MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Référentiel d'exigences de sécurisation de livraison

-

Socle commun d'hygiène numérique de livraison
(Périmètre V1)

2022\CYBER\5\NP

Table des matières

1 Préambule

1.1 Principes et concepts

Ce document comprend un certain nombre d’exigences ayant pour but de réduire le risque cyber dans les phases de livraison des systèmes d’armes au MINARM et d’améliorer la protection des interfaces numériques correspondantes.

Ce référentiel comporte des règles d’hygiène numérique basées sur des solutions de cyber-sécurité déjà disponibles et/ou sur des solutions déjà mises en œuvre.

Ce référentiel sera mis à jour annuellement, revu progressivement en tenant compte de la spécificité des systèmes d’armes ainsi que de leurs processus de livraison et amélioré afin de tenir compte de l’évolution de la menace.

Les industriels se doivent d’appliquer au mieux les exigences transverses de ce référentiel.

Pour mémoire, le terme de **solution** employé dans le document correspond à l’ensemble des moyens techniques permettant d’assurer les contrôles de sécurité.

1.2 Enjeux et objectifs

L'objectif cible du document est de proposer des règles communes d'hygiène numérique de livraison.

A court terme, ce document propose un tronc commun (socle V1) de règles pour **un premier périmètre** qui s'attache à :

> Contrôler l'absence de malwares détectables par les outils du marché identifiés, dans les données transférées (1) et dans les équipements connectés, lors des phases d'intégration amont (2) ou de livraison (3) liées aux SA, sans impact majeur sur les processus concernés (4).
>
> (1) via supports IT ou transferts dématérialisés.
> (2) Phase d'intégration amont : moment où un composant pourrait être facilement analysable avant d'être « scellé » dans un ensemble appelé à être livré.
> (3) Phases de livraison : test, recette, livraison, mise à jour, MCO…
> (4) Les processus d'intégration et de livraison pendant lesquels auraient lieu les contrôles.

Pour rappel, le scénario de risque retenu pour le périmètre V1 est celui de la contamination d'un SI client, lors d'une livraison liée à un SA, par un malware qui aurait pu être détecté par un outil du marché lors de cette livraison.

1.3 Champ d'application

Le présent document s'applique à l'ensemble de leurs structures (personnel, moyens informatiques, organisation) impliquées dans les processus liés aux systèmes d'armes eux-mêmes ou liées aux systèmes d'information de leur écosystème numérique.

Pour en faciliter la prise en compte, s'approprier la démarche et en contrôler l'applicabilité, il appartient à chaque industriel de créer un référentiel, propre à sa société, (ou de modifier un document déjà existant) avec les exigences retenues.

Par définition, un système d'information **complexe** correspond à la combinaison de sous-systèmes dont certains peuvent être testés dans le périmètre V1. Cette complexité provient, soit de contraintes techniques, soit de la multiplicité des sous-systèmes inclus.

1.4 Rôles et responsabilités

Ce document rappelle les rôles fonctionnels possibles dans le cadre de l'application et du contrôle des règles. L'organisation définie et la nomenclature associée sont de la responsabilité de l'industriel. On trouve par exemple les rôles suivants :

- Les utilisateurs de la solution,
- Les administrateurs de la solution,
- Les responsables de la sortie ou de l'entrée du support physique ou numérique,
- Les exploitants / installateurs et mainteneurs de la solution (mise à jour, …),
- Les responsables des systèmes et moyens industriels,
- Les RSSI et OSSI,
- Les PSO…

2 Exigences de sécurité proposées

Définition : une **exigence** est un besoin identifié, formalisé au travers d'un **objectif** à atteindre pour lequel il est nécessaire de mettre en place **les mesures** adaptées.

Dans la suite du document, le terme **exigence** sous-entend le « couple » objectif associé / mesures à mettre en place pour l'atteindre.
Les exigences doivent être en accord avec le cadre du contrat en cours pour lequel la livraison du support s'effectue.

