PREMIER MINISTRE

n°931/SGDN/DCSSI

Paris, le 26 mars 2003

GUIDE TECHNIQUE

pour la réalisation et l'utilisation

de scellés de sécurité

pour les équipements

des systèmes d'information.

DIRECTION CENTRALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Version : 1.0/2003

SOMMAIRE

1 : REFERENCES

[1] **Instruction générale interministérielle n° 900/SGDN/SSD/DR & n°900/DISSI/SCSSI/DR du 20/07/93, sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées,** voir :
Article 10 : Articles contrôlés de sécurité des systèmes d'information (ACSSI).
Article 14 : Principe d'intégrité des moyens de protection.

[2] **Recommandation n° 901/DISSI/SCSSI du 02/03/94, pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense**, voir :
Article 9 : Surveillance des moyens de protection des systèmes d'information.
Article 13 : Principe d'intégrité des moyens de protection.

[3] **Instruction interministérielle n° 910/SGDN/SSD/DR & 910/DISSI/SCSSI/DR du 19/12/94, sur les articles contrôlés de la sécurité des systèmes d'information**, voir :
Article 3 : Définition (d'un ACSSI).
Article 4 : Principes fondamentaux de la doctrine ACSSI.
Article 10 : Traitement des incidents.

[4] **Directive n° 911/DISSI/SCSSI/DR du 20/06/95, relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI),** voir :
Chapitre 2 : gestion des ACSSI.

[5] **Instruction interministérielle n°2000/SGDN/SSD/DR du 01/10/86, sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marchés et autres contrats.**

2 : AVANT PROPOS

Les équipements des systèmes d'information qui traitent des informations sensibles qui peuvent être classifiées de défense, sont des cibles pour les attaquants qui cherchent à compromettre les informations traitées ou traitantes.

C'est pourquoi il est important de protéger ces équipements par des mesures capables :

- d'empêcher leur compromission,

- de révéler leur compromission lorsque, malgré tout, celle-ci s'est produite.

La panoplie des mesures contre la compromission comprend des mesures techniques de protection de l'intégrité physique des équipements.

Parmi ces mesures techniques, l'utilisation de scellés de sécurité présente généralement un bon compromis coût/efficacité, à condition de respecter les principes énoncés dans ce guide.

Remarque :
Un scellé de sécurité n'a pas vocation à rendre impossible les attaques contre un équipement. En revanche, s'il est bien conçu et bien placé, il dissuadera l'attaquant désireux de ne pas laisser de trace. L'utilisation de scellés de sécurité illustre le principe de défense dans la profondeur.

3 : OBJET DU GUIDE

Ce guide a pour objet de présenter les principes généraux à connaître pour la réalisation et l'utilisation de scellés destinés à la protection des équipements des systèmes d'information.

Le respect de ces principes réduira les risques d'atteintes à l'intégrité physique des équipements des systèmes d'information protégés avec des scellés.

4 : DEFINITION

Dans ce guide, on appelle **scellé de sécurité** le dispositif capable de mettre en évidence une tentative d'atteinte à l'intégrité physique de l'équipement sur lequel il est placé, que cette tentative ait réussi ou non.

5 : CHAMP D'APPLICATION

Ce guide s'adresse aux acteurs de la sécurité des systèmes d'information des administrations et services déconcentrés de l'Etat, qui sont susceptibles d'être commanditaires ou utilisateurs de scellés de sécurité pour la protection des équipements des systèmes d'information dont ils ont la charge.

Il s'applique lors de la réalisation des scellés de sécurité, au moment de la spécification du besoin, puis au moment de la vérification de la livraison.

Il s'applique aussi lors de la définition des conditions d'emploi de ces scellés.

Dans les deux cas, c'est un document de portée générale qui doit amener les personnes qui décideront la réalisation et l'utilisation de scellés de sécurité, à préciser les principes énoncés, pour tenir compte :

- des menaces particulières qui pèsent localement sur leur système,

- des vulnérabilités connues des équipements de leur système,

- des caractéristiques des scellés éventuellement disponibles.

6 : REALISATION

La réalisation de scellés de sécurité peut se décomposer en trois étapes : la spécification, la fabrication[1] et la vérification de la livraison. La spécification incombe au commanditaire ; c'est l'énoncé du besoin à satisfaire sous des contraintes à préciser. La fabrication est l'activité du fournisseur. La vérification de la livraison incombe au commanditaire qui doit s'assurer de la conformité de la fourniture par rapport à sa spécification.

