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-2018/19

MICRO-SESAME

Version V2018.1.2.25223

Paris, le 19 octobre 2018

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2018/19

Nom du produit

MICRO-SESAME

Référence/version du produit

Version V2018.1.2.25223

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

TIL Technologies
350 rue de la Lauzière
13592 Aix-en-Provence Cedex 3

Développeur

TIL Technologies
350 rue de la Lauzière
13592 Aix-en-Provence Cedex 3

Centre d'évaluation

Oppida
4-6 avenue du vieil étang, Bâtiment B,
78180 Montigny le Bretonneux, France

Fonctions de sécurité évaluées

Protection en transmission du code PIN
Protection des données échangées entre serveur et coffrets (UTL)
Protection des données échangées entre coffrets (UTL) et modules déportés (ML-P2)
Sécurisation des coffrets (UTL)
Sécurisation des modules déportés (ML-P2)
Sécurisation du lecteur-clavier
Signature du firmware

Fonction(s) de sécurité non évaluées

Sans objet

Restriction(s) d'usage

Oui (cf. §3.2)

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 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 est « MICRO-SESAME, version V2018.1.2.25223 » développé par *TIL TECHNOLOGIES*. Ce produit est un ensemble de composants appartenant à une solution de contrôle d'accès physique.
Le produit évalué inclut :

- l'Unité de Traitement Local (UTL) représentée dans la figure 1. Ce module est également nommé TILLYS-NG dans la suite de ce document ;
- les modules d'extension ML-P2 permettant la gestion des 2 lecteurs de badges. Ce module est connecté à l'UTL par bus RS485 (Bus MLV3). Il peut être installé dans le même coffret physique que l'UTL, ou bien de façon déportée ;
- les lecteurs/claviers de modèle EVO KB LEC05XF5240-NB5 et EVO ST LEC05XF5200-NB5 (correspondant à une référence STid ARCW33BPH57AD1)[1].

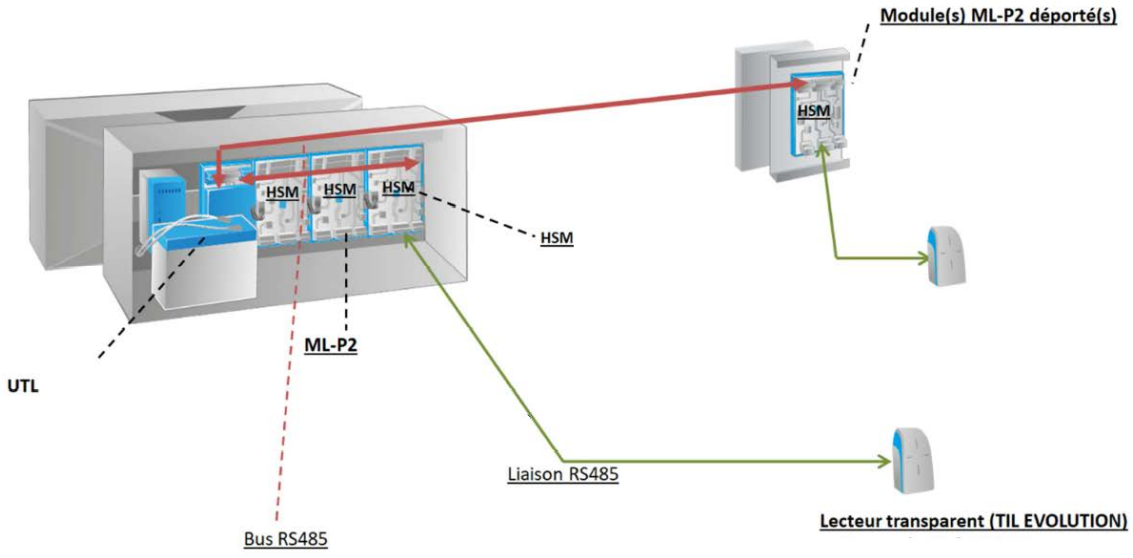

Figure 1 - Architecture du produit évalué

Le produit évalué interagit avec :

- une partie représentée dans la figure 2 sous le terme « Server ». Cette partie intègre les postes clients, les bases de données et le serveur pour la configuration et l'exploitation de la solution ;
- des badges d'accès.

