de deux manières, **localement** aux équipements, mais aussi à distance **via des stations dédiées à l'administration** cloisonnées et filtrées du reste du système (sous-réseau distinct). Les équipements installés doivent être compatibles avec cette architecture et ce mode de fonctionnement.

[E-ARCH2] Le Titulaire prévoit les deux modes d'administration (local et distant)

[E-ARCH3] Le Titulaire prend en compte la contrainte de stations cloisonnées et dédiées à l'administration du système

Le système ne doit pas être connecté à Internet. Il doit pouvoir fonctionner de manière « off-line » sans aucun lien Internet y compris de manière ponctuelle.

[E-ARCH4] Le Titulaire prend en compte la contrainte du mode de fonctionnement du système sans connexion Internet

Dans le cas où une ou plusieurs bases de données sont déployées, tous les accès, hors gestes d'administration du SGBD effectués par un administrateur, doivent se faire via un applicatif dédié (frontal web par exemple). Les flux réseau à destination du serveur de bases de données seront donc fermés, à l'exception de ceux provenant du serveur applicatif (serveur web ou logiciel serveur par exemple).

[E-ARCH5] Le Titulaire prend en compte la restriction d'accès aux bases de données

4.9. GESTION DES MATÉRIELS EMBARQUANT DES MICROLOGICIELS

Les exigences du présent paragraphe s'appliquent aux matériels équipés de micrologiciels.

[E-FIRM1] Le Titulaire doit fournir les procédures de mise à jour des micrologiciels inclus dans les matériels livrés (hors fourniture CEA).

Les équipements doivent pouvoir être **administrés depuis un système d'information CEA** à travers une connexion distante.

[E-FIRM2] Les équipements doivent être administrables à distance dans le respect de l'exigence [E-ARCH3] et [E-MAT6].

Les interfaces d'administration web, y compris web services, **doivent être désactivées**, sauf contrainte opérationnelle validée avec le CEA (par exemple absence d'autre solution d'administration à distance). La méthode de désactivation est fournie, ainsi que la liste des équipements possédant ce type d'interface.

[E-FIRM3] Sauf besoin opérationnel dûment justifié, le Titulaire désactive les interfaces d'administration web

[E-FIRM4] Le Titulaire fournit le mode opératoire ainsi que la liste des équipements concernés par la désactivation des interfaces d'administration web

De la même manière, les **interfaces matérielles** (USB, Ethernet, fibre, …) **non utilisées doivent être désactivées**, et la méthode de désactivation/réactivation est documentée.

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-FIRM5] **Le Titulaire désactive les interfaces matérielles non utilisées**

[E-FIRM6] **Le Titulaire fournit le mode opératoire ainsi que la liste des équipements concernés par la désactivation des interfaces matérielles**

Les équipements fournis par le Titulaire doivent préférentiellement pouvoir transmettre des **journaux** (système, sécurité, etc.) **au format *syslog***.

[E-FIRM7] **Le Titulaire doit privilégier l'usage d'équipements qui peuvent transmettre leurs journaux à un serveur au format *syslog*.**

Les équipements installés doivent pouvoir employer des **protocoles sécurisés** (protocole avec chiffrement et authentification des pairs - ssh, ftps, https, etc.). Les matériels proposant des protocoles non-sécurisées (rsh, telnet, ftp, http, tout protocole non chiffré, etc.) sont interdits. Si de tels matériels n'existent pas au regard d'une contrainte opérationnelle dûment justifiée par le Titulaire, les protocoles non-sécurisés sont désactivés sur les matériels concernés, et la procédure de désactivation est fournie.

[E-FIRM8] **Le Titulaire doit proposer des équipements ne présentant que des protocoles sécurisés**

[E-FIRM9] **Dans le cas contraire, le Titulaire démontre l'impossibilité de [E-FIRM8], désactive les protocoles non-sécurisés et fournit la procédure de désactivation.**

Si une **fonction de télémaintenance ou de télédiagnostique** est intégrée par défaut sur des équipements approvisionnés par le Titulaire, elle doit être désactivée. La méthode de désactivation est fournie.

