Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CSPN-2011/13

## Coffre-fort Linsecure
## 1.0

*Paris, le 22 novembre 2011*

*Le directeur général de l'agence nationale de la sécurité des systèmes d'information*

Patrick Pailloux
**[ORIGINAL SIGNE]**

SÉCURITÉ CERTIFICATION

# Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

| |
|---|
| *Référence du rapport de certification*<br>**ANSSI-CSPN-2011/13** |
| *Nom du produit*<br>**Coffre-fort Linsecure** |
| *Référence/version du produit*<br>**1.0** |
| *Catégorie de produit*<br>**Stockage sécurisé** |
| *Critères d'évaluation et version*<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*** |
| *Développeur(s)*<br>**Linagora SA**<br>**80, rue Roque de Fillol**<br>**92800 Puteaux**<br>**France** |
| *Commanditaire*<br>**Linagora SA**<br>**80, rue Roque de Fillol**<br>**92800 Puteaux**<br>**France** |
| *Centre d'évaluation*<br>**Oppida**<br>**4-6, avenue du Vieil Etang - Bât B**<br>**78180 Montigny Le Bretonneux**<br>**Tél : 01 30 14 19 00, mél : cesti@oppida.fr** |

# Préface

## La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

# Table des matières

**1. LE PRODUIT ..... 6**

1.1. PRESENTATION DU PRODUIT ..... 6
1.2. DESCRIPTION DU PRODUIT EVALUE ..... 6
*1.2.1. Catégorie du produit ..... 6*
*1.2.2. Identification du produit ..... 7*
*1.2.3. Services de sécurité ..... 7*
*1.2.4. Configuration évaluée ..... 7*

**2. L'EVALUATION ..... 8**

2.1. REFERENTIELS D'EVALUATION ..... 8
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L'EVALUATION ..... 8
2.3. TRAVAUX D'EVALUATION ..... 8
*2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité ..... 8*
2.3.1.1. Spécification de besoin du produit ..... 8
2.3.1.2. Biens sensibles manipulés par le produit ..... 8
2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection ..... 8
2.3.1.4. Fonctions de sécurité ..... 8
2.3.1.5. Utilisateurs typiques ..... 8
*2.3.2. Installation du produit ..... 9*
2.3.2.1. Plate-forme de test ..... 9
2.3.2.2. Particularités de paramétrage de l'environnement ..... 9
2.3.2.3. Options d'installation retenues pour le produit ..... 9
2.3.2.4. Description de l'installation et des non-conformités éventuelles ..... 10
2.3.2.5. Durée de l'installation ..... 10
2.3.2.6. Notes et remarques diverses ..... 10
*2.3.3. Analyse de la documentation ..... 10*
*2.3.4. Revue du code source (facultative) ..... 10*
*2.3.5. Fonctionnalités testées ..... 10*
*2.3.6. Fonctionnalités non testées ..... 11*
*2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités ..... 11*
*2.3.8. Avis d'expert sur le produit ..... 11*
*2.3.9. Analyse de la résistance des mécanismes et des fonctions ..... 11*
2.3.9.1. Liste des fonctions et des mécanismes testés - résistance ..... 11
2.3.9.2. Avis d'expert sur la résistance des mécanismes ..... 11
*2.3.10. Analyse des vulnérabilités (conception, construction…) ..... 11*
2.3.10.1. Liste des vulnérabilités connues ..... 11
2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert ..... 12
*2.3.11. Accès aux développeurs ..... 12*
*2.3.12. Analyse de la facilité d'emploi et préconisations ..... 12*
2.3.12.1. Cas où la sécurité est remise en cause ..... 12
2.3.12.2. Recommandations pour une utilisation sûre du produit ..... 12
2.3.12.3. Avis d'expert sur la facilité d'emploi ..... 12
2.3.12.4. Notes et remarques diverses ..... 12
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES ..... 13
2.5. ANALYSE DU GENERATEUR D'ALEAS ..... 13

**3. LA CERTIFICATION ..... 14**

3.1. CONCLUSION ..... 14
3.2. RESTRICTIONS D'USAGE ..... 14

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est « Coffre-fort Linsecure**,** version 1.0 **»** développé par Linagora SA. Il s'agit d'un dispositif logiciel dont la fonction est de chiffrer, de signer et de sceller les données tracées par le capteur, afin d'en garantir l'intégrité et l'exhaustivité dans le temps. Ce produit s'appuie sur diverses librairies open source pour assurer son fonctionnement.

Ce coffre-fort électronique est évalué dans le contexte particulier de l'ouverture du marché français des jeux d'argent et de paris en ligne. Pour pouvoir proposer des offres de jeux aux consommateurs français, un « opérateur » doit, entre autre, permettre à une « autorité » (ARJEL[1]) de surveiller ses activités transactionnelles. Pour cela, un dispositif doit être installé chez l'opérateur pour recueillir et archiver les traces de certaines opérations au sein de son système d'information.

