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-2016/10

Sous-système de chiffrement de disques dm-crypt
Noyau Linux 4.4.2 – cryptsetup 1.7.0

Paris, le 16 juin 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CSPN-2016/10

Nom du produit

Sous-système de chiffrement de disques dm-crypt

Référence/version du produit

Noyau Linux 4.4.2 – cryptsetup 1.7.0

Référence de la cible de sécurité

Cible de sécurité CSPN dm-crypt version 4.4.2

Référence : CSPN-ST-dm-crypt-1.01, version 1.01 du 24/02/2016

Catégorie de produit

Stockage sécurisé

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Secrétariat général de la défense et de la sécurité nationale
51 Boulevard de la Tour Maubourg
75700 Paris Cedex SP

Centre d'évaluation

AMOSSYS
4bis allée du Bâtiment
35000 Rennes
France

Fonctions de sécurité évaluées

Chiffrement/déchiffrement des données
Authentification des utilisateurs
Protection des clés de chiffrement des données

Fonctions de sécurité non évaluées

Aucune

Restrictions d'usage

Recommandations (voir 2.3.8.2)

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

1.1. Présentation du produit

Le produit évalué est le « Sous-système de chiffrement de disques *dm-crypt* » correspondant à la version 4.4.2 du noyau *Linux* associé à *cryptsetup* 1.7.0.

Le produit constitue une partie de l'infrastructure *device-mapper* du noyau *Linux*, et se base sur les routines de chiffrement issues des interfaces de programmation du noyau.

dm-crypt permet :

- de créer un disque virtuel chiffré, contenu dans un fichier ou sur une partition du disque dur, et de le monter comme un disque physique réel ;
- de chiffrer et déchiffrer de façon automatique, à la volée et transparente ;
- de chiffrer une partition entière (y compris le système d'exploitation, les fichiers temporaires, *swap* etc.) ou un périphérique de stockage (clé USB ou disque dur).

Deux modes de chiffrement sont offerts :

- le mode *plain*, qui utilise une seule *passphrase* pour le chiffrement d'un volume ;
- le mode LUKS (*Linux Unified Key System*) dans lequel jusqu'à huit *passphrases* peuvent être définies pour ouvrir un même volume LUKS, permettant de donner accès à un même volume à autant d'utilisateurs qu'il y a de clés sans que ceux-ci n'aient besoin de partager de secret.