[E-FIRM10] **Le Titulaire identifie les matériels disposant de fonctions de télémaintenance et/ou télédiagnostique et désactive la fonction.**

[E-FIRM11] **Le Titulaire fournit le mode opératoire de la désactivation des fonctions de télémaintenance et/ou télédiagnostique**

Dans le cas où les équipements embarquent des **certificats tiers**, leur remplacement est à effectuer par le Titulaire. La méthode de remplacement est fournie.

[E-FIRM12] **Le Titulaire remplace les certificats tiers présents par défaut sur les équipements**

[E-FIRM13] **Le Titulaire fournit la méthode de remplacement des certificats**

De manière générale, les fonctionnalités ou services inutilisés sur les équipements sont désactivés. La méthodologie de désactivation est documentée et fournie par le Titulaire.

[E-FIRM14] **Les fonctionnalités ou services inutilisés sont désactivés.**

[E-FIRM15] **Le Titulaire fournit la méthode de désactivation**

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

4.10. GESTION DES LOGICIELS

Hormis les logiciels métiers, les logiciels (systèmes d'exploitation, logiciels de bureautique, systèmes de gestion de base de données, service web …) sont soit **fournis par le CEA**, **soit validés par le CEA**.

[E-LOGI1] Les logiciels sont soit de fourniture CEA, soit validés par le CEA

Si l'acquisition d'un logiciel est réalisée par le Titulaire, ce dernier **déclare l'origine du logiciel** (production propre, ou logiciel tiers de quel éditeur, etc.), fournit les **sources d'installation** et les **procédures d'installation** (y compris la procédure de génération du code exécutable) et de paramétrage pas à pas, afin que l'installation soit reproductible dans l'environnement de production. En outre, **le CEA est indiqué comme propriétaire des licences**, ainsi que comme organisme couvert par la garantie et la maintenance. A défaut, un transfert de propriété est prévu au moment de la livraison. Les licences doivent être fournies sous format logiciel, les *dongles* matériels sont interdits.

[E-LOGI2] Le Titulaire fournit les sources d'installation des logiciels qui sont de sa fourniture

[E-LOGI3] Le Titulaire fournit les procédures d'installation des logiciels

[E-LOGI4] Le Titulaire indique le CEA comme propriétaire des licences lors de l'acquisition, à défaut il prévoit un transfert de propriété

[E-LOGI5] Le Titulaire fournit des licences au format logiciel (pas de *dongle* physique)

En complément de [E-ARCH4], l'installation des logiciels doit pouvoir s'effectuer via des installeurs « off-line », autosuffisants et qui ne nécessitent **pas de recours à une connexion Internet**, même ponctuelle. La gestion des mises à jour, la gestion et l'activation des licences, et le fonctionnement du système doivent pouvoir se faire sur un réseau fermé sans accès à Internet, même ponctuel.

[E-LOGI6] Le Titulaire prend en compte la contrainte « off-line » et déconnecté d'Internet dans le choix, l'installation et le cycle de vie de ses logiciels.

Les logiciels ne doivent envoyer aucune donnée sur Internet. A défaut, ils doivent pouvoir être paramétrés pour désactiver de façon permanente tout envoi. L'ensemble des procédures de désactivation des envois doit être documenté et fourni.

[E-LOGI7] Le Titulaire prend en compte la contrainte liée au renvoi des données sur Internet

[E-LOGI8] Le Titulaire fournit la méthode de désactivation des renvois de données vers Internet le cas échéant

Seuls les logiciels strictement nécessaires au bon fonctionnement du système en production sont installés dans l'environnement de production. La liste exhaustive (incluant le nom, l'éditeur, les versions, le chemin d'installation et le nom de l'exécutable) de ces logiciels est fournie.

[E-LOGI9] Le Titulaire n'installe que les logiciels nécessaires au bon fonctionnement du Système

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-LOGI10] Le Titulaire fournit la liste exhaustive des logiciels installés

Les logiciels doivent pouvoir se lancer et fonctionner de manière nominale dans un **contexte utilisateur sans privilèges d'administration**.

[E-LOGI11] Le Titulaire propose des logiciels fonctionnant en contexte simple utilisateur

Les logiciels doivent être compatibles avec une **authentification utilisateur via SSO** (Single Sign-On) de type Kerberos, ou avec un protocole de fédération d'identité type SAML. Les requêtes LDAP ne sont pas considérées comme du SSO.