Ces exigences ne dispensent pas de l'application des mesures de sécurité standards et déjà en place pour les systèmes d'information (en particulier les équipements et postes bureautiques).

Les exigences sont identifiées par leur préfixe « **LIV xx** », numérotées par ordre d'apparition et sont ainsi formées :

LIV xx : Libellé de l'exigence
Objectif : visé

Mesure(s) : proposée(s) à titre d'illustration

Rappel / Note : facultatif

Des **mesures** sont proposées pour illustrer chaque **exigence**. Chaque industriel peut choisir de les utiliser ou pas ; chaque industriel met en œuvre celles qui lui permettent d'atteindre l'**objectif** visé.

2.1 Organisation et processus fonctionnels

Rappels :

- Le terme de livraison porte sur la livraison effectuée ou reçue ; on parlera donc de livraison au sens large pour les livraisons et les réceptions.
- Chaque acteur respecte le processus de livraison/réception et ne connecte pas un support informatique non préalablement contrôlé.

LIV 01 : Acteurs et gestion de la sécurisation des livraisons

Objectif : disposer d'une organisation et de procédures permettant la gestion de la sécurisation des livraisons.

Note : la sécurisation des livraisons correspond à toute la démarche qui concourt à mener à bien et à réduire le risque cyber pesant sur les livraisons (personnes, processus, outils et solutions, organisation, points de contrôle, …).

Mesures :

- La (ou les) procédure de contrôle des supports en entrée/sortie est écrite, diffusée et simple à appliquer.
- La procédure de contrôle des supports en entrée/sortie est maintenue périodiquement.
- L'organisation associée doit être décrite et connue par chacun des acteurs concernés (cf. §1.4).

LIV 02 : Gestion en cas de livraison/réception urgente

Objectif : en cas de livraison urgente disposer d'une procédure spécifique, pour laquelle le client a été averti.

Remarque : Une livraison urgente correspond à une livraison ne permettant pas le suivi du processus standard de livraison (cf LIV 01).

Mesures :

- La gestion d'une livraison à caractère urgent doit faire l'objet d'une procédure connue et accessible à tous les acteurs concernés et mettant en évidence les spécificités par rapport à une livraison « classique ».
- Le caractère d'urgence de la livraison ainsi que la gestion appropriée doivent être mentionnés explicitement dans le certificat d'innocuité.
- Les actions relatives au traitement d'une livraison urgente doivent être tracées.

Note : La procédure d'urgence ne doit pas permettre de contourner les exigences de base hors d'un contexte le justifiant clairement.

2.2 Processus opérationnels

LIV 03 : Mise en place de processus de contrôle opérationnels

Objectif : disposer d'un (ou plusieurs) processus de vérification de l'innocuité des livraisons.

Note : Plusieurs processus différents peuvent être proposés en fonction de la sensibilité ou du niveau de classification de la livraison. Il est impératif d'utiliser la solution dont le niveau de sensibilité correspond à celui des données hébergées sur le support à contrôler.

Mesures :

- L'industriel met à disposition des acteurs internes concernés une ou plusieurs solutions. Elles doivent être faciles à produire et à renseigner, accessibles et disponibles.
- Tous les utilisateurs doivent préalablement contrôler leurs supports amovibles ou extractibles avant toute insertion sur un équipement. Pour cela ils utilisent la solution mise à leur disposition.
- L'analyse sur une station blanche ne peut pas être réalisée si la date de mise à jour des bases antivirales de la station est supérieure à x jours (seuil fixé avec le client et/ou par le contrat).
- Un rapport doit pouvoir être généré et récupéré par l'utilisateur comme preuve de l'analyse effectuée. Il devra être explicite et compréhensible. Ce rapport fait apparaître *a minima* les différents champs listés au §2.4 (cf. LIV 10).
- Le rapport pourra se matérialiser sous forme d'un document signé via la clé ACID du responsable ayant validé le processus de vérification de l'innocuité.
- Une procédure/note désignant le responsable de la validation finale du rapport ou certificat doit être écrite : ce peut être par exemple
    - Soit le responsable métier du système d'information ou du moyen industriel contenant le support validé,
    - Soit le RSSI ou équivalent,
    - Soit le responsable de la sortie (contrôle de conformité) ou de l'entrée du support (contrôle réception).