[1] L'évaluation a été effectuée sur ce lecteur/clavier, mais le développeur indique également la compatibilité de l'UTL avec le lecteur transparent (sans saisie de code PIN) de référence EVO ST (LEC05XF5200-NB5).

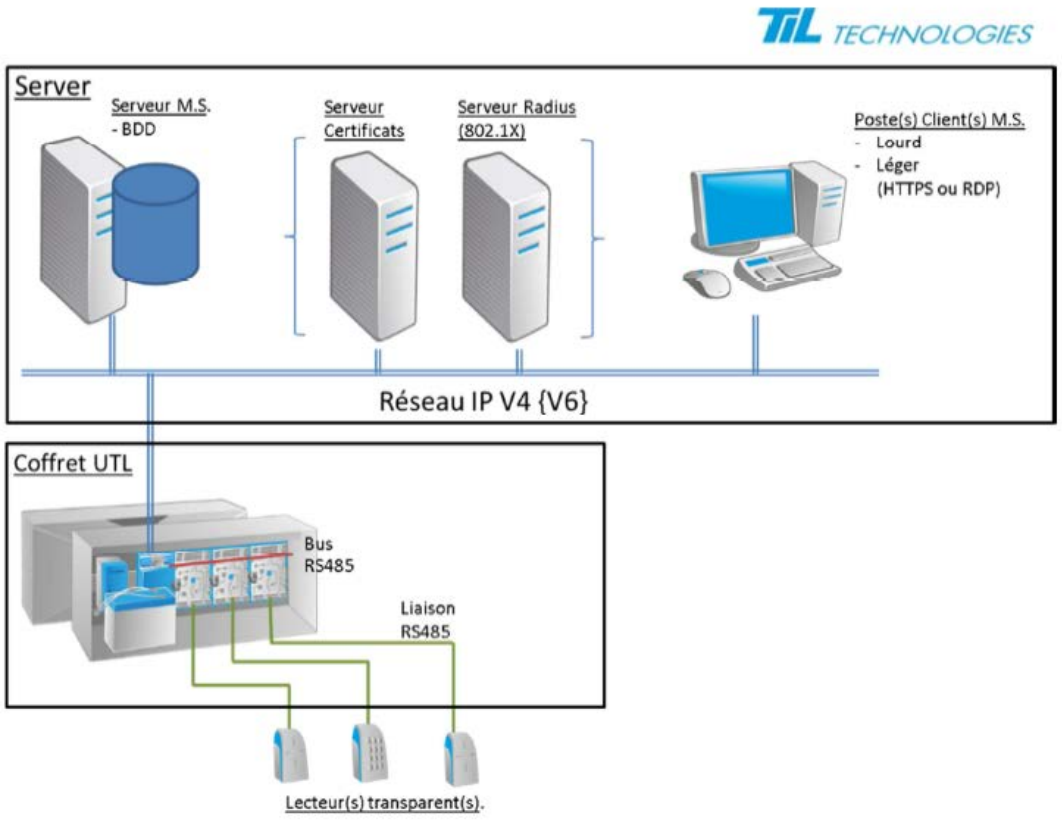

Figure 2 - Environnement du produit évalué

Pour assurer les contrôles sur les accès, le système d'accès remplit les fonctions suivantes :

- identification par badge RFID (sans contact) et authentification PIN code ;
- traitement des droits d'accès gérés au niveau du coffret d'accès (UTL) ;
- automatisme d'accès (déverrouillage, séquencement d'opérations de contrôle de l'ouvrant, état de l'accès physique) géré au niveau du coffret.

