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-2015/07

Mécanisme de cloisonnement *runtime* de KNOX Workspace version 2.3

Paris, le 3 décembre 2015

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

[Original signé]
Guillaume POUPARD

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

ANSSI-CSPN-2015/07

Nom du produit

Mécanisme de cloisonnement runtime de KNOX Workspace version 2.3

Référence/version du produit

Version 2.3

Catégorie de produit

Environnement d'exécution sécurisé

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Samsung Electronics France
1 rue Fructidor
CS 2003
93484 Saint-Ouen Cedex

Centre d'évaluation

Trusted Labs
6 rue de la Verrerie
92190 Meudon Cedex

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 « **Mécanisme de cloisonnement *runtime* de KNOX Workspace version 2.3** » développé par *SAMSUNG ELECTRONICS FRANCE*.

SAMSUNG KNOX est une plateforme basée sur *Android* permettant de faire cohabiter, de manière sécurisée, plusieurs environnements sur un même équipement – typiquement, un environnement professionnel et un environnement personnel.
KNOX s'appuie pour son fonctionnement sur des éléments matériels et logiciels tiers.

La cible de cette évaluation est un sous-ensemble de KNOX correspondant aux fonctionnalités assurant l'isolation et le cloisonnement dynamiques des applications installées dans des environnements (ou conteneurs) différents.

Figure 1 - Présentation de la solution KNOX

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
☐ 99 – autres

1.2.2. Identification du produit

Nom du produit	KNOX Container Technology
Numéro de la version analysée	2.3
Détail des versions	Conteneur 2.3.0 sur SM-G900F (Android 5.0.1) Conteneur 2.3.1 sur SM-N910F (Android 5.0.0) SE for Android 2.2.1

La version certifiée du produit peut être identifiée à l'aide des empreintes suivantes :

Fichier	**Empreinte SHA1**
N910F_XXU1BOC5_XXU1BOC4_OXX1BOC2.zip	479535dc90822fe1e8c61d8901b50c048270db7b
G900F_XEF_XXU1BOD3_XXU1BOD3_OXX1BOD1.zip	e60e36087d141943c097210097c3893f62dabfca
S14.16 KNOX 2.3 Workspace User Guide_D0.2.pdf	b83e352669b8d12e38cc3f4ac3690feb054e5569

1.2.3. Services de sécurité évalués

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :
- l'isolation dynamique des conteneurs KNOX ;
- le filtrage des applications installées ;
- l'authentification de l'utilisateur et protection de l'accès au conteneur ;
- la gestion de l'état du conteneur ;
- la gestion des droits d'accès aux interfaces externes pour les applications.

1.2.4. Configuration évaluée

L'évaluateur a disposé pour son analyse de deux téléphones *Samsung Galaxy Note 4* (SM-N910F) et deux téléphones *Samsung Galaxy S5* (SM-G900F). Les versions de KNOX, SE for *Android* et *Android* associées sont détaillées au 1.2.2.
Seul le mode d'administration *Corporate liable* a été pris en compte pour cette évaluation (voir 2.3.2.2).

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 charge de travail pour cette évaluation a été de 40 hommes jours, du fait du périmètre fonctionnel de la cible et des conditions d'évaluation (évaluation en « boîte noire »).

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 au chapitre 2.1.1 de la cible de sécurité « Application security services ».

2.3.1.2. Biens sensibles manipulés par le produit

Conforme au chapitre 3.2 de la cible de sécurité « Assets protected by the TOE ».

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

Conforme au chapitre 4 de la cible de sécurité « Threats ».

2.3.1.4. Fonctions de sécurité

Conforme au chapitre 5 de la cible de sécurité « Security functions ».

2.3.1.5. Utilisateurs typiques

Conforme au chapitre 2.5 de la cible de sécurité « Typical users ».

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Comme indiqué au 1.2.4, l'évaluateur a eu à sa disposition deux téléphones *Samsung Galaxy Note 4* (SM-N910F) et deux téléphones *Samsung Galaxy S5* (SM-G900F), déjà équipés de KNOX Workspace.
L'application EDM, développée par *SAMSUNG* pour ses besoins propres, a également été fournie.