LIV 04 : Mise à disposition de solutions techniques

Objectif : disposer de solutions techniques de vérification de l'innocuité des livraisons permettant d'analyser les supports avant livraison.

Notes :

- Plusieurs solutions peuvent être proposées en fonction de la sensibilité ou du niveau de classification de l'information objet de la livraison.
- Pour mémoire, l'exigence et les mesures associées s'appliquent au périmètre V1 défini au paragraphe §1.2.

Rappel : le principe de station blanche (ou station de décontamination) est fréquemment utilisé chez les industriels de défense ; il fait l'objet de règles de configuration et d'utilisation strictes.

Mesures :

- Des stations blanches sont mises à disposition des utilisateurs ; on peut trouver différents types de stations (postes fixes, kiosques, …) en fonction de la solution retenue par l'industriel.
- Pour les supports à contrôler qui sont non extractibles, une solution sous forme de clé antivirale (bootable ou non) est proposée.
- Une autre solution technique pourra être proposée.

LIV 05 : Mise à jour des outils et solutions mis à disposition (MCO, MCS)

Objectif : disposer d'outils mis à jour permettant de garantir la meilleure couverture de sécurisation.

Mesures :

- Une procédure décrivant l'installation, la configuration et le suivi des stations blanches doit être disponible pour les équipes d'administration et de gestion de ces stations.
- Les mises à jour pour les stations en réseau doivent être régulières (quotidiennes) et faire l'objet d'une procédure documentée.
- Un système de diode permettant de transférer les mises à jour de l'outil vers un réseau dédié « non connecté » peut être implémenté.
- Les mises à jour des stations isolées doivent faire l'objet d'une procédure documentée et remise au responsable de la station.

LIV 06 : Opérations de maintenance : Connexion d'un équipement au SI client

Objectif : disposer d'un équipement de maintenance dont l'innocuité a été vérifiée, ce dans les limites définies du périmètre en cours (Version 1) et au-delà des exigences client existantes.

Mesures :

- Les supports, reçus dans le cadre d'opérations de maintenance, sont autorisés à la connexion sous réserve d'un contrôle antiviral déjà mené par l'émetteur (fourniture du certificat valide) ou bien doivent faire l'objet d'un contrôle avant connexion mené par le personnel destinataire.
- Il convient d'éviter, en mettant en œuvre les meilleures pratiques de sécurisation, le risque de propagation virale lié à la connexion successive du même équipement de l'industriel à plusieurs SI client.
- En cas de découverte d'une infection sur l'équipement de l'industriel, ce dernier enregistre l''incident et prévient immédiatement le client final (afin que celui-ci prenne toutes les mesures qui s'imposent).

LIV 07 : Gestion des faux positifs et faux négatifs

Objectif : dérouler le contrôle selon un processus formalisé conforme au référentiel établi afin que les remontées et alertes soient présentes et justifiées dans le certificat d'innocuité.

Mesures :

- La gestion des faux positifs doit faire l'objet d'une procédure écrite.
- La détection de faux positifs doit être explicite dans le certificat d'innocuité.
- En cas de potentiel faux positif, l'utilisateur doit envoyer au SOC ou CERT le rapport d'analyse (sauvegardé sur un second media) pour demander une analyse plus approfondie par les équipes dédiées, pour décision.
- Dans l'attente du retour des équipes compétentes (support informatique, SOC, développement/ métier, RSSI), il ne faut pas connecter le support suspect.