[1] En fait : la conception, la fabrication et la production.

La spécification.

L'activité de spécification donne lieu à l'établissement d'un cahier des charges qui peut s'organiser comme suit :

1- Expression du besoin.

Le besoin est une mesure technique capable de signaler les tentatives d'atteinte à l'intégrité physique des équipements des systèmes d'information.

2- Expression des contraintes.

Cinq contraintes principales sont à préciser au fournisseur pour qu'il puisse concevoir, fabriquer et produire, dans de bonnes conditions, la solution attendue.

1. La solution doit être sensible aux agressions sur elle-même et sur l'équipement qu'elle protége (principe de réduction des risques de non-détection d'une agression).

   Pour cela, la solution doit posséder un ou plusieurs caractères susceptibles de se modifier de façon irréversible dès la première tentative d'atteinte contre la solution elle-même ou contre l'intégrité physique de l'équipement qu'elle protége.

   Dans la plupart des cas, la modification de ces caractères doit pouvoir être perçue aisément par un large public d'usagers.

2. La solution doit pouvoir se conserver dans des conditions d'ambiance normale, avant son emploi, pendant une durée à préciser. De même, les caractères sensibles de la solution doivent rester stables dans les conditions d'ambiance normale d'emploi de l'équipement qu'elle protège, pendant une durée à préciser (principe de réduction des risques de fausses alarmes).

   Il est recommandé d'indiquer au fournisseur que la solution attendue soit :
   - insensible à l'échauffement électrique dû au fonctionnement normal de l'équipement,
   - insensible aux interactions naturelles entre le dispositif et l'équipement (il conviendra probablement de fournir des échantillons de supports au fournisseur),
   - résistante aux variations des conditions d'emploi (température, hygrométrie, …) dans toute la plage définie dans la fiche de caractéristique technique de l'équipement,
   - résistante aux frottements non exagérés et à l'usage de solvants ordinaires de nettoyage (eau, savon, alcool, produits usuels d'entretien).

   Il est recommandé de fixer une durée raisonnable de fiabilité optimum de la solution au-delà de laquelle celle-ci devra être remplacée.

3. La mise en œuvre de la solution devrait être simple et rapide. Elle ne devrait pas entraîner d'opération de maintenance particulière, hormis le renouvellement normal de la solution elle-même, en fin de cycle de vie.

4. La solution doit être difficile à contrefaire, même si elle est analysée.

Le caractère difficile de la contrefaçon mérite d'être précisé.
En demandant un niveau de difficulté ordinaire, le commanditaire déclare attendre que la solution ne puisse pas être imitée avec des moyens courants de reproduction. Par ailleurs, il attend aussi que la solution soit facilement et rapidement authentifiable par un large public d'usagers.

En demandant un niveau de difficulté moyen, le commanditaire déclare attendre que la solution ne puisse pas être imitée avec des moyens spécialisés accessibles auprès d'industriels ou de laboratoires, au titre, par exemple, d'une prestation commerciale. Par ailleurs, il attend aussi que la solution soit toujours facilement et rapidement authentifiable par un large public d'usagers, et qu'il soit possible de conduire une authentification plus poussée avec des agents avertis munis éventuellement d'outils spéciaux.

En demandant un niveau de difficulté élevé, le commanditaire déclare attendre que la solution ne puisse pas être imitée avec des moyens spécialisés tels que ceux dont peut disposer une agence gouvernementale. Par ailleurs, il attend aussi que la solution soit toujours facilement et rapidement authentifiable par un large public d'usagers, et qu'il soit possible de conduire une authentification très poussée avec des experts et des moyens technologiques appropriés.

5. La solution ne doit pas pouvoir être produite au-delà des quantités commandées.

Le commanditaire devrait énoncer ses besoins en sécurité pour tout le processus de conception, fabrication, production, conservation et livraison de la solution (voir [5]). Il devrait assister la Personne responsable des marchés de l'administration (PRM) dans son choix de la procédure de marché adaptée. Il peut prévoir des visites, contrôles ou inspections de sécurité chez le fournisseur. Dans ce cas, les modalités de ces visites, contrôles ou inspections sont à définir formellement avec le fournisseur.

L'ensemble des informations et outils originaux qui permettent de produire industriellement la solution, devrait faire l'objet de mesures de protection explicites. La destruction de ces informations et outils peut être demandée à la fin de la production. Dans ce cas, le processus de destruction est à définir formellement avec le fournisseur.

3- Spécifications techniques supplémentaires.