L'environnement obtenu correspond ainsi à la Figure 2 - Schéma de l'environnement d'évaluation.

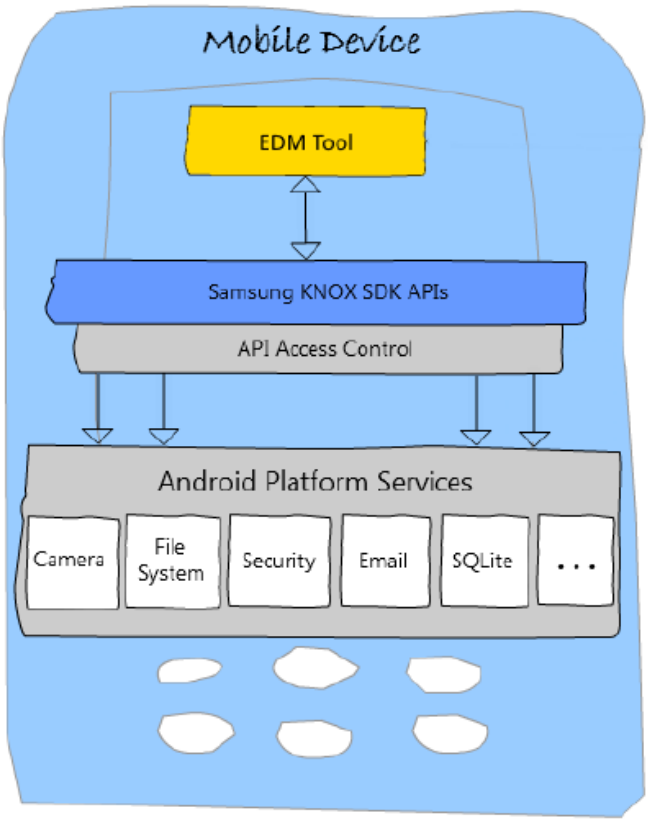

Figure 2 - Schéma de l'environnement d'évaluation

2.3.2.2. Particularités de paramétrage de l'environnement

L'outil EDM – *Enterprise Mobility Management* a été fourni par le développeur afin de permettre la gestion des conteneurs et des politiques MDM (*Mobile Device Management* ou gestion de terminaux mobiles). Lors de son premier lancement, l'application EDM propose de choisir entre deux types d'administration : *Corporate liable* et BYOD (*Bring Your Own Device* ou Amenez Votre Equipement personnel de Communication). La première option a été retenue pour l'évaluation.
Pour le reste, les options par défaut ont été retenues (certaines ont pu être modifiées a posteriori pour le besoin de certains tests - par ex. activation du mode *USB debugging*).

2.3.2.3. Options d'installation retenues pour le produit

Voir au 1.2.4.

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

Sans objet.

2.3.2.5. Durée de l'installation

Sans objet. Le produit est livré déjà installé sur les équipements, seule la configuration de l'EDM a été effectuée par l'évaluateur.

2.3.2.6. Notes et remarques diverses

Néant.

2.3.3. Analyse de la documentation

Aucune remarque particulière n'a été formulée par l'évaluateur.

2.3.4. Revue du code source (facultative)

Le code source n'a pas été fourni pour cette évaluation.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Isolation des données	**Conforme**
Filtrage des applications	**Conforme**[1]
Authentification de l'utilisateur	**Conforme**[2]
Gestion de l'état du conteneur	**Conforme**
Gestion de l'accès aux interfaces externes	**Conforme**[1]

2.3.6. Fonctionnalités non testées

Sans objet.

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

Des comportements limites ont été relevés mais ne remettent toutefois pas en cause la sécurité globale de la solution pour le cas d'usage considéré et moyennant le respect des recommandations formulées au 2.3.12.2.

2.3.8. Avis d'expert sur le produit

Le produit est jugé globalement conforme à sa cible de sécurité.

[1] Le filtrage des applications et des équipements repose sur un système de listes blanches et listes noires pouvant porter à confusion et générer des comportements non souhaités. Une bonne compréhension du mécanisme et une configuration rigoureuse sont essentielles pour assurer un comportement conforme à la politique de sécurité définie.

