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-2017/14

TinySE+ revision 1.0
Matériel : SCB256I rev A
Logiciel : IOTOS version 1.1.1

Paris, le 12 juin 2017

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

Référence du rapport de certification

ANSSI-CSPN-2017/14

Nom du produit

TinySE+

Référence/version du produit

Revision 1.0

Matériel : SCB256I rev A

Logicel : IOTOS version 1.1.1

Catégorie de produit

Matériel et logiciel embarqué

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

SAFRAN Identity & Security
11 boulevard Galliéni
92130 Issy Les Moulineaux
France

Centre d'évaluation

THALES (TCS – CNES)
290 allée du Lac
31670 LABEGE
France

Fonctions de sécurité évaluées

Authentification mutuelle
Intégrité des messages
Protection contre le rejeu

Fonction(s) de sécurité non évaluées

Néant

Restriction(s) d'usage

Non

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 CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué (TOE) est « TinySE+, revision 1.0 », développé par *SAFRAN STARCHIP S.A.S.* Composée du logiciel IOTOS, lui-même exécuté sur le microcontrôleur SCB256I de *SAFRAN STARCHIP*, la TOE est destinée à être utilisée dans des objets de type Internet des objets (*Internet of Things*, IoT) pour permettre d'identifier les données provenant d'un objet IoT auprès d'un serveur distant. Une fois embarquée, la TOE est « esclave », c'est le processeur principal de l'objet qui va initier les communications avec la TOE au travers du bus I2C.

Plusieurs clés cryptographiques sont chargées lors de la production de la TOE. Le but est de pouvoir réaliser une authentification mutuelle entre la TOE et le serveur distant et également apposer un code d'authentification de message (*Message Authentication Code*, MAC) afin de garantir l'intégrité et l'authenticité des données échangées entre ces deux entités distantes.

La figure ci-dessous explicite l'architecture du produit.

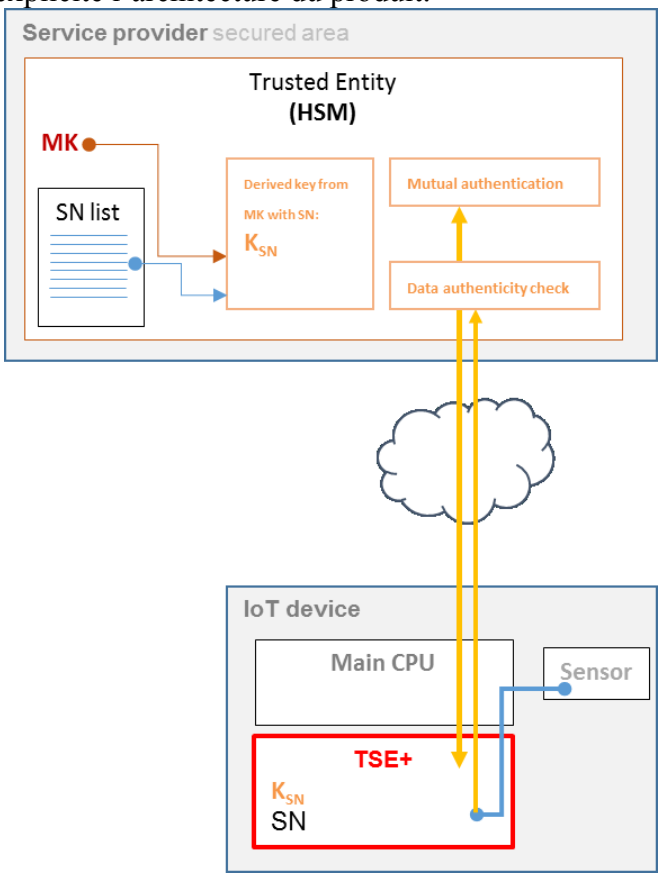

Figure 1 - Architecture Produit.

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 – pare-feu
☐ 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 – terminal de réception numérique (*Set top box*, STB)
☒ **12 – matériel et logiciel embarqué**
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	TinySE+
Numéro de la version du produit analysé	1.0
Numéro de la version du matériel	SCB256I révision A
Numéro de la version du logiciel	IOTOS 1.1.1

La version certifiée du produit peut être identifiée en utilisant les commandes suivantes :

- *READ TINY SE+ INFO* permettant d'obtenir la version du logiciel ;
- *READ OTP* permettant d'obtenir le numéro de série du matériel. De ce numéro de série on récupère le *Product ID* (21ème octet), qui doit être égal à 19, et le *Product revision* (23ème octet), qui doit être égal à 01, donnant ainsi la version SCB256I révision A.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- authentification mutuelle ;
- intégrité des messages ;
- protection contre le rejeu.

1.2.4. Configuration évaluée

Dans le cadre de l'évaluation, la TOE a été livrée sur un boîtier de type « *Dual in-line* » (DIL) permettant un accès direct au composant.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

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

2.3.1. Installation du produit

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

Dans le cadre de l'évaluation, la TOE a été livrée sur un boîtier de type « *Dual in-line* » (DIL) permettant ainsi un accès direct au composant.

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

Le produit a été livré tel que, sans être intégré dans un objet IoT.
L'évaluateur ne peut donc pas se prononcer sur cet aspect.

2.3.1.3. Durée de l'installation

Non applicable.

2.3.1.4. Notes et remarques diverses

Non applicable.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source de la partie logicielle. Il estime que le code est bien structuré, les bonnes pratiques de codages et de sécurité sont respectées.

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 [CDS].

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

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

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDE] fournis.

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

Aucun n'avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le RTE.

2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit n'implémente pas de cryptographie et n'a donc pas fait l'objet d'une analyse des mécanismes cryptographiques au titre de cette évaluation CSPN. En effet, il met en œuvre les services du composant sur lequel il s'appuie, évalué par ailleurs. Le bon usage de ces services par le produit a en revanche été vérifié.

2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

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 « TinySE+, version 1.0 » 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.
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]	*TINYSE+ CSPN SECURITY TARGET* Référence : SEC135 rev 5 ; Version : Révision 5 ; Date : *30 mars 2017*
[RTE]	*Rapport Technique d'Evaluation CSPN Projet: TINYSE+ CSPN* Référence : Johnny_CSPN_RTE ; Version : 3.0 ; Date : *31 mai 2017*
[GUIDE]	*SCB256I - SECURITY GUIDANCE* Référence : TEP072 ; Version : Révision 2 ; Date : *27 mars 2017*

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 www.ssi.gouv.fr/
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 janvier 2014 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr/.