[E-LOGI12] Le Titulaire propose des logiciels compatibles avec le SSO

Si le logiciel requiert l'utilisation de **comptes de service**, le logiciel prendra en charge les comptes managés de type GMSA.

[E-LOGI13] Le Titulaire propose des logiciels compatibles GMSA

Le Titulaire doit s'assurer de **l'intégrité des logiciels et des programmes lors des téléchargements**. Il vérifie la correspondance entre la signature des logiciels et des programmes calculée lors du téléchargement et la signature fournie par l'éditeur ou le constructeur.

[E-LOGI14] Le Titulaire s'assure de l'intégrité des logiciels et des programmes lors des téléchargements en vérifiant les signatures

L'intégralité des micrologiciels, logiciels et données doit passer par une station blanche CEA avant leur intégration dans l'environnement de production. Cette exigence s'applique également en plateforme d'intégration sur site CEA.

[E-LOGI15] Le Titulaire fait passer les micrologiciels, logiciels et données par la station blanche CEA

Les logiciels et bibliothèques utilisés **doivent être maintenus par l'éditeur**, au moment de la mise en production, en cohérence avec ce qui a été testé sur les différentes plateformes.

[E-LOGI16] Le Titulaire maintient à jour les logiciels jusqu'à la mise en production et sur toute la durée du marché

Les **fonctionnalités de développement**, de débogage et de tests sont **désactivées dans l'environnement de production**.

Les outils de développement pour l'intégration et la maintenance corrective ou évolutive des logiciels ou matériels de la solution doivent être isolés de l'environnement de production. Ils sont utilisables sur des **stations CEA dédiées à ces actions**, en dehors de l'environnement de production.

[E-LOGI17] Le Titulaire désactive les fonctions de développement, de débogage et de test dans l'environnement de production

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-LOGI18] Le Titulaire prévoit des stations dédiées au développement situées en dehors de l'environnement de production

Les logiciels et les programmes pour lesquels il n'existe pas de contrat entre l'éditeur et le Titulaire et/ou le CEA (par exemple les logiciels *Open Source* ou logiciel gratuit) doivent être fournis sous la forme de code source et recompilés sur site. La procédure de compilation, les sources et l'origine de ces sources sont fournies.

[E-LOGI19] Le Titulaire doit recompiler sur site tout logiciel produit par le Titulaire, Open Source ou gratuit

[E-LOGI20] Le Titulaire fournit la procédure, les sources et l'origine des logiciels et des programmes

4.11. GESTION DES COMPTES ET MOTS DE PASSE

Les **comptes par défaut** de tous les composants du Système (applications, serveurs, équipements réseaux, équipements industriels (incluant caméra et élément de téléphonie), etc.) doivent être désactivés. La méthode de désactivation est documentée.

Les **mots de passe par défaut** associés à ces comptes doivent être listés et la méthode pour les modifier doit être fournie.

[E-MDP1] Le Titulaire désactive les comptes par défaut sur les équipements et applications

[E-MDP2] Le Titulaire fournit la procédure de désactivation des comptes par défaut

[E-MDP3] Le Titulaire fournit la liste des mots de passe par défaut et la méthode de désactivation

Une **matrice des comptes informatiques** et leurs privilèges doit être fournie pour chaque profil y compris sur les équipements bas niveau d'informatique industrielle. Les profils peuvent être des profils applicatifs spécifiques (par exemple administrateur applicatif, maintenancier, exploitant, …).

[E-MDP4] Le Titulaire fournit la matrice des comptes informatiques

Le Titulaire n'a **aucun droit d'administration informatique dans l'environnement de production**, que ce soit pendant la phase d'intégration ou après. Les gestes nécessitant des privilèges d'administration informatique sont réalisés par le CEA, en suivant les procédures fournies par le Titulaire.

[E-MDP5] Le Titulaire ne dispose pas de droit d'administration dans l'environnement de production

Aucun mot de passe ne doit être stocké en clair ou sous forme de hash (md5, sha1, etc.) sur le système. Si une contrainte opérationnelle ou technique dûment justifiée nécessite le stockage de mots de passe, ils doivent être stockés **sous forme chiffrée à l'état de l'art**.

