



CEA/CESTA/DIR/ASSI

DO 8 19/11/12



diffusé le : 19/11/12

**PROCEDURE DE TRAITEMENT DE L'ANNEXE  
RELATIVE A L'ENTREE ET A LA SORTIE DU  
CEA/CESTA DE MATERIEL A MEMOIRE  
REMANENTE**

	RÉDACTEURS	VERIFICATEURS		ÉMETTEUR
NOM	M. Guidon Th. Falgon	R. Kiesser	M. Sabine	J.-P. Giannini
FONCTION	ASSI CESTA DLP/ASSI	Officier de Sécurité du CESTA	Assistant Qualité CESTA	Directeur
DATE				
VISA				

SUIVI DES MODIFICATIONS		
ÉDITION	Nature des modifications	Date
A	Émission initiale	19/11/12

## SOMMAIRE

<b>1.....</b>	<b>DOMAINE D'APPLICATION</b>	<b>4</b>
<b>2.....</b>	<b>GLOSSAIRE</b>	<b>4</b>
<b>3.....</b>	<b>REFERENTIEL DOCUMENTAIRE</b>	<b>5</b>
3.1.	DOCUMENTS DE REFERENCE .....	5
3.2.	DOCUMENTS APPLICABLES .....	5
<b>4.....</b>	<b>REGLES FONDAMENTALES</b>	<b>5</b>
<b>5.....</b>	<b>TYPE D'INFORMATION CONTENUE SUR LES MEMOIRES REMANENTES</b>	<b>5</b>
5.1.	DONNEES APPARTENANT AU PATRIMOINE SCIENTIFIQUE ET TECHNIQUE DU CEA ...	5
5.2.	DONNEES D'ETALONNAGE, DE REGLAGE .....	6
5.3.	DONNEES SYSTEME STANDARDS .....	6
<b>6.....</b>	<b>TYPE D'INTERVENTION NECESSITANT LA SORTIE D'UN EQUIPEMENT</b>	<b>6</b>
6.1.	UTILISATION A L'EXTERIEUR POUR BESOIN PROFESSIONNEL .....	6
6.2.	UTILISATION A L'EXTERIEUR POUR BESOIN PERSONNEL .....	7
6.3.	PRESTATION DE MAINTENANCE .....	7
6.4.	PRET DU MATERIEL POUR REALISATION D'UNE PRESTATION .....	7
6.5.	MATERIEL DECLARE A DOUBLE EMPLOI « CIVIL/DEFENSE » .....	8
<b>7.....</b>	<b>OPERATIONS REALISABLES SUR LES MEMOIRES REMANENTES</b>	<b>8</b>
7.1.	ECHANGE AVEC UNE MEMOIRE NEUVE OU VIDE .....	8
7.2.	DONNEES RELATIVES AU PATRIMOINE SCIENTIFIQUE ET TECHNIQUE DU CEA.....	8
7.3.	EFFACEMENT SECURISE .....	8
7.4.	ARCHIVE SUR SUPPORT NON REINSCRIPTIBLE .....	9
7.5.	REALISATION D'UNE LISTE DES FICHIERS CONTENUS SUR LA MEMOIRE .....	9
7.6.	SAUVEGARDE DES FICHIERS MODIFIES.....	9
<b>ANNEXE A.</b>		<b>11</b>
<b>ANNEXE B.</b>		<b>13</b>

## 0. Objet

Ce document définit la procédure à appliquer par les salariés CEA ou par les employés d'entreprises extérieures, **en complément de la procédure [R2]**, pour réaliser la sortie du site puis éventuellement le retour sur le site de matériels ayant une mémoire rémanente, appartenant au CEA dont le CEA/CESTA est détenteur.

## 1. Domaine d'application

La présente procédure s'applique à tous les matériels à mémoire rémanente implantés dans les installations des sites du CESTA et du TEE.

Le terme matériel désigne les matériels, y compris les ESM, les matériaux, outils, instruments, emballages et objets divers présents dans les installations du CEA/CESTA.

Le terme mémoire rémanente désigne, par sa définition, tout matériel capable de retenir toute information (*par exemple, les mémoires USB, les disques durs externes, Cdrom, DVD, appareil de mesure de type multimètre, ...*).