Remarque et évolution : Il serait souhaitable de disposer d'une base de faux positifs régulièrement mise à jour aussi bien pour les fichiers ou logiciels COTS que pour les logiciels correspondant à des développements / traitements internes à l'industriel.

2.3 Moyens / Méthodes / Outils

LIV 08 : Centralisation et exploitation des rapports produits par les solutions

Objectif : assurer le stockage et l'intégrité des rapports produits par les outils et solutions (journaux, certificats d'innocuité) et être en capacité de les exploiter.

Mesures :

- L'ensemble des analyses doit être conservé et récupérable.
- Les historiques doivent être accessibles par le RSSI (ou équivalent) et inclure au minimum les critères suivants : Date d'analyse ; Nom du fichier détecté ; Nom du malware détecté.
- La durée de conservation des certificats et journaux doit être *a minima* d'un an après la livraison du SA – à défaut d'une durée spécifiée dans le contrat.

LIV 09 : Complémentarité des solutions de contrôle

Objectif : disposer de plusieurs solutions complémentaires afin d'optimiser la couverture, notamment pour celles reposant sur des bases de signatures.

Mesures :

- Les systèmes de lutte basés sur les signatures doivent utiliser au moins deux bases d'origines distinctes.

Remarque : Une station blanche embarque plusieurs solutions.

2.4 Formalisation du résultat

LIV 10 : Formalisation du certificat d'innocuité

Objectif : générer un certificat d'innocuité conforme, c'est-à-dire contenant les informations nécessaires minimales validées par le groupe de travail.

Note : Le certificat doit être valide et doit avoir été généré dans une fourchette de temps compatible avec la durée de validité correspondant à la contrainte du destinataire ou client final.

Mesures :

- Le certificat doit être facilement exportable et/ou imprimable.
- Le certificat est généré automatiquement par l'outil retenu par chaque industriel : toutes les informations attendues ne peuvent y apparaitre. La partie des justifications concernant les Faux Positifs et fichiers en erreur est à renseigner manuellement et est à joindre au CDIn.
- Le certificat doit comporter obligatoirement les champs détaillés ci-après, répartis en quatre thèmes :
    - Identification du CDIn
    - Outils et options
    - Eléments testés
    - Résultats détaillés.

Informations nécessaires minimales du CDIn (v1)

Identification du CDIn

- Nom de l'industriel ;
- Date et heure UTC de l'analyse (dates de début et de fin);
- Identifiant d'analyse (contenant le nom système de la machine) ;
- Statut global de l'analyse (comprenant le nombre de menaces):
    - OK [signifie support évalué comme sain]
    - Infecté
    - Avec suspicion [support avec fichiers suspects ou faux positifs à prendre en compte]
    - Avec erreur [avec fichiers en erreur car non contrôlés par l'outil]
- EN OPTION : Condensat du certificat d'innocuité.

Outils et options

- Nom des antivirus ; état des moteurs (version des moteurs, de la base virale, date de dernière mise à jour) retenus ;
- Options d'analyse retenues :
    - Quarantaine, suppression, archivage, … ;
    - Profondeur de l'analyse.

Eléments testés

- Identifiant technique du support analysé (ou numéro de série) ;
- Condensat global du contenu du support contrôlé;
- Taille contrôlée ;
- Nombre de fichiers analysés ;
- Si nombre de fichiers important, résultat du contrôle par partition ou système de fichiers ;
- EN OPTION : la liste totale des fichiers contrôlés du support ;
- EN OPTION : la liste totale des hashs des fichiers contrôlés.

Résultats détaillés

- Nombre et liste des fichiers en **erreur** (Jaune) (par exemple fichiers non contrôlés) ;
- Nombre et liste des fichiers **suspicieux**, potentiellement les faux positifs (orange) ;
- Nombre et liste des **infections** (rouge) supposées ;
- Pour chaque remontée, disposer du condensat du fichier et si possible de la justification remontée par l'antivirus ;
- **Important**, pour chaque remontée, disposer du chemin d'accès complet du fichier.