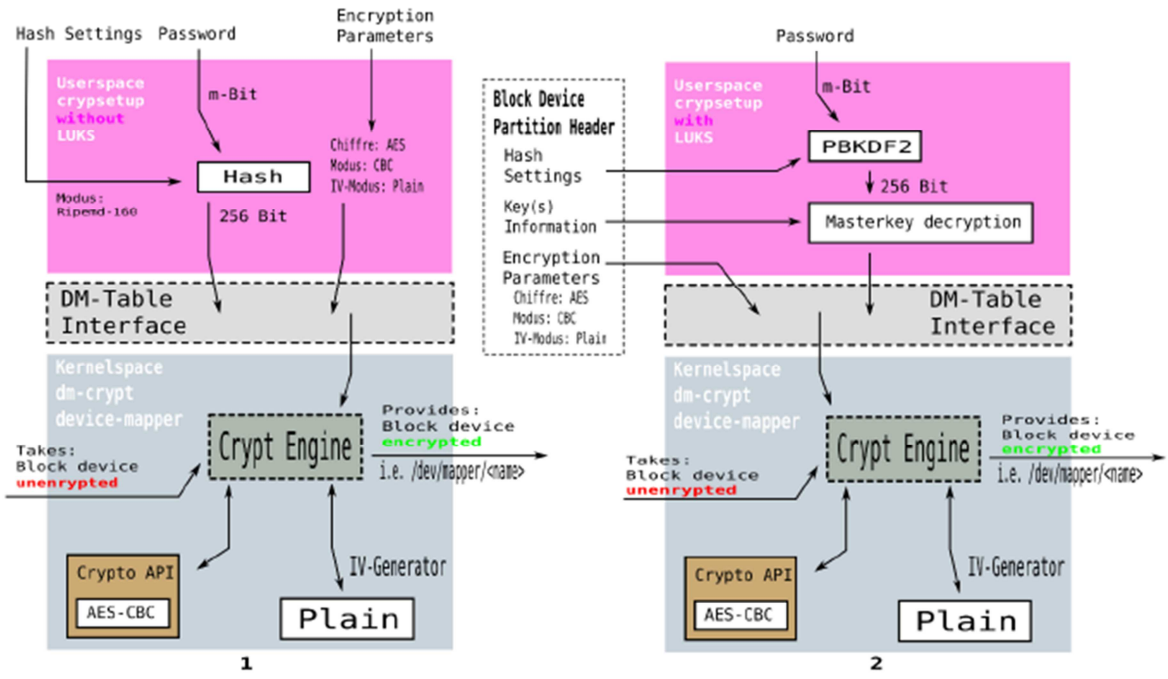

Figure 1 – comparaison des modes Plain (1) et LUKS (2) du chiffrement *dm-crypt*

dm-crypt peut être utilisé :

- soit au moment de l'installation du système d'exploitation (phase de partitionnement des disques) ;
- soit sur un système déjà installé.

1.2. Description du produit évalué

La cible de sécurité [CDS] 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 – environnement d'exécution sécurisé
☐ 11 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☐ 13 – automate programmable industriel

1.2.2. Identification du produit

Nom du produit	*dm-crypt*
Numéro de version du noyau Linux	4.4.2
Numéro de version de *cryptsetup*	1.7

La version de la TOE peut être vérifiée à l'aide des commandes « `uname –a` » et « `cryptsetup –version` », comme illustré sur la figure suivante.

```
root@debian:~# uname -a
Linux debian 4.4.2 #1 SMP Mon Feb 22 10:49:24 CET 2016 x86_64 GNU/Linux
root@debian:~# cryptsetup --version
cryptsetup 1.7.0
root@debian:~# _
```

Figure 2 - Identification de la version de la TOE

1.2.3. Configuration évaluée

Aucune option ou configuration particulière n'est nécessaire préalablement à l'utilisation du produit. En revanche, dans le cadre de cette évaluation, seul le mode LUKS (voir 1.1) a été considéré, de même que les mécanismes cryptographiques suivants, utilisés par défaut :

- AES-256 en mode XTS[1][2] ;
- SHA-256 pour la dérivation de clefs PBKDF2[3] à partir du mot de passe défini par l'utilisateur.

[1] *XEX-based tweaked-codebook mode with ciphertext stealing* est un mode opératoire de chiffrement par blocs utilisé notamment pour le chiffrement de disques.
[2] Par défaut, *cryptsetup* utilise le mode XTS avec la méthode *plain64* pour la génération des vecteurs d'initialisation. La méthode *essiv* (*encrypted sector, salt initial vector*) est également supportée.
[3] *Password-Based Key Derivation Function 2* est un standard pour la dérivation de clefs cryptographiques à partir d'un mot de passe saisi par l'utilisateur, défini dans la RFC 2898.

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 dans la procédure ANSSI-CSPN-CER-P-01/1.1 (voir [CER]).

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

L'évaluation a été réalisée sur un PC embarquant un système d'exploitation *Debian Jessie* 64 bits.
Le noyau *Linux*, initialement en version 3.16.0.4, a été mis à jour en version 4.4.2 par l'évaluateur, qui a également réalisé l'installation de *cryptsetup* en version 1.7 à partir des sources.

2.3.1.2. Particularités de paramétrage de l'environnement et options d'installation

Pour les tests de conformité et de robustesse, une partition `/dev/sdb1` a été créée et protégée avec *dm-crypt/*LUKS. La figure suivante présente les spécifications de l'entête LUKS :

start offset	field name	length	data type	description
0	magic	6	byte[]	magic for LUKS partition header, see LUKS_MAGIC
6	version	2	uint16_t	LUKS version
8	cipher-name	32	char[]	cipher name specification
40	cipher-mode	32	char[]	cipher mode specification
72	hash-spec	32	char[]	hash specification
104	payload-offset	4	uint32_t	start offset of the bulk data (in sectors)
108	key-bytes	4	uint32_t	number of key bytes
112	mk-digest	20	byte[]	master key checksum from PBKDF2
132	mk-digest-salt	32	byte[]	salt parameter for master key PBKDF2
164	mk-digest-iter	4	uint32_t	iterations parameter for master key PBKDF2
168	uuid	40	char[]	UUID of the partition
208	key-slot-1	48	key slot	key slot 1
256	key-slot-2	48	key slot	key slot 2
...	...	...	...	...
544	key-slot-8	48	key slot	key slot 8
592	total phdr size			

Figure 3 - Entête LUKS

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

Sans objet.