Sont exclus du champ d'application de la présente procédure :

- les matériels classifiés qui doivent être traités suivant le référentiel documentaire en vigueur disponible auprès de l'Officier de Sécurité du CESTA,
- les matériels dits sensibles (matières dangereuses, éléments d'armes, ...) dont la sortie du Centre et le transport sont traités dans « l'instruction particulière pour l'organisation et la réalisation des transports sensibles effectués au profit des unités du CESTA » (SYM R0705 ZAL INQ 97000968),
- les matériels appartenant à des entreprises extérieures ou à des visiteurs.

La gestion des matériels (sortie définitive, sortie temporaire, prêt à un agent pour une durée déterminée, prévision de l'éventuel retour sur le Centre, ...) est sous la responsabilité du CI détenteur. Cette gestion sort du cadre de la présente procédure.

## 2. Glossaire

ASI	Administrateur de Sécurité Informatique
ASSI	Agent de Sécurité des Systèmes d'Information Centre
ASSI-U	Agent de Sécurité des Systèmes d'Information Unité
CEA	Commissariat à l'Energie Atomique
CESTA	Centre d'Etudes Scientifiques et Techniques d'Aquitaine
CI	Chef d'Installation
DAM	Direction des Applications Militaires
Demandeur	Salarié CEA à l'origine de la demande de sortie de l'équipement
DO	Diffusion Ordinaire
DR	Diffusion Restreinte
ESM	Equipement de Surveillance et de Mesure
PV	Procès Verbal

### 3. Référentiel Documentaire

#### 3.1. Documents de référence

- [R1] Règlement intérieur CEA/CESTA
- [R2] Procédure générale de sortie et de retour de matériels du CEA/CESTA
- [R3] Manuel de Management du CESTA (version en vigueur sur l'intranet)

#### 3.2. Documents Applicables

Sans objet

### 4. Règles Fondamentales

Une mémoire qui est connectée au CEA/CESTA à un système DAM, reste la propriété de la DAM. Sauf cas traités par la suite, elle ne sort plus du centre. Sa fin de vie se traduit par sa destruction physique.

Avant tout transfert (ou utilisation), l'innocuité de la mémoire est vérifiée. Un contrôle antiviral est accompli avec un fichier de définition de virus à jour (de l'ordre de la semaine, dans tous les cas inférieur à 1 mois).

Si cette mémoire a été détenue par une société contractante avant d'être la propriété du CEA/CESTA, cette mémoire est conservée par l'ASSI-U afin de pouvoir contrôler son innocuité au cas d'apparition d'un programme malveillant.

Autant que possible, un clone de la mémoire d'un équipement devant stocker des données sensibles, est réalisé avant toute utilisation.

### 5. Type d'information contenue sur les mémoires rémanentes

Il faut distinguer les différents types d'informations pouvant être enregistrées sur les mémoires rémanentes. Suivant le type de ces informations, les procédures de sortie et d'entrée sont différentes et s'adaptent à la protection de la confidentialité pour la sortie et à la protection de la disponibilité et de l'intégrité pour l'entrée.

*Rappel : les équipements ayant hébergé des données classifiées, sont exclus de cette procédure.*

L'information peut être enregistrée sur une mémoire interne à un équipement ou sur un support amovible. Le traitement à réaliser sera identique quelque soit le support.

Le type d'intervention nécessitant l'utilisation de la mémoire définira les actions à effectuer sur la mémoire en fonction des types définis ci après.

#### 5.1. Données appartenant au patrimoine scientifique et technique du CEA

Cette catégorie regroupe les informations générées par l'utilisation de l'équipement dans les activités CEA.

Pour un instrument de mesure cela regroupe les données d'acquisition (temporaires, avant et après traitement, ..), les données de réglage dès lors qu'elles définissent certaines particularités d'utilisation.

Les fichiers de configuration d'un système intègrent également cette catégorie s'ils correspondent à une stratégie propre au CEA (compte et mot de passe utilisateur, configuration domaine, paramétrage réseau, ...).

Par nature, toutes ces données appartenant au patrimoine scientifique et technique, leur niveau de confidentialité est au minimum DR (sensible).

## **5.2. Données d'étalonnage, de réglage**

Cette catégorie regroupe les informations permettant de contrôler ou de régler un équipement afin de s'assurer de son bon fonctionnement.