Ce dispositif est communément nommé « coffre-fort électronique ». C'est ce produit qui est la cible de l'évaluation en vue d'une certification de sécurité de premier niveau.

Le système comporte également un capteur, hors du périmètre de cette certification, permettant de formater les données circulant entre le joueur et la plateforme de jeu, et de les transférer vers le module d'entrée du coffre-fort.

## 1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

### *1.2.1. Catégorie du produit*

| |
|---|
| ☐ 1 - détection d'intrusions |
| ☐ 2 - anti-virus, protection contre les codes malicieux |
| ☐ 3 – firewall |
| ☐ 4 - effacement de données |
| ☐ 5 - administration et supervision de la sécurité |
| ☐ 6 - identification, authentification et contrôle d'accès |
| ☐ 7 - communication sécurisée |
| ☐ 8 - messagerie sécurisée |
| ☒ **9 – stockage sécurisé** |
| ☐ 10 - matériel et logiciel embarqué |
| ☐ 99- Autres |

[1] Autorité de Régulation des Jeux En Ligne

### *1.2.2. Identification du produit*

Le coffre-fort est composé d'un ensemble de logiciels et de fichiers de configuration. Le produit certifié est identifiable par le numéro de version et l'empreinte de trois de ces éléments :

| Élément | Version | Emplacement et empreinte |
|---|---|---|
| mini-sensor | 0.9 | /secure/soft/linsecure/lib/mini-sensor-0.9-SNAPSHOT.jar<br>**3502c7740e21fb8a74ac04ed3b9533e4** |
| vault | 0.9 | /secure/soft/linsecure/lib/vault-0.9-SNAPSHOT.jar<br>**f2f714d4c1bc36d00ef08c2113ace22c** |
| webservices | 0.9 | /secure/soft/linsecure/lib/webservices-0.9-SNAPSHOT.jar<br>**f243c3285db7210bd0b64262e1d0c826** |

Pour connaître les numéros de version de l'ensemble des briques logiciels, un script est mis à disposition de l'utilisation. Ce dernier, appelé « version », se trouve dans le répertoire /usr/local/bin et son empreinte est la suivante :

**78ec0f9a076220675f67521a2bdc69b2**

### *1.2.3. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- le contrôle de l'accès au coffre-fort ;
- le scellement des traces ;
- l'horodatage des traces ;
- le chaînage des traces ;
- le chiffrement des traces.

### *1.2.4. Configuration évaluée*

Deux modes de fonctionnement sont disponibles pour ce produit :

- le mode « ***standalone*** », qui comprend une seule machine physique sur laquelle toutes les ressources utiles au fonctionnement du coffre sont présentes ;
- le mode « **haute-disponibilité** », qui reprend le même principe de fonctionnement que le mode « *standalone* », mais sur lequel les ressources sont réparties sur plusieurs machines.

Le produit a été évalué en mode « *standalone* ».

De plus, le produit a été configuré pour utiliser un espace de stockage local. Cette évaluation ne couvre donc pas l'utilisation d'un espace de stockage réseau de type SAN ou NAS.

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

## 2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

## 2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

### *2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité*

#### 2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Argumentaire (description) du produit »).

#### 2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles à protéger »).

#### 2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des menaces »).

#### 2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité du produit »).

#### 2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.7 « Description des profils »).

### *2.3.2. Installation du produit*

#### 2.3.2.1. Plate-forme de test

La plate-forme de test était composée :

- d'un processeur Intel Core2 ;
- d'une carte compact flash 16 Go ;
- de deux interfaces réseau Gigabit;
- d'une carte HSM Thales nShield Solo 500/4000 F3.

L'architecture logicielle évaluée est la suivante :

| Logiciel | Version |
|---|---|
| Système d'exploitation GNU/Linux | Debian 5.0.8 |
| Xerces | 2.8.0 |
| ActiveMQ | 5.3.1 |
| Bouncycastle | 1.45 |
| Jaxb | 2.2.1 |
| JaxWS | 2.1.4 |
| Apache | 2.2.9-10 + lenny9 |
| OpenSSH | 1:5.5p1-5 |
| OpenSSL | 0.98g-15 + lenny11 |
| JDK | 1.6_0.22 |
| Ntp | 1:4.2.4p4 + dsfg-8lenny3 |
| JDK | 1.6_0.22 |

Linagora a fourni deux applications clientes permettant de tester les fonctionnalités du coffre-fort :

- WSClient : permet l'interaction avec le produit via le WSDL de l'ARJEL ;
- DecryptTrace : permet le déchiffrement des archives.

Le dossier d'exigences techniques de l'ARJEL [DET] stipule qu'en production, chaque opérateur doit intégrer les appels à l'API du coffre-fort au code de son capteur [DET]. Ces outils ne font pas partie du périmètre de ce certificat.