LIV 11 : Formalisation du dossier global d'attestations pour un système complexe

Objectif : Formaliser la notion de « dossier global d'attestations », des points de vue organisationnel et opérationnel, dossier regroupant les CDIn générés pour les sous-systèmes constituant le système complexe livré.

Mesures :

- Le dossier global regroupera plusieurs certificats d'innocuité correspondant aux différents sous-systèmes composant la livraison.

LIV 12 : Mise sous scellés du support contrôlé, à des fins de stockage et transport

Objectif : sceller le support contrôlé, physiquement ou logiquement, afin d'en maintenir l'intégrité lors de son stockage ou transport.

Mesures :

- A la fin du contrôle du support, celui-ci ainsi que le certificat d'innocuité produit sont introduits dans une enveloppe indéchirable ou un emballage scellé remis à la personne responsable du transfert vers le client final. Le contenant est décacheté en présence du transporteur par le client destinataire à la remise de la livraison.

2.5 Maîtrise du risque

LIV 13 : Communication et sensibilisation des utilisateurs

Objectif : porter à la connaissance de tous les acteurs les exigences techniques et organisationnelles en matière de livraison (organisation, processus, mesures, responsabilités, …)

Mesures :

- L'organisation (acteurs, rôles, responsabilités, prévention, récupération, procédures, …) doit être décrite, disponible et remise aux acteurs intéressés.
- Chaque utilisateur (utilisateur, prestataire, partenaire, mainteneur, …) doit être régulièrement sensibilisé.
- En cas de soupçon, l'utilisateur doit contacter au plus vite son correspondant sécurité.
- L'organisation en place doit être mise à jour régulièrement.

LIV 14 : Communication sur les moyens mis à disposition

Objectif : porter à la connaissance de tous les acteurs les exigences et outils à utiliser en matière de livraison, dans le cadre de ce référentiel.

Mesures :

- Chaque utilisateur (utilisateur, prestataire, partenaire, mainteneur, …) doit connaitre la localisation de l'outil ou solution qu'il peut être amené à utiliser. Pour ce faire, une liste des stations et outils et leur localisation doivent être disponibles.
- L'existence des solutions sous-entend l'adhésion de tous les utilisateurs à la démarche.

3 Synthèse des exigences

LIV 01 : Acteurs et gestion de la sécurisation des livraisons

LIV 02 : Gestion en cas de livraison/réception urgente

LIV 03 : Mise en place de processus de contrôle opérationnels

LIV 04 : Mise à disposition de solutions techniques

LIV 05 : Mise à jour des outils et solutions mis à disposition (MCO, MCS)

LIV 06 : Opérations de maintenance : Connexion d'un équipement au SI client

LIV 07 : Gestion des faux positifs et faux négatifs

LIV 08 : Centralisation et exploitation des rapports produits par les solutions

LIV 09 : Complémentarité des solutions de contrôle

LIV 10 : Formalisation du certificat d'innocuité

LIV 11 : Formalisation du dossier global d'attestations pour un système complexe

LIV 12 : Mise sous scellés du support contrôlé, à des fins de stockage et transport

LIV 13 : Communication et sensibilisation des utilisateurs

LIV 14 : Communication sur les moyens mis à disposition

ANNEXES du REFSELI

4 Annexe 1 : Gestion des « faux positifs »

Cette annexe formalise le processus de traitement des « faux positifs » que chaque industriel s'engage à intégrer dans le processus de livraison.

4.1 Contrôle de la livraison conformément aux exigences du REFSELI déclinées localement

A noter : afin que le contrôle couvre l'intégralité de la livraison, l'utilisateur doit en maîtriser « l'architecture » (exemples des fichiers ISO, compressés ou chiffrés …).

4.2 Obtention d'un rapport d'analyse utilisable pour le CDIn qui peut avoir trois statuts

[•] Le rapport est sans alerte : livraison réputée SAINE, la livraison peut continuer.