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	MICRO-SESAME
Numéro de la version évaluée	V2018.1.2.25223, correspondant - au TILLYS-NG version V2.0.0.5961 - aux modules ML-P2 version V2.0.0.878 et V2.0.0.953 - aux lecteurs transparents : o EVO ST (LEC05XF5200-NB5) o EVO KB (LEC05XF5240-NB5)[1]

[1] L'évaluation a été effectuée sur ce lecteur/clavier, mais le développeur indique également la compatibilité de l'UTL avec le lecteur transparent (sans saisie de code PIN) de référence EVO ST (LEC05XF5200-NB5).

L'identification du produit évalué est possible au travers de l'interface d'administration du TILLYS-NG. Les versions sont les suivantes :

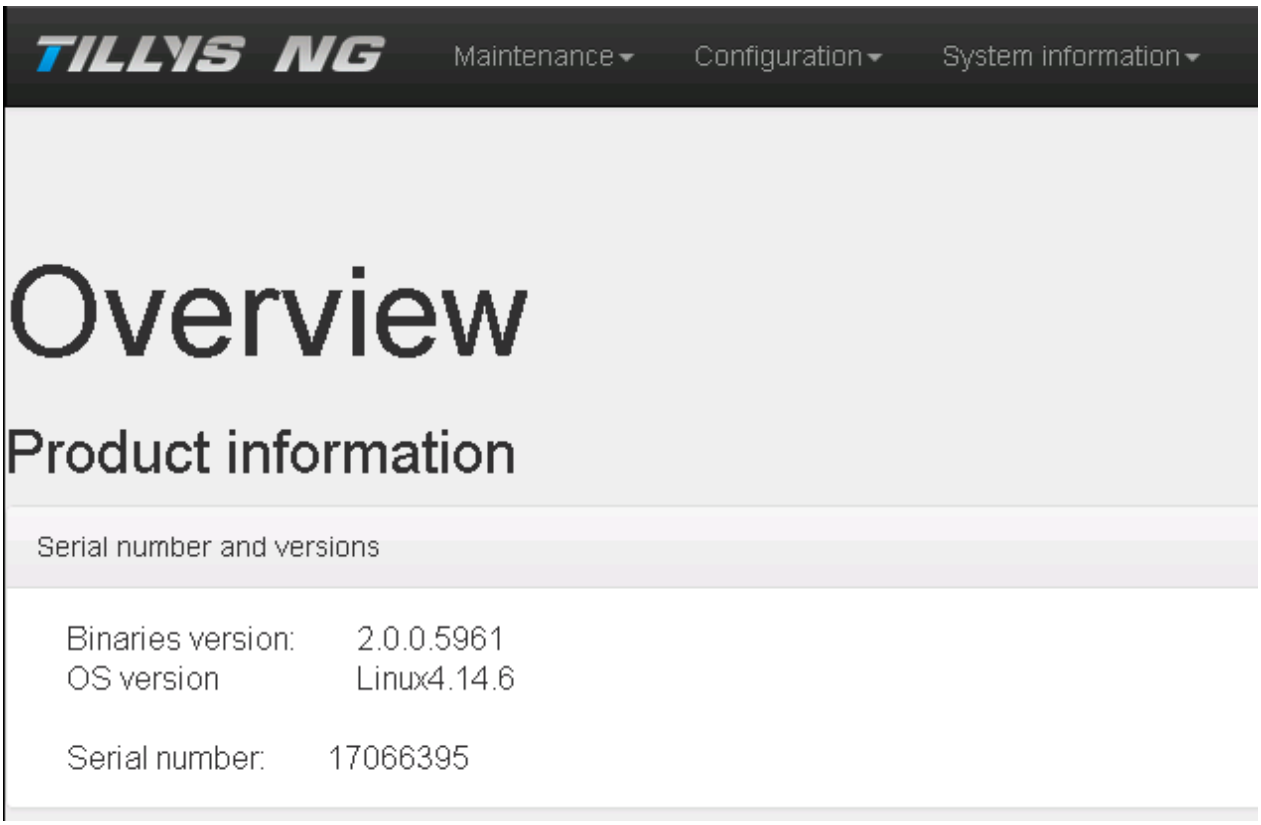

Figure 3 : Identification de la version des binaires du TILLYS-NG