[2] Des cas où le mécanisme n'a pas eu le comportement attendu ont été observés, sans remettre en cause la conformité globale de la fonction.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctionnalités listées au 2.3.5 ont été soumises à des tests de pénétration.

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Les fonctions de sécurité sont jugées résistantes pour un niveau d'attaquant « modéré ».

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Afin de tester la détection par KNOX du *rootage* du téléphone (hors cible, voir 3.2), l'évaluateur a tenté d'exploiter la vulnérabilité du système *Android* identifiée sous la référence CVE-2014-3153. Celle-ci s'est révélée non applicable sur la version d'*Android* utilisée pour l'évaluation.
D'autres vulnérabilités sur l'environnement ont été identifiées qui ne remettent pas en cause la sécurité du produit pour le périmètre dans les conditions d'emploi considérés.
La vulnérabilité « *Samsung Galaxy KNOX Android Browser Remote Code Execution* » a été testée ; elle s'est révélée non applicable sur la version évaluée.

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

Une vulnérabilité potentielle a été identifiée lors de l'analyse de conformité. Après avoir initié un changement de code PIN ou de méthode d'authentification dans un conteneur, un utilisateur ayant basculé hors du conteneur peut revenir sur celui-ci sans qu'il lui soit demandé de se ré-authentifier ; il peut alors définir un nouveau code PIN ou une nouvelle méthode d'authentification sans avoir à saisir le code actuel.
Moyennant le respect des recommandations formulées au 2.3.12.2, cette vulnérabilité n'est pas considérée comme critique.

2.3.11. Accès aux développeurs

Sans objet. Une fois la cible et les éléments nécessaires à l'évaluation livrés, l'évaluateur n'a pas eu à solliciter le développeur.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Plusieurs comportements limites du produit ont été identifiés ; ils tiennent essentiellement à la gestion des autorisations par liste blanche et liste noire, et à la gestion de l'authentification.
En outre, le temps minimal d'inactivité au bout duquel un conteneur est verrouillé est fixé à 5 min ; un temps plus court (de l'ordre de 30s voire 1min) offrirait un meilleur niveau de sécurité.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Il est recommandé que l'administrateur soit particulièrement vigilant dans la définition des listes blanches et des listes noires afin de ne pas compromettre la politique de sécurité.

Toute solution de MDM utilisée pour accompagner le déploiement de KNOX devrait intégrer ces particularités de fonctionnement, dans son implémentation ou à défaut dans sa documentation, laquelle doit être aussi claire et précise que possible pour l'administrateur et l'utilisateur de la solution.

L'utilisateur doit également se montrer vigilant lorsqu'il bascule entre un conteneur et une application externe ; il reste en effet authentifié dans le conteneur, et un attaquant qui prendrait possession du terminal à ce moment-là pourrait accéder au contenu du conteneur sans devoir s'authentifier.
L'utilisateur doit se montrer vigilant quant à la protection de l'accès au conteneur ; il est ainsi fortement recommander de garder le terminal sous sa surveillance dès lors qu'un conteneur est ouvert et de verrouiller systématiquement celui-ci dès qu'il n'est plus utilisé.

La sécurité de la solution évaluée repose en outre sur le respect des hypothèses définies dans la cible et qui sont rappelées au 3.2.

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

Au-delà des recommandations mentionnées au 2.3.12.2, l'utilisation du produit ne présente aucune difficulté pour l'utilisateur.
L'administrateur doit lui être particulièrement vigilant lors de la configuration ; cette tâche peut être facilitée par l'outil de MDM utilisé, l'outil EDM mis en œuvre par l'évaluateur étant un développement interne à *SAMSUNG* qui n'est pas destiné à être fourni aux clients de la solution KNOX.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques utilisés par KNOX étaient exclus du périmètre de cette évaluation.

2.4.1. Analyse du générateur d'aléas

Sans objet.

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 « Mécanisme de cloisonnement *runtime* de KNOX Workspace version 2.3 » 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 du présent rapport de certification ; le périmètre ne couvre ainsi pas toute la solution KNOX Workspace mais se limite aux fonctionnalités assurant le cloisonnement dynamique entre conteneurs.