[•] Le rapport signale un fichier suspect : livraison suspendue, une analyse complémentaire est nécessaire. Elle est définie dans le paragraphe suivant.

[•] Le rapport signale un fichier malveillant : livraison potentiellement infectée ; par défaut la livraison est bloquée et le support doit être traité comme « dangereux » et avec les mesures de protection adaptées.

4.3 Démarche de traitement des fichiers identifiés comme suspects ou malveillants.

1. Formalisation de la prise en compte (ex : Ouverture d'un ticket d'incident).
2. Si une analyse précédente, de moins de 6 mois et dans un cadre d'emploi similaire, a permis de catégoriser l'alerte comme FP (« faux positif ») alors le justificatif est à joindre au rapport d'analyse.
3. Si l'alerte n'est pas localement connue ou si son analyse est antérieure à 6 mois, elle doit être escaladée afin de :

   Interpréter les éléments du rapport et vérifications élémentaires (Hash connu, alerte de plusieurs AV, version/ date des moteurs, niveau de scan, …) [niv. 1],

   Analyser formellement et de façon tracée les fichiers concernés [niv. 2.] Quatre conclusions possibles :

   - [•] Les fichiers sont identifiables comme FP par complément d'information (ex : Analyse déjà effectuée suite à un signalement par une autre entité, faux positif signalé par l'éditeur de la librairie, ...)
   - [•] Les fichiers sont catégorisables comme FP par analyse technique (identification et justification des éléments de signature ayant déclenché l'alerte, exécution en sandbox, vérification des sources, …)
   - [•] La nature des fichiers reste incertaine, les analyses n'ont pas abouti. La livraison doit être précédée d'un échange spécifique avec le client et d'une éventuelle analyse commune des éléments concernés.
   - [•] Les fichiers sont effectivement malveillants.

A noter qu'en fonction de l'origine des fichiers suspects (ex : IT/métier), des chaines de traitement distinctes peuvent être déclenchées.

Remarque : la sensibilité du justificatif d'analyse est à apprécier au cas par cas en fonction des éléments concernés.

4.4 Consolidation du rapport avec les éléments permettant de justifier la catégorisation des fichiers suspects.

- Validation du rapport (avec justificatifs) par le responsable identifié (OSSI/RSSI, responsable projet, ...)

4.5 Consolidation des bases de FP.

- Référencement, capitalisation régulière et mise à disposition des bases de FP aux utilisateurs concernés.
- Mise à disposition aux tiers [encore à définir]

4.6 Informations nécessaires présentes dans le justificatif d'analyse

Chaque fichier suspicieux analysé doit faire l'objet d'une justification formelle jointe au CDIn.

Cette justification doit contenir *a minima* les informations suivantes :

Éléments de contexte :

- Objet
- Date de la fiche
- Référence formelle de la prise en compte (ex : ticket d'incident « interne ») (cf. § III.1.)
- Descriptif ou contexte

Éléments d'identification du fichier suspect :

- Nom du fichier suspect
- Hashs associés
- Pour chaque fichier ayant soulevé l'alerte, nom de la menace et informations reçues de l'outil AV (nom, versions moteur et signature)

Éléments d'analyse :

- Date de fin de l'analyse
- Description de l'analyse
- Résultats et recommandations éventuelles, notamment si le fichier est effectivement malveillant
- Entité ou fonction et nom du responsable de l'analyse (RSSI/ OSSI, responsable CERT ou SOC, responsable métier)

Éléments de conclusion :

- Conclusion
- Statut :
  - [•] Faux positif
  - [•] Levée de doute impossible à confirmer factuellement
  - [•] Élément malveillant

A noter :

- La sensibilité du justificatif est à apprécier au cas par cas, notamment au regard de l'annexe de sécurité.
- L'origine d'une justification doit pouvoir être tracée et contrôlée. La mise en place dans un second temps de signatures électroniques pourra être envisagée.
- Les échanges autour des méthodologies et outils d'analyse permettraient de mettre en cohérence les résultats trouvés par chaque acteur.