[E-MDP6] Le Titulaire prend en compte la contrainte du stockage des mots de passe sur le Système

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

4.12. SAUVEGARDE ET RESTAURATION

Le Titulaire doit décrire les **processus de sauvegarde** de tous les équipements et configurations essentiels au fonctionnement nominal du système, y compris des bases de données, ainsi que la procédure de restauration. Avant la mise en production, il est demandé au Titulaire de tester la restauration « from scratch » des éléments du système, avec les procédures en question, en présence du CEA.

[E-SVG1] Le Titulaire décrit les processus de sauvegardes et de restauration mis en place.

4.13. PROCESSUS DE DÉVELOPPEMENT, DÉPLOIEMENT ET CYCLE DE VIE

Le Titulaire confirme avec le CEA le besoin d'une **plateforme de développement** / qualification / préproduction, et ses conditions de réalisation (fourniture des matériels, logiciels, et lieu d'implantation).

[E-DVP1] Le Titulaire demande confirmation au CEA quant au besoin d'une plateforme et ses conditions de réalisation

En particulier si des installations ou des développements sont réalisés chez le Titulaire, tous les matériels (jusqu'au plus bas niveau du système) et logiciels doivent être réinstallés une fois livrés sur site CEA.

[E-DVP2] Le Titulaire prend en compte la contrainte de réinstaller sur site CEA tout ce qui est installé ou développé en externe CEA

Le Titulaire doit fournir les dossiers de recette (vérifications, plan de tests, etc.) afin de n'omettre aucune étape pour **valider le bon fonctionnement de l'ensemble** y compris la surveillance, la sauvegarde du système et sa restauration en cas d'incident. Il est en charge de valider ces dossiers avec le CEA.

[E-DVP3] Le Titulaire fournit les dossiers de recette du système

Le Titulaire fournit un document **Plan de gestion de l'obsolescence**. Ce document contient, pour chaque composant de la solution, les éléments suivants :

- date de fin de commercialisation
- date de fin de support constructeur (et date de fin de support étendu, le cas échéant)

Le Titulaire veille à proposer des composants suffisamment récents et pérennes (c'est à dire maintenus par le constructeur ou l'éditeur sur la durée du marché a minima).

[E-DVP4] Le Titulaire propose des composants récents et pérennes.

[E-DVP5] Le Titulaire fournit le Plan de gestion de l'Obsolescence.

4.14. SOLUTIONS DE CHIFFREMENT

Toute solution de chiffrement proposée doit être préalablement **validée par le CEA**. La solution livrée ne doit pas contenir de solutions cryptographiques (authentification et chiffrement) propriétaires. Les solutions de chiffrement utilisées par le logiciel doivent être à jour et conformes à l'état de l'art.

[E-CHIF1] Le Titulaire valide avec le CEA les solutions de chiffrement qu'il propose. Elles doivent être à jour, et ne pas contenir de solution cryptographique propriétaire.

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

Le Titulaire doit fournir la **liste des fonctionnalités cryptographiques** (chiffrement, authentification) présentes sur chaque composant du système.

[E-CHIF2] **Le Titulaire fournit la liste des fonctionnalités cryptographiques pour chaque composant**

Aucun certificat auto-signé ne devra être utilisé le cas échéant. Tout certificat doit être remplaçable et la méthode de remplacement est fournie.

[E-CHIF3] **Le Titulaire n'emploie pas de certificat auto-signé.**

[E-CHIF4] **Le Titulaire fournit la méthode de remplacement des certificats**

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

5. ANNEXE 1 : SYNTHÈSE DES EXIGENCES ET DES LIVRABLES

[E-ARCH0] Exemple d'exigence. Le Titulaire doit faire ….5

[E-FORM1] Le Titulaire rédige et fournit la Matrice de réponse aux exigences.7

[E-INT1] Le Titulaire désigne un interlocuteur dédié aux échanges informatiques avec le CEA, et assure la continuité de la fonction sur la durée du marché. .7

[E-INT2] Le Titulaire s'assure de la compétence technique informatique de l'interlocuteur au regard des technologies objet du marché 7