Une mire de réglage, une acquisition de référence, une courbe d'étalonnage sont des données de cette catégorie.

La confidentialité de ces informations peut être de niveau DR (sensible) ou DO (ordinaire) sans toutefois être publique.

## **5.3. Données système standards**

Cette catégorie correspond aux informations contenues dans un équipement livré par le fournisseur à l'exclusion des données de la catégorie précédente (étalonnage et réglage) éventuellement présentes.

A l'exception des évolutions de version, ces informations sont communes aux équipements d'une même famille.

Ces informations n'ont pas de confidentialité. Elles sont publiques. Cependant, leur intégrité est indispensable pour garantir le fonctionnement correct de l'équipement.

# **6. Type d'intervention nécessitant la sortie d'un équipement**

Suivant le type d'intervention, les opérations à effectuer sur un équipement peuvent varier. Pour cela nous allons décrire les différents types d'interventions identifiées et décliner les gestes à réaliser.

## **6.1. Utilisation à l'extérieur pour besoin professionnel**

L'équipement est utilisé à l'extérieur pour une activité professionnelle. L'équipement reste sous la responsabilité d'un salarié CEA/DAM. L'utilisation par du personnel sous contrat de prestation ou de collaboration n'est pas totalement exclue.

Pour les besoins de l'intervention l'équipement peut être amené à être connecté à une installation ou un équipement n'appartenant pas au CEA/DAM.

Les informations nécessaires à l'intervention peuvent être des catégories suivantes : données système, données étalonnage et réglage, données du patrimoine scientifique et technique. Dans la mesure du possible, avant la sortie de la mémoire rémanente de l'équipement, les données du patrimoine scientifique et technique sont effacées. Dans tous les cas celles-ci sont limitées au juste nécessaire.

Pour la sortie il convient donc de s'affranchir des données inutiles. Le demandeur constituera un moyen pour préserver la liste des données d'étalonnage, de réglage ainsi que les données du patrimoine scientifique et technique placées sur la mémoire. Les données système publiques sont également totalement et parfaitement identifiées. Si la mémoire a contenu d'autres informations, les espaces libres sont effacés de manière sécurisée.

Au retour de l'équipement un test d'innocuité complet est effectué. Un comparatif des informations est réalisé entre la liste établie avant la sortie de l'équipement et celle après intervention à l'extérieur du CEA/CESTA. Un PV mentionnant les fichiers modifiés ou ajoutés doit être établi. Ces fichiers sont sauvegardés sur un support non réinscriptible afin de permettre des contrôles ultérieurs. Les espaces libres sont effacés de manière sécurisée.

## 6.2. Utilisation à l'extérieur pour besoin personnel

Ce type d'utilisation est soumis à l'autorisation du Chef de Département avec copie à la Direction du CEA/CESTA. Cette autorisation traite les aspects assurance en cas de bris ou de vol du matériel prêté.

Pour toute la durée du prêt, l'équipement reste sous l'entière responsabilité du salarié CEA/DAM sortant le matériel.

En aucun cas, l'équipement ne doit être connecté à un système extérieur n'appartenant pas au CEA/DAM. Le besoin d'une sortie d'information est à effectuer sur du matériel CEA, au plus tard au retour de l'équipement au CEA/CESTA.

L'équipement ne doit contenir aucune donnée du patrimoine scientifique et technique. Les données d'étalonnage et de réglage peuvent être préservées.

Pour la sortie il convient donc de s'affranchir des données inutiles. L'unité détentrice constituera un moyen pour préserver la liste des données d'étalonnage et de réglage placées dans la mémoire. Les données système publiques sont également totalement et parfaitement identifiées. Si la mémoire a contenu d'autres informations, les espaces libres sont effacés de manière sécurisée.

Au retour de l'équipement un test d'innocuité complet est effectué. Un différentiel des informations par rapport à la sortie est établi. Les informations introduites sont obligatoirement supprimées. Les espaces libres sont effacés de manière sécurisée. L'état de l'équipement est totalement identique à celui observé à son départ (à l'exclusion des différentes traces).

## 6.3. Prestation de maintenance

L'équipement doit subir une maintenance corrective ou évolutive. Cette maintenance concerne le système (évolution du logiciel fourni par le constructeur par exemple) ou le contrôle et la vérification de son fonctionnement (réglage et étalonnage). L'équipement est confié à du personnel extérieur sous contrat pour la prestation.

Le demandeur doit s'assurer que l'équipement concerné n'a pas hébergé de donnée classifiée. Dans ce cas, une autre procédure a été appliquée comme mentionné au § 1.

Pour les besoins de l'intervention, l'équipement peut être amené à être connecté à une installation ou un équipement n'appartenant pas au CEA/DAM.

Les informations nécessaires à l'intervention peuvent être des catégories suivantes : données système, données étalonnage et réglage. Les données du patrimoine scientifique et technique doivent être absentes.

Pour la sortie, il convient donc de s'affranchir des données inutiles. Le demandeur constituera un moyen pour préserver la liste des données d'étalonnage et de réglage placées dans la mémoire. Les données système publiques sont également totalement et parfaitement identifiées. Si la mémoire a contenu d'autres informations, les espaces libres sont effacés de manière sécurisée.

Au retour de l'équipement un test d'innocuité complet est effectué. Si l'intervention ne concerne que le réglage et l'étalonnage, un PV de fin de prestation établit les fichiers modifiés qui sont sauvegardés sur un support non réinscriptible afin de permettre des contrôles ultérieurs. Si l'intervention modifie de manière plus importante le contenu de la mémoire rémanente, l'ensemble de la mémoire doit être enregistrée sur un support non réinscriptible constituant ainsi le nouveau référentiel pour l'équipement. Dans tous les cas, les espaces libres sont effacés de manière sécurisée.

## 6.4. Prêt du matériel pour réalisation d'une prestation

Des spécificités ou des exigences particulières nécessitent que l'équipement soit prêté à une société extérieure dans le cadre d'un contrat ou d'une convention. Le CEA peut être amené à exprimer un certain nombre de contraintes, comme des règles de gestion, d'utilisation et/ou de protection.

Pour les besoins de l'intervention, l'équipement peut être amené à être connecté à une installation ou un équipement n'appartenant pas au CEA/DAM.

Dans la mesure du possible, les mémoires rémanentes sont neuves et ne contiennent aucune information. Il est admis que les équipements neufs livrés à la réception du CESTA ne contiennent pas d'information CEA. Il convient donc de favoriser l'utilisation de ce type de matériel dans le cadre de prêt afin de réduire les changements de mémoires rémanentes.

Si la catégorie de matériel ne permet pas d'utiliser des mémoires neuves, il sera nécessaire d'effectuer un effacement complet des mémoires. Enfin, si la prestation nécessite de garder certaines informations, celles-ci doivent être réduites au juste besoin et clairement identifiées avec leurs catégories.

A l'exception des mémoires neuves, pour la sortie il convient donc de supprimer les données inutiles. Le demandeur établira la liste des données persistant sur les mémoires. Les espaces libres sont effacés de manière sécurisée. Si possible une archive du contenu de la mémoire sur support non réinscriptible est effectuée.

Au retour, le matériel est remis dans l'état de sortie. L'archive effectuée lors de la sortie est privilégiée pour la remise en état. Dans le cas contraire, un test d'innocuité complet est effectué et les espaces libres sont effacés de manière sécurisée.

Si la prestation consiste à livrer certains éléments enregistrés dans les mémoires rémanentes, le passage à l'état initial est toujours obligatoire. Il est suivi par une procédure d'installation effectuant les modifications nécessaires. Cette procédure fait l'objet d'un PV de réception.

## **6.5. Matériel déclaré a double emploi « civil/defense »**

Des matériels sont jugés sensibles vis-à-vis de la prolifération (comme des FTD10000, IN7100).

Ainsi, ils doivent être protégés spécifiquement contre le vol ou la perte, quelle que soit le niveau de sensibilité des informations stockées.

Il faut donc tracer :

- le transfert de responsabilité entre le détenteur CEA et l'emprunteur extérieur,
- les mesures de protection mises en place pour ces matériels par l'emprunteur.

## **7. Opérations réalisables sur les mémoires rémanentes**

### **7.1. Echange avec une mémoire neuve ou vide**

L'échange de mémoire par une mémoire neuve ou vide est la solution à privilégier dans tous les cas.

Si la mémoire n'est plus dans son emballage d'origine scellé, il est nécessaire de vérifier si elle est vierge. Dans le cas contraire, il est nécessaire de procéder à son effacement sécurisé (cf. § ci-après).

Les données nécessaires à la prestation peuvent être copiées directement depuis une archive non réinscriptible (cf § ci-après).

L'échange de mémoire est obligatoire si la classification de la mémoire résidente est supérieure au niveau de classification de l'intervention.

### **7.2. Données relatives au patrimoine scientifique et technique du CEA**

Les données relatives à l'utilisation de l'équipement dans le domaine informatique CEA (telles que les mots de passe, etc...) doivent être remplacées par des données temporaires exportables auprès du prestataire.

Au retour du matériel, les données initiales seront restaurées.

### **7.3. Effacement sécurisé**



Cette opération est à effectuer, lorsque la mémoire utilisée (d'origine ou échangée pour l'intervention) a contenu ou a pu contenir des informations inutiles pour l'intervention.

Si cet effacement ne peut être effectué, cette exception doit être mentionnée dans le formulaire de sortie de l'équipement.

Dans le monde informatique Microsoft, lorsque la mémoire est totalement vide, le logiciel développé par DLG/STIA (SURCHARG) peut être utilisé. Si la mémoire n'est pas totalement vide, le logiciel CIPHER est préconisé.

Le logiciel LUKS peut être utilisé dans le monde Linux.

#### **7.4. Archive sur support non réinscriptible**

Une archive sur support non réinscriptible peut être générée à la réception d'un équipement. Elle pourra servir pour reconfigurer l'équipement avant et/ou après une intervention. Le même principe peut-être retenu au retour de l'équipement après l'intervention ayant nécessité sa sortie.

Si ce support n'a pas été créé à la réception de l'équipement, il peut être généré avant la sortie du matériel. Il sera utilisé pour disposer d'une référence permettant d'identifier les modifications ou de reconfigurer l'équipement à son retour.

La constitution d'archives sur supports non réinscriptible est à privilégier par rapport à la constitution de listes.

#### **7.5. Réalisation d'une liste des fichiers contenus sur la mémoire**

Lorsque les moyens ne permettent pas de créer un support non réinscriptible, la liste des fichiers enregistrés sur la mémoire doit être établie avant la sortie du matériel. Cette liste exhaustive et détaillée permet d'effectuer un contrôle au retour de l'équipement.

Pour certaines interventions, il est indispensable d'établir au retour de l'équipement la liste exhaustive et détaillée des fichiers enregistrés sur la mémoire. Cette liste est un moyen de contrôle et d'évaluation de l'équipement à son retour.

#### **7.6. Sauvegarde des fichiers modifiés**

La comparaison entre la liste précédente établie lors de la sortie de l'équipement et la liste des fichiers présents à son retour, permet d'identifier les fichiers modifiés ou ajoutés. Ces derniers sont alors sauvegardés sur un support non réinscriptible afin de permettre des contrôles ultérieurs.

# LOGIGRAMMES

Cas	Etape	Acteur	Libellé de l'opération	Appel à la procédure	Action au niveau du formulaire
Sortie	S1	Demandeur	Demande de sortie d'un équipement		formulaire D_Auto_Mat* formulaire C_D_Auto_Mat : cadres "Modèle concerné" "Motif de la demande" "Date limite souhaitée pour le retour"  Signature
	S2	Autorité	Validation Motif de la sortie	cf. § 6	Signature
	S3	ASSI-U	Définition des données Choix des opérations relatifs à la sortie et au retour	cf. § 5 cf. § 7	formulaire C_D_Auto_Mat : cadre "Avis ASSI-U"
	S4	ASSI-U ou prestataire	Réalisation des opérations relatifs à la sortie		Signature
	S5	ASSI	Vérification du respect de la procédure Avis sur les opérations préconisées		Signature
	S6	Demandeur	Sortie de l'équipement		
	S7	FLS	Contrôle des autorisations de sortie et des équipements		formulaire D_Auto_Mat : cadre "Sortie"
Entrée	E1	Demandeur**	Entrée de l'équipement		formulaires D_Auto_Mat & C_D_Auto_Mat précédemment renseignés
	E2	FLS	Contrôle de l'autorisation de sortie et des équipements		formulaire D_Auto_Mat : cadre "Entrée"
	E3	ASSI-U ou prestataire	Réalisation des opérations relatifs au retour Archivage de la liste et des supports	cf. S3 cf. § 7	Trace papier à joindre au formulaire
	E4	ASSI-U	Vérification du respect de la procédure		Archivage du formulaire et de la trace papier

\* : ce formulaire est attaché à la procédure amont de sortie de matériel (avec ou sans mémoire)

\*\* : Le demandeur n'est pas nécessairement la même personne que dans le circuit de sortie du matériel. Il doit nécessairement être un salarié CEA

**Formulaire d'autorisation  
d'entrée/sortie d'un système  
d'information**

# ANNEXE relative à la demande d'Autorisation d'Entrée-/Sortie, pour du MATÉRIEL CEA avec MEMOIRE REMANENTE

IDENTIFICATION DE L'UTILISATEUR

NOM	PRENOM	UNITE	Tel

CARACTÉRISTIQUES DES INFORMATIONS TRAITÉES

niveau SD	niveau CD	protégé (CD > DO)	niveau DO
Réseau X	Réseau RIG	Non connecté	CEANET
Réseau S	Non connecté		Non connecté
RTE			
Non connecté			
Autre réseau: _____	Autre réseau: _____	Autre réseau: _____	Autre réseau: _____

MATÉRIEL CONCERNE

CODE BARRE GDI (s'il existe)

MOTIF DE LA DEMANDE

--

AVIS DU ASSI-U

--

AVIS DE L'ASSI

--

VISAS

Utilisateur	Chef d'unité	ASSI-U	ASSI

Destinataires: chef d'unité, ASSI-U puis ASSI  
Etablissement public à caractère industriel et commercial  
R.C.S. - PARIS - B 775 685 019

## **Annexe B.**

# **Commandes à lancer dans le cas d'un équipement équipé d'un système d'exploitation Windows**

### **Avant la sortie de l'équipement**

« Démarrer »

« Exécuter »

Cmd

*Se positionner en tête de l'arborescence à contrôler*

Dir/s/b > etat\_avant.txt

### **Au retour de l'équipement**

Effectuer la même opération et sauvegarder le résultat dans le fichier etat\_retour.txt

Identifier les fichiers rajoutés

« Démarrer »

« Exécuter »

Cmd

*Mettre les 2 fichiers précités dans le même espace*

FC etat\_avant.txt etat\_retour.txt

Nota : vous pouvez obtenir de l'aide sur les options de la commande FC, en tapant « / ? »

Comparer les versions des fichiers, avant et après la sortie

C.E.A. - DAM

<b>1. Organisme Emetteur (*)</b> Centre : CESTA Direction : DAM Département : Service : Section :		<b>2. Classification (**): DO</b> <b>3. Référence à</b> E.P : Projet : Contrat :	
<b>IDENTITÉ DU DOCUMENT</b>			
<b>4. Nature</b>  Procédure	<b>5. Identification</b> Document secret      Autres documents DO		<b>6. Date</b>  19/03/2013
<b>7. Nbre de pages</b>  16			
<b>8. AUTEUR (S) : M. GUIDON – Th. FALGON</b>			
<b>9. TITRE : Procédure générale de sortie et de retour de matériels du CEA/CESTA.</b>			
<b>10. RÉSUMÉ</b>			
<b>11. DESCRIPTEUR (S) PROPOSÉ (S)</b>			
<b>Logistique, Matériel, Sécurité, Informatique</b>			
<b>Partie réservée au BCA et à ODIR</b>			
N° informatique :		N° du bulletin de résumés :	
		n° bobine	
Nature du mouvement :		Microfilm	
		n° dossier	
Diffusion Extérieure E - I			
<b>Code de classement</b>			

(\*) Sigles

(\*\*) Rayer la mention inutile

**LISTE DE DIFFUSION**

Destinataires		Nombre d'exemplaires	
Unité	Nom ou fonction	PJ	Ex.
CESTA/BCA			1
CESTA/DIR			1
CESTA/DAIA			1
CESTA/DLG			1
CESTA/DLP			1
CESTA/DSGA			1

**+ Tous les services + tous les labos + unités hébergées**