#### 2.3.2.2. Particularités de paramétrage de l'environnement

L'installation est fournie à l'opérateur sous forme de cartes Compact Flash. La phase finale de l'installation concernant la personnalisation de l'installation (IP, sous-réseau, NTP, injection des certificats …) est réalisée par le personnel Linagora et verrouillée. Le système livré clé en main ne nécessite que la configuration du réseau et l'initialisation de l'environnement cryptographique.

#### 2.3.2.3. Options d'installation retenues pour le produit

La configuration du produit suivante a été retenue pour l'évaluation :

- un seul espace de stockage a été créé sur le disque dur local ;
- toutes les clés de d'authentification sont des clés RSA de 2048 bits ;
- la clé de signature des traces a été générée dans le HSM ;

- trois comptes utilisateurs (auditeur ARJEL, opérateur, capteur) ont été créés, chacun étant identifié par un bi-clef RSA 2048 bits unique ;
- un pare-feu applicatif est installé et correctement configuré ;
- le produit a été configuré pour utiliser deux interfaces réseau physiques (administrative et applicative) séparées.

Cette configuration est conforme à [DET].

#### 2.3.2.4. Description de l'installation et des non-conformités éventuelles

L'évaluateur a supervisé l'installation du produit de manière à s'assurer qu'il était installé conformément au manuel d'installation **[GUIDES]**. L'installation du produit a été réalisée en 4 étapes :

1. installation du système à partir d'une clé USB *bootable* fournie ;
2. installation des composants hors distribution, dont le HSM ;
3. personnalisation de la configuration et initialisation de l'environnement cryptographique ;
4. scellement de la plateforme.

#### 2.3.2.5. Durée de l'installation

L'installation, la configuration et les tests de bon fonctionnement ont été effectués par un développeur de Linagora sur une journée.

#### 2.3.2.6. Notes et remarques diverses

L'installation du coffre-fort pour l'évaluation a été effectuée par Linagora.

### *2.3.3. Analyse de la documentation*

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. Le manuel d'exploitation n'a pas été jugé assez universel. Il présente une intégration du coffre-fort déjà réalisée et ne permet pas d'intégrer le produit à un autre type d'infrastructure.

### *2.3.4. Revue du code source (facultative)*

Les évaluateurs n'ont pas eu accès au code source.

### *2.3.5. Fonctionnalités testées*

| Fonctionnalité | Résultat |
|---|---|
| Authentification forte et mutuelle | **Réussite** |
| Scellement des traces | **Réussite** |
| Horodatages des traces | **Réussite** |
| Chainage des traces | **Réussite** |

| | |
|---|---|
| Chiffrement des traces | **Réussite** |
| Durcissement du système | **Réussite** |

#### *2.3.6. Fonctionnalités non testées*

Sans objet.

#### *2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités*

Les tests de conformité ont permis de tester la plupart des fonctionnalités offertes par le produit.

Les utilitaires permettant le test du produit par les évaluateurs ainsi que le capteur permettant la création de traces sont hors périmètre de la cible de sécurité [CDS] et n'ont donc pas été analysés.

#### *2.3.8. Avis d'expert sur le produit*

Le produit est fonctionnellement conforme à la cible de sécurité [CDS]. Le coffre-fort est également conforme aux exigences de l'ARJEL décrites dans [DET], bien que celles-ci souffrent d'une erreur de conception en ce qui concerne la suppression des derniers évènements sauvegardés.

#### *2.3.9. Analyse de la résistance des mécanismes et des fonctions*

##### 2.3.9.1. Liste des fonctions et des mécanismes testés

| Fonction et mécanisme |
|---|
| Mécanismes d'authentification et de contrôle d'accès |
| Validation des données d'entrée |
| Mécanisme de chiffrement des documents |

##### 2.3.9.2. Avis d'expert sur la résistance des mécanismes

La résistance des mécanismes de sécurité est conforme à l'état de l'art. Il n'a pas été mis en évidence de vulnérabilités exploitables dans le cadre de l'évaluation du produit. Les mécanismes de sécurité qui s'appuient sur la cryptographie font l'objet d'une analyse théorique particulière dont les principales conclusions sont données au chapitre 2.4.

#### *2.3.10. Analyse des vulnérabilités (conception, construction…)*

##### 2.3.10.1. Liste des vulnérabilités connues

La cible de sécurité [CDS] stipule que les correctifs de sécurité des différents logiciels utilisés par le produit doivent être appliqués dès leur publication (cf. §2.3.12.2).

Aucune vulnérabilité publique n'a pu être exploitée lors de l'évaluation.

#### 2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Aucune.

### *2.3.11. Accès aux développeurs*

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

### *2.3.12. Analyse de la facilité d'emploi et préconisations*

#### 2.3.12.1. Cas où la sécurité est remise en cause

Sans objet.