[E-DOC1] Le Titulaire tient à jour la documentation du Système tout au long du marché .7

[E-CART1] Le Titulaire fournit la cartographie du système .8

[E-QUAL1] Le Titulaire privilégie des produits qualifiés ANSSI.8

[E-MAT1] Les ressources informatiques (ordinateurs, commutateurs, routeurs, etc.) sont soit de fourniture CEA, soit validées par le CEA .9

[E-MAT2] Le CEA doit être indiqué comme propriétaire des matériels au regard des licences, garanties et maintenances ..9

[E-MAT3] Si le matériel est de fourniture CEA, le Titulaire indique les prérequis matériels minimaux (RAM, CPU, etc.) et fournit les procédures d'installation.9

[E-MAT4] Les matériels sont blanchis et réinstallés avant installation sur site CEA.9

[E-MAT5] Les périphériques amovibles (clef USB, etc.) sont fournis par le CEA et dédiés au système. Le Titulaire ne les connecte pas sur d'autres éléments extérieurs au système. .9

[E-MAT6] Le Titulaire doit proposer des équipements ne présentant pas de modules d'émission/réception sans-fil .9

[E-MAT7] Dans le cas contraire, le Titulaire démontre l'impossibilité de [E-MAT6], désactive les fonctionnalités et fournit la procédure de désactivation. .9

[E-MAT8] Le Titulaire propose des matériels double-alimentés électriquement .9

[E-PDT1] Le Titulaire conçoit le système pour qu'il s'intègre dans le socle informatique du CEA .10

[E-PDT2] Les logiciels métiers doivent supporter les mises à jour du système d'exploitation.10

[E-PDT3] Le Titulaire fournit les procédures de mise en maintenance des applications, de validation post-mise à jour et le bordereau de livraison des versions .10

[E-ARCH1] Le Titulaire fournit un schéma d'architecture informatique générale du système .10

[E-ARCH2] Le Titulaire valide avec le CEA l'architecture informatique générale du système.10

[E-ARCH3] Le Titulaire prévoit les deux modes d'administration (local et distant).10

[E-ARCH4] Le Titulaire prend en compte la contrainte de stations cloisonnées et dédiées à l'administration du système .10

[E-ARCH5] Le Titulaire prend en compte la restriction d'accès aux bases de données.11

[E-FIRM1] Le Titulaire doit fournir les procédures de mise à jour des micrologiciels inclus dans les matériels livrés (hors fourniture CEA). .11

[E-FIRM2] Les équipements doivent être administrables à distance dans le respect de l'exigence [E-ARCH4] et [E-MAT6].11

[E-FIRM3] Sauf besoin opérationnel dûment justifié, le Titulaire désactive les interfaces d'administration web .11

[E-FIRM4] Le Titulaire fournit le mode opératoire ainsi que la liste des équipements concernés par la désactivation des interfaces d'administration web.11

[E-FIRM5] Le Titulaire désactive les interfaces matérielles non utilisées.11

[E-FIRM6] Le Titulaire fournit le mode opératoire ainsi que la liste des équipements concernés par la désactivation des interfaces matérielles .11

[E-FIRM7] Le Titulaire doit privilégier l'usage d'équipements qui peuvent transmettre leurs journaux à un serveur au format syslog. 11

[E-FIRM8] Le Titulaire doit proposer des équipements ne présentant que des protocoles sécurisés .12

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-FIRM9] Dans le cas contraire, le Titulaire démontre l'impossibilité de [E-FIRM8], désactive les protocoles non-sécurisés et fournit la procédure de désactivation. 12

[E-FIRM10] Le Titulaire identifie les matériels disposant de fonctions de télémaintenance et/ou télédiagnostique et désactive la fonction. 12

[E-FIRM11] Le Titulaire fournit le mode opératoire de la désactivation des fonctions de télémaintenance et/ou télédiagnostique 12

[E-FIRM12] Le Titulaire remplace les certificats tiers présents par défaut sur les équipements 12