Pour orienter le fournisseur vers une catégorie de solutions présentant un rapport coût/efficacité bien ciblé, le commanditaire peut prendre conseil auprès d'experts et indiquer, par exemple, qu'il attend une solution ayant la forme d'étiquettes holographiques autocollantes.

Pour satisfaire des besoins particuliers, le commanditaire peut indiquer la taille et la forme de la solution attendue. Il peut aussi demander sa personnalisation avec un logo et un texte original et indélébile.

Pour satisfaire des besoins supplémentaires d'authentification, de comptabilité et de gestion, tant de la solution elle-même que de l'équipement qu'elle protège, le commanditaire peut demander l'inscription d'un numéro de série et d'un code à barres indélébiles sur la solution.

Remarque sur les spécifications déterministes.
La spécification déterministe consiste à exprimer son besoin en décrivant la solution désirée sans la raisonner explicitement. Cette méthode est à proscrire car elle peut, d'une part, se heurter au principe fondamental de mise en concurrence du code des marchés publics et, d'autre part, conduire à l'acquisition d'une solution inadaptée.

La vérification.

A la fin de la fabrication[2], la vérification de la solution est une opération indispensable pour la cohérence de la démarche de sécurité engagée. Elle incombe au commanditaire qui devrait s'assurer au moins de la conformité de la fourniture aux exigences fixées dans son cahier des charges. Elle est contractuelle dans le cadre d'une opération d'achat public, et fait partie de la recette.

La vérification de conformité et plus particulièrement l'estimation de l'efficacité de la solution sont des activités qui peuvent présenter des difficultés quand le commanditaire n'a pas la possibilité de reproduire lui-même les menaces contre lesquelles il souhaite se prémunir. Dans ce cas, le commanditaire peut faire appel à la DCSSI, via sa voie fonctionnelle SSI.

7 : EMPLOI

L'emploi de scellés de sécurité peut être envisagé sur tous les équipements des systèmes d'information traitant des informations sensibles. Il parait judicieux toutefois de réserver cette mesure aux équipements les plus sensibles (chiffreurs, filtres, routeurs, concentrateurs, serveurs, baies de stockage, …) de ces systèmes afin d'éviter la dissémination de scellés susceptible de faciliter leur analyse à des fins de contrefaçon. Dans certains cas, les notifications d'agrément (voir [1]), ou de caution (voir [2]), peuvent faire mention d'une recommandation, ou de l'obligation, d'apposer un scellé de sécurité sur le moyen de cryptologie ou le moyen de sécurité informatique agréé ou cautionné.

L'emploi de scellés de sécurité devrait s'accompagner d'une information des usagers du système d'information qui doivent accepter, comprendre et jouer le rôle de surveillant. Il entraîne la mise à jour de la documentation de sécurité du système bénéficiaire de la mesure. Cette mise à jour devrait indiquer la conduite à tenir en cas de découverte d'un indice suspect laissant supposer que l'équipement protégé a fait l'objet d'une investigation.

Apposition.

1- Détermination de l'emplacement

L'emplacement du scellé de sécurité peut être matérialisé sur les équipements ou indiqué dans la documentation de ceux-ci. Certaines notifications d'agrément ou de caution peuvent fournir des recommandations, ou fixer des règles strictes, pour le positionnement de ces scellés.

[2] Ou mieux, à la livraison du prototype ou d'un lot d'essai, si cela est prévu avec le fournisseur.

Quand ce n'est pas le cas, pour déterminer le meilleur emplacement possible pour un scellé, il convient de rechercher l'endroit qui gênera le plus l'attaquant (le scellé est un obstacle à placer sur son chemin), et qui facilitera le mieux la détection de l'attaque (le scellé est aussi un signal d'alarme qui doit pouvoir être perçu par le plus grand nombre d'usagers).

Les emplacements à privilégier pour disposer des scellés de sécurité sont généralement :
- les jonctions de boîtiers,
- les limites des parties amovibles, des modules, des ouvertures, des trappes, des capots, …
- les têtes de vis affleurantes, les boulons encastrés, certains rivets, certaines soudures, …
- les charnières, les verrous, …

2- Opérations de mise en place

La technique pour apposer un scellé devrait être demandée au fournisseur. Celui-ci doit la fournir, même si elle paraît élémentaire.

Les opérations de mise en place devraient respecter scrupuleusement les indications sur la préparation des surfaces (dégraissage, dépoussiérage), les temps de prise (entre 1 et 24 heures à température normale) et les pressions de serrage.