#### 2.3.12.2. Recommandations pour une utilisation sûre du produit

Compte « *root* »

Il est fortement recommandé que seule l'« autorité » possède le login / mot de passe d'accès au compte *root*, car il permet d'accéder à l'ensemble des fonctions du système. Ce mot de passe doit suivre une politique de création et une politique de gestion conformes à la note du CERTA (No CERTA-2005-INF-001).

La plate-forme doit pouvoir être mise à jour. Il est préconisé que les mises à jour se fassent sous la responsabilité de l'« autorité ». La mise à jour pourrait, par exemple, être réalisée directement par l'« autorité » (le développeur fournit à l'« autorité » l'ensemble de la procédure de mise à jour, ainsi que les logiciels si besoin), ou indirectement (l'« autorité » s'authentifie en tant que « *root* », et laisse le développeur effectuer la mise à jour sous sa surveillance).

Quel que soit le mode d'intervention, la présence de l'« autorité » est préconisée afin de s'assurer de la non-altération des dépôts et des traces déjà stockés.

Accès physique au poste

Aucun système de chiffrement du disque n'étant mis en place, l'équipement hébergeant l'application devrait être scellé afin de détecter toute ouverture physique illégitime du boîtier. Ce scellé devrait être vérifié lors de chaque audit de la plate-forme.

De plus, il est recommandé de protéger la séquence de démarrage du poste (BIOS et gestionnaire de démarrage) afin d'empêcher les élévations de privilèges.

#### 2.3.12.3. Avis d'expert sur la facilité d'emploi

L'utilisation du produit pour un opérateur est très simple d'emploi et son exploitation est correctement décrite dans les guides [GUIDES].

#### 2.3.12.4. Notes et remarques diverses

Afin d'assurer une utilisation sûre du produit, il doit être installé et configuré par Linagora.

## 2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué offre les services cryptographiques suivants :

- authentification forte et mutuelle ;
- scellement des traces ;
- horodatages des traces ;
- chaînage des traces ;
- chiffrement des traces.

Lors de l'installation du produit, le choix des protocoles et le paramétrage de certains algorithmes permettent de mettre en œuvre des algorithmes non-conformes au référentiel de l'ANSSI [REF-CRY].

Le développeur doit donc vérifier que la configuration qu'il met en place est conforme à ce référentiel.
Par ailleurs, certains mécanismes cryptographiques mis en œuvre par le produit ne sont pas conformes au référentiel [REF-CRY]. Cependant, l'utilisation de contre-mesures adaptées a permis de ne pas remettre pas en cause le niveau de résistance aux attaques visé par la CSPN.
Il est recommandé que ces mécanismes soient mis en conformité et qu'ils soient évalués lors d'une prochaine certification du produit. Des mesures organisationnelles doivent provisoirement être mises en place pour pallier ce manquement (§2.3.12.2).

## 2.5. Analyse du générateur d'aléas

Le générateur d'aléas a fait l'objet d'une analyse et est conforme au référentiel [REF-CRY] de l'ANSSI.

# 3. La certification

## 3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Coffre-fort Linsecure**,** 1.0 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

## 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *LinSecure - Coffre-fort électronique pour le jeu en ligne - Cible de sécurité CSPN ;*<br>Référence : *Linagora_DOC_LinSecure_Cible-de-securite-CSPN* ;<br>Date : *10/30/2010* |
| [RTE] | *Rapport Technique d'Évaluation (RTE) - CSPN LINSECURE ;*<br>Référence : *OPPIDA/DOC/2011/BCF/642/1.2.1* ;<br>Date : *10/18/2011* |
| [ANA-CRY] | *Rapport d'évaluation des mécanismes cryptographiques ;*<br>Référence : *OPPIDA/2011/DOC/642/CRYPTO/2.0* ;<br>Date : *6/22/2011* |
| [DET] | *Dossier des Exigences Techniques de l'ARJEL ;*<br>Version : *1.0 ;*<br>Date : *19/05/2010* |
| [GUIDES] | Guide d'installation :<br>*Manuel d'installation du Coffre-fort Linsecure ;*<br>Référence : *7244-01_DOC_Oppida_LinSecure_Installation_v1.1* ;<br><br>Guide d'administration :<br>*Manuel d'exploitation Coffre-fort LinSecure ;*<br>Référence : *7244-01_DOC_AubSail_LinSecure_Exploitation_v1.1* ; |

# Annexe 2. Références à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. | |
| [CSPN] | Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011.<br><br>Documents disponibles sur www.ssi.gouv.fr |
| [REF-CRY] | Référentiel général de sécurité, version 1.0, annexe B1 :<br>Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20.<br><br>Documents disponibles sur www.ssi.gouv.fr |