2.3.1.4. Durée de l'installation

L'installation de la plateforme et de la TOE a duré moins d'une journée.

2.3.1.5. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est principalement accessible sur internet. La documentation officielle de *dm-crypt* est fournie avec les sources du noyau, elle est également disponible sur le site https://www.kernel.org.
La documentation de *cryptsetup* est également disponible sur la page du projet sous la forme d'un *wiki*.

Globalement, la documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit.

2.3.3. Revue du code source (facultative)

Une revue du code a été réalisée sur les sources de *dm-crypt* et de *cryptsetup*.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité.

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Comme la plupart des solutions de chiffrement de disques, *dm-crypt* ne fournit aucune protection en intégrité des données stockées sur le disque. Une modification illégitime du contenu chiffré pourrait ainsi être effectuée par un attaquant sans être détectée par l'utilisateur.

En outre, la clé maîtresse pour le chiffrement du disque est stockée pendant la durée d'utilisation de la partition, en mémoire RAM, et peut donc se retrouver sur la partition de SWAP si le système est mis en hibernation à ce moment-là.

Enfin, *dm-crypt* ne permettant pas le chiffrement des fichiers nécessaires au démarrage de la machine, un attaquant pourrait en modifier le noyau et/ou les modules pour y introduire un logiciel malveillant afin notamment d'enregistrer les mots de passe saisis par l'utilisateur.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Eu égard aux limites identifiées au 2.3.8.1, l'évaluateur formule les recommandations listées ci-après, dont certaines figurent également dans les manuels ou wikis associés au produit.

a. Concernant le poste de travail, en cours d'utilisation de *dm-crypt*

R1. Sécuriser le poste de travail

dm-crypt et *cryptsetup* ne sont pas protégés contre des logiciels malicieux (*keyloggers*, etc).
L'évaluateur recommande donc de sécuriser le poste par des mises à jour régulières, une protection antivirale, une protection du BIOS, un contrôleur d'intégrité, etc.

R2. Ne pas autoriser l'hibernation du système ou configurer le système pour qu'il chiffre le swap

Les données sensibles qui se trouvent en mémoire au moment de la mise en veille prolongée (alors qu'un volume chiffré est monté) peuvent être accessibles dans le fichier d'hibernation si celui-ci n'est pas chiffré.
L'évaluateur recommande donc de désactiver la mise en hibernation du poste lorsque *dm-crypt* est utilisé ou de configurer le système pour qu'il chiffre la partition de *swap*.

R3. Chiffrer le swap.

Bien que *dm-crypt* protège ses clés de chiffrement et empêche qu'elles puissent être transférées sur le *swap* – sauf lors de la mise en veille (voir *R2*), celui-ci peut contenir d'autres données sensibles (mots de passe, données temporaires, données utilisateur, etc.) en cas de surcharge du système en cours d'utilisation de *dm-crypt*.

R4. Mesurer l'intégrité de la partition de boot

dm-crypt et *cryptsetup* ne peuvent pas chiffrer la partition qui contient les fichiers de démarrage. Il est conseillé d'avoir une mesure d'intégrité pour vérifier si les fichiers dans `/boot` ont été modifiés lorsque l'ordinateur est laissé sans surveillance. Une deuxième possibilité est de démarrer à partir d'un dispositif amovible.

b. Concernant les données d'authentification

R5. Choisir un mot de passe résistant.

Un adversaire peut effectuer une attaque par force brute sur le mot de passe utilisé pour la clé maîtresse.
Les recommandations pour la définition d'un mot de passe robuste sont détaillées dans le document NTMDP2[4].

R6. Stocker le(s) fichier(s) de clés (keyfiles) sur un support externe sécurisé.