8 : GESTION

Un scellé de sécurité est un article qui par son intégrité contribue à la sécurité d'un système d'information. Il est donc, par définition, un article contrôlé de la sécurité des systèmes d'information (ACSSI - voir [3], article 3). Toutefois, il ne mérite pas de porter pour lui-même la mention ACSSI (voir [3], article 8).

Tant que le scellé n'est pas apposé sur un équipement, il présente une attractivité certaine pour les personnes malveillantes. Il est donc nécessaire de le protéger contre le vol. C'est pourquoi des règles de stockage, de comptabilité et de distribution devraient être appliquées.

Dès que le scellé est en place, il devient un composant de l'équipement qu'il protège. Sa gestion est alors liée à cet équipement.

Les opérations de surveillance et de maintenance des équipements des systèmes d'information sont susceptibles de consommer des scellés. Il convient de fixer les règles de remplacement des scellés détruits légitimement, ou dont le vieillissement jugé normal les rend impropres à continuer de remplir leur fonction.

9 : TRAITEMENT DES INCIDENTS

La modification d'un caractère sensible d'un scellé de sécurité est un « indice suspect laissant supposer que le moyen (protégé par le scellé) a fait l'objet d'une investigation ou d'un piégeage ». On parle alors de risque de compromission. Le traitement de l'incident devrait se faire conformément à la réglementation en vigueur rappelée en annexe.

ANNEXE

Rappel de la réglementation des ACSSI

- *Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information n° 910/SGDN/SSD/DR & 910/DISSI/SCSSI/DR du 19/12/94,* et particulièrement son article 10 :

  « Tout incident réel ou supposé, perte ou disparition d'un document ou d'un moyen, découverte d'un **indice suspect laissant supposer que le moyen a fait l'objet d'une investigation ou d'un piégeage**, doit faire immédiatement l'objet d'un rapport confidentiel au FSSI acheminé par le canal de la voie SSI. L'information doit être communiquée à la DCSSI, brsque l'incident est de nature à mettre en cause la sécurité d'un moyen de protection utilisé dans un autre ministère.

  L'autorité responsable du ministère concerné, en liaison avec la DCSSI le cas échéant, évalue les risques réels de compromission et fait alors prendre les mesures correctives adaptées. »

- *Directive n° 911/DISSI/SCSSI/DR du 20/06/95 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI),* et particulièrement son paragraphe 7 :

  « La conduite à tenir en cas de compromission réelle ou supposée d'une information classifiée est indiquée dans l'IGI 1300. Le présent article traite des mesures complémentaires pour les ACSSI.

  Toute personne qui constate un vol, une perte ou une **compromission** rend compte le plus rapidement possible au détenteur dépositaire de son organisme, sans préjudice des autres dispositions pouvant être prises par chaque département ministériel. Le détenteur dépositaire avertit alors l'autorité dont il dépend directement dans la voie fonctionnelle SSI, en application des articles 6 et 10 de l'II 910. Le compte rendu de perte ou de compromission est complété ensuite par un rapport circonstancié et détaillé.

  Dans le cas d'un paramètre secret présent en deux ou plusieurs sites, sa compromission dans l'un des sites peut être très grave. Elle peut toutefois se révéler sans conséquence pour la sécurité des informations si elle est décelée avant utilisation, signalée à temps, et si les mesures correctives appropriées sont prises (par exemple, passage sur la clé de secours). Il importe donc que le détenteur dépositaire alerte ou fasse alerter immédiatement l'autorité responsable de la sécurité du système d'information concerné par l'incident, autorité pouvant d'ailleurs relever d'un département ministériel distinct de celui dans lequel la compromission s'est produite.

  Cette autorité évalue les risques de compromission (possible, probable ou certaine), prend les mesures correctives nécessaires et apprécie les conséquences de l'incident de sécurité quant à la protection des informations traitées. Elle avertit alors toutes les autorités utilisatrices susceptibles, de ce fait, d'avoir été victimes d'une compromission d'informations.

Lorsque est retrouvé un document, un matériel ou un support de logiciel ayant fait l'objet d'un compte rendu de perte, un nouveau compte rendu de vol, de perte ou de compromission est établi, exposant les conditions de sa récupération. L'autorité responsable de la sécurité confirme ou informe les mesures prises. L'article retrouvé ne peut être réutilisé qu'après vérification de son intégrité et sur ordre de l'autorité qualifiée. En aucun cas, un paramètre secret retrouvé ne sera utilisé ou réutilisé; il sera détruit. »