La validité du certificat repose sur le respect des hypothèses sur l'environnement définies dans la cible de sécurité, dont certaines portent sur d'autres mécanismes de KNOX, et qui sont rappelées ici :

- le mécanisme de *Secure Boot* vérifie l'authenticité du *firmware* du téléphone lors du démarrage, protégeant contre la modification non autorisée de la chaine de *boot* (A.SECURE_BOOT) ;
- le mécanisme de *Trusted Boot* assure que l'utilisation des clés contenues dans le *Keystore* de la TIMA[1] est conditionnée à la vérification de l'intégrité des images du *bootloader* et du noyau (A.TRUSTED_BOOT) ;
- les fonctions PKM[2] et RKP[3] de la TIMA protègent contre la modification du code et des données du noyau par les processus utilisateurs et vérifient à intervalles réguliers que les mécanismes de sécurité de SE pour *Android* fonctionnent correctement. En particulier, la TIMA s'assure que SE pour *Android* fonctionne en mode *enforcing* (A.RUNTIME_INTEGRITY) ;
- le système de fichiers du conteneur est chiffré et protège les données utilisateur de façon adéquate lorsque le terminal est éteint. Les mécanismes utilisés ne permettent pas le déchiffrement des données protégées sans connaissance de la clé secrète (A.SECURE_FS) ;
- les clés utilisées pour le chiffrement du conteneur sont liées au terminal et à l'utilisateur, et sont protégées de sorte qu'il n'est pas possible pour un utilisateur ou une application non autorisé d'en faire usage (A.SECURE_FS_KEYS) ;

[1] *TrustZone-based Integrity Measurement Architecture*, mécanisme propriétaire permettant la vérification en temps réel de l'intégrité du noyau et se basant sur la technologie TrustZone d'ARM.
[2] *Periodic Kernel Measurement*, vérification périodique du noyau.
[3] *Real-time Kernel Protection*, protection temps-réel du noyau.

- la méthode d'authentification de l'utilisateur sur le conteneur est définie sur *password*. Les méthodes basées sur un motif, une empreinte ou un code PIN sont hors du périmètre de cette cible (A.USER_AUTH_PASSWORD) ;
- les applications font l'objet de vérifications par l'*Android* Package Manager pendant leur installation, leur mise à jour et leur démarrage. Les applications dont les vérifications d'intégrité échouent ne peuvent pas être installées ni utilisées. Lors de la mise à jour d'une application, vérification est faite que la mise à jour provient de la même source que l'application originale (A.APPLICATION_INTEGRITY) ;
- les processus des applications sont isolés par le mécanisme de *sandboxing* de machines virtuelles d'*Android*, ceci afin de garantir l'isolation mémoire et le contrôle des privilèges de façon dynamique (A.APPLICATION_SANDBOX) ;
- la politique MDM est fournie au terminal via un mécanisme de livraison sécurisé et authentifié. La politique MDM est gérée par un Administrateur formé et compétent, sans intentions malveillantes (A.REMOTE_MANAGEMENT) ;
- la politique SE pour *Android* ne peut être mise à jour à distance que par les serveurs de Samsung ; les mises à jour sont signées afin de garantir leur intégrité et leur authenticité. Le système refuse toute mise à jour dont la signature serait invalide. La politique SE pour *Android* ne peut être mise à jour que par un service système sur le terminal (A.MAC_POLICY_UPDATE).

Annexe 1 Références documentaires du produit évalué

[CDS]	*CSPN Security Target KNOX Container Technology* Référence : *CP-2013-RT-789-1.0-en* ; Version : 1.0-en.
[RTE]	*Rapport Technique d'Evaluation KNOX (Dispar)* *Samsung Technologie de conteneur Knox 2.3* Référence : CP-2015-RT-624-1.0 ; Version : 1.0 ; Date : 7 septembre 2015.
[GUIDES]	Guide d'utilisation : *Samsung, S14.16.Samsung KNOX User Guide Notes.D0.2* Date : 25 juin 2015.

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/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.