[4] « Note technique - Recommandations de sécurité relatives aux mots de passe », éditée par l'ANSSI.

Ceci permet d'éviter qu'un adversaire puisse récupérer le fichier de clé pour l'accès à la partition chiffrée et tenter un accès non autorisé.

R7. Séquestrer la clé maitre pour un recouvrement en cas d'oubli (ou, similairement, créer une copie de sauvegarde de l'entête LUKS)

Les données ne pourront plus être récupérées en cas de perte du mot de passe. De même, en cas de panne matérielle, les données seront irrécupérables.
Par conséquent, l'évaluateur recommande de séquestrer la clé maitresse et les options de chiffrement sur un support de stockage à accès physique restreint pour un recouvrement via l'outil *dmsetup*.

c. Concernant l'utilisation de *dm-crypt*

R8. Démonter le volume dès que les données stockées ne sont plus utilisées.

Tant que le volume est monté, la clé maîtresse et les données sensibles sont conservées en clair dans la RAM. Le démontage conditionne leur effacement.
A noter que la commande `luksSuspend` peut être utilisée depuis un terminal par un utilisateur disposant des droits *root* pour effacer de la mémoire les données sensibles et empêcher l'accès à la partition chiffrée. La page de manuel associée à la commande fournit les informations nécessaires à son utilisation.

R9. En cas de suspicion de compromission d'un mot de passe il est conseillé de détruire le slot associé et d'en ajouter un autre.

Il est à noter que le changement de mot de passe ne modifie pas la clé maîtresse qui sert au chiffrement symétrique du disque. En cas de suspicion de compromission d'un des mots de passe, il est recommandé de créer un nouveau conteneur chiffré, avec un nouveau mot de passe et d'y transférer le contenu de l'ancien conteneur.

R10. Démonter les volumes, voire éteindre le système, en cas d'absence.

La recommandation est plus stricte que R7 et vise à se prémunir d'une attaque de type *coldboot*. L'évaluateur recommande de quitter le poste quelques secondes à minutes après l'extinction du système afin d'éviter une intrusion physique qui permettrait de *dumper* les données rémanentes en mémoire et accéder à des données sensibles.

R11. Utiliser des algorithmes conformes à l'état de l'art et au RGS.

Voir [RGS] pour les règles et recommandations relatives au choix des mécanismes cryptographiques. La configuration utilisée pour cette évaluation fait appel à des mécanismes jugés conformes.

R12. Utiliser de manière préférentielle le périphérique bloquant /dev/random.

Il est conseillé de choisir, lors de la création d'une partition chiffrée, le périphérique bloquant `/dev/random` comme source d'aléa.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier des environnements UNIX.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

dm-crypt utilise le générateur d'aléas du noyau Linux, hors du périmètre de l'évaluation, pour générer la graine servant à la dérivation du mot de passe utilisateur ainsi que la clef maitresse de chiffrement. Ce générateur met en œuvre un retraitement de nature cryptographique qui n'est cependant pas conforme aux règles du [RGS]. Pour autant, aucune vulnérabilité exploitable, dans le contexte d'emploi du produit et pour le niveau d'attaquant considéré, n'était connue de l'évaluateur au moment de l'évaluation.

A noter que l'utilisateur a la possibilité, lors de la création d'une partition chiffrée, de choisir le périphérique bloquant `/dev/random` au lieu du périphérique non-bloquant (`/dev/urandom`), utilisé par défaut, comme source d'aléa.

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 « Sous-système de chiffrement de disques *dm-crypt* » correspondant à la version 4.4.2 du noyau *Linux* soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN dm-crypt version 4.4.2* Référence : *CSPN-ST-dm-crypt-1.01*; Version : *1.01* ; Date : *24 février 2016.*
[RTE]	*Rapport Technique d'Évaluation CSPN Produit dm-crypt - noyau Linux 4.4.2* Référence : *CSPN-RTE-DM-CRYPT-1.01* ; Version : 1.01 ; Date : *18 mai 2016.*
[GUIDES]	Guides disponibles sur le site https://www.kernel.org et dans les manuels accessibles en ligne de commande.

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 des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur http://www.ssi.gouv.fr/
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.