[E-FIRM13] Le Titulaire fournit la méthode de remplacement des certificats 12

[E-FIRM14] Les fonctionnalités ou services inutilisés sont désactivés. 12

[E-FIRM15] Le Titulaire fournit la méthode de désactivation 12

[E-LOGI1] Les logiciels sont soit de fourniture CEA, soit validés par le CEA 12

[E-LOGI2] Le Titulaire fournit les sources d'installation des logiciels qui sont de sa fourniture 13

[E-LOGI3] Le Titulaire fournit les procédures d'installation des logiciels 13

[E-LOGI4] Le Titulaire indique le CEA comme propriétaire des licences lors de l'acquisition, à défaut il prévoit un transfert de propriété 13

[E-LOGI5] Le Titulaire fournit des licences au format logiciel (pas de dongle physique) 13

[E-LOGI6] Le Titulaire n'installe que les logiciels nécessaires au bon fonctionnement du Système 13

[E-LOGI7] Le Titulaire fournit la liste exhaustive des logiciels installés 13

[E-LOGI8] Le Titulaire propose des logiciels fonctionnant en contexte simple utilisateur 13

[E-LOGI9] Le Titulaire propose des logiciels compatibles avec le SSO 14

[E-LOGI10] Le Titulaire propose des logiciels compatibles GMSA 14

[E-LOGI11] Le Titulaire s'assure de l'intégrité des logiciels et des programmes lors des téléchargements en vérifiant les signatures 14

[E-LOGI12] Le Titulaire fait passer les micrologiciels, logiciels et données par la station blanche CEA 14

[E-LOGI13] Le Titulaire maintient à jour les logiciels jusqu'à la mise en production 14

[E-LOGI14] Le Titulaire désactive les fonctions de développement, de débogage et de test dans l'environnement de production 14

[E-LOGI15] Le Titulaire prévoit des stations dédiées au développement situées en dehors de l'environnement de production.. 14

[E-LOGI16] Le Titulaire doit recompiler sur site tout logiciel Open Source ou gratuit 14

[E-LOGI17] Le Titulaire fournit la procédure, les sources et l'origine des logiciels et des programmes 15

[E-MDP1] Le Titulaire désactive les comptes par défaut sur les équipements et applications 15

[E-MDP2] Le Titulaire fournit la procédure de désactivation des comptes par défaut 15

[E-MDP3] Le Titulaire fournit la liste des mots de passe par défaut et la méthode de désactivation 15

[E-MDP4] Le Titulaire fournit la matrice des comptes informatiques 15

[E-MDP5] Le Titulaire ne dispose pas de droit d'administration dans l'environnement de production 15

[E-MDP6] Le Titulaire prend en compte la contrainte du stockage des mots de passe sur le Système 15

[E-SVG1] Le Titulaire décrit les processus de sauvegardes et de restauration mis en place 15

[E-DVP1] Le Titulaire confirme avec le CEA le besoin d'une plateforme et ses conditions de réalisation 16

[E-DVP2] Le Titulaire prend en compte la contrainte de réinstaller sur site CEA tout ce qui est installé ou développé en externe CEA 16

[E-DVP3] Le Titulaire fournit les dossiers de recette du système 16

[E-DVP4] Le Titulaire propose des composants récents et pérennes. 16

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation

[E-DVP5] Le Titulaire fournit le Plan de gestion de l'Obsolescence. 16

[E-CHIF1] Le Titulaire valide avec le CEA les solutions de chiffrement qu'il propose. Elles doivent être à jour, et ne pas contenir de solution cryptographique propriétaire....16

[E-CHIF2] Le Titulaire fournit la liste des fonctionnalités cryptographiques pour chaque composant 16

[E-CHIF3] Le Titulaire n'emploie pas de certificat auto-signé. 16

[E-CHIF4] Le Titulaire fournit la méthode de remplacement des certificats....17

6. DIFFUSION

CEA/DIF/ED

CEA/LR/DIR

CEA/CESTA/DIR

CEA/CEG/DIR

CEA/VA/DIR

CEA/DAM/DAN

CEA/DAM/DMSI

CEA/DAM/DSNP

CEA/DAM/DPN

CEA/DAM/DRH

CEA/DAM/DCG

CEA/DAM/DQSCG

CEA/DAM/DS

CEA/DAM/DSID

Chrono

Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué sans son autorisation