5 Annexe 2 : Dossier global d'attestations

Cette annexe formalise les informations nécessaires à la constitution d'un « dossier global d'attestations » (DGDA) dont la forme, les processus de constitution, les processus de gestion et le niveau de sensibilité restent de la responsabilité de l'industriel.

Pour les systèmes « ultra complexes », une arborescence de dossiers est possible afin d'organiser les éléments par sous-systèmes. Le dossier global d'attestations d'un système complexe vise à synthétiser et recenser les CDIn et leurs pièces justificatives ; il n'a pas pour vocation, dans le cadre du périmètre actuel du REFSELI, à rassembler tous les éléments de preuve de « confiance numérique » et d'innocuité du système.

Le dossier global d'attestations (dans le périmètre *V1*) est constitué de trois parties principales :

A. La synthèse du dossier

- Contexte ou/et référence du contrat ;
- *Option : organisme destinataire ;*
- Nombre de CDIn ;
- Synthèse des statuts des CDIn (Ex : 23 OK – 2 Suspicieux – 0 Infecté) ;
- Versionning du dossier ;
- *Option : nom du responsable ou porteur du DGDA.*

B. L'index détaillé des CDIn

Avec pour chaque élément contrôlé :

- Identification du composant testé, non ambiguë pour le métier (Exemple : PBS / décomposition du produit) ;
- Identifiant du CDIn ;
- Date du contrôle (+ justification si date expirée) ;
- Statut du contrôle ;
- Liste des justificatif(s) éventuel(s) des faux positifs (ou liens vers ces justificatifs) ;
- Niveau de sensibilité du composant (ex : DR, S, TS, ...) ;
- *Option : Contrôle du composant à la réception : existe-t-il des contraintes ne permettant pas de tester le composant à la réception O/N ? Si oui, renseigner le champ libre pour argumentaire (technique/SDF/légal/garantie/ MCS…) ;*
- *Option : Condensat de chaque CDIn ;*
- *Option : Condensat des justificatifs des FP associés aux CDIn.*

C. Les métadonnées du dossier

A noter que ces informations peuvent être réparties au sein du DGDA.

- *Option : Condensat du DGDA ;*
- *Option : Signature globale du DGDA ;*
- Niveau de classification du DGDA (marquage à anticiper).

La constitution du DGDA reste sous la maîtrise de l’industriel. L’ensemble des éléments du DGDA doit être vérifiable par le client sous un format ou via des moyens adaptés qui sont à définir au préalable entre l’industriel et le client.

Nota : Pour faciliter l’exploitation du DGDA, il sera veillé à lui conserver une sensibilité inférieure ou égale au niveau Diffusion Restreinte (les éventuels éléments classifiés feront l’objet d’annexes dédiées supplémentaires).

L’élargissement du périmètre du dossier global d’attestations à d’autres éléments de confiance et la mise en place d’une garantie de son intégrité pourront être étudiés lors des prochaines évolutions du REFSELI.

6 Glossaire

AV	AntiVirus
CDIn	Certificat D'Innocuité
CERT	Computer Emergency Response Team ; centre d'alerte et de réaction aux attaques informatiques
COTS	Commercial Off The Shelf
DGDA	Dossier Global D'Attestations
FP	Faux Positif
MCO	Maintien en Conditions Opérationnelles
MCS	Maintien en Conditions de Sécurité
MOI	Maître d'Œuvre Industriel
OSSI	Officier de Sécurité des Systèmes d'Information
PSO	Product Security Officer
RSSI	Responsable de la Sécurité des Systèmes d'Information
SA	Système d'Armes
SDF	Sureté De Fonctionnement
SI	Système d'Information
SOC	Security Operation Center
USB	Universal Serial Bus

7 Suivi des versions

Version	Date	Commentaires
V1.0	28/10/22	Version initiale

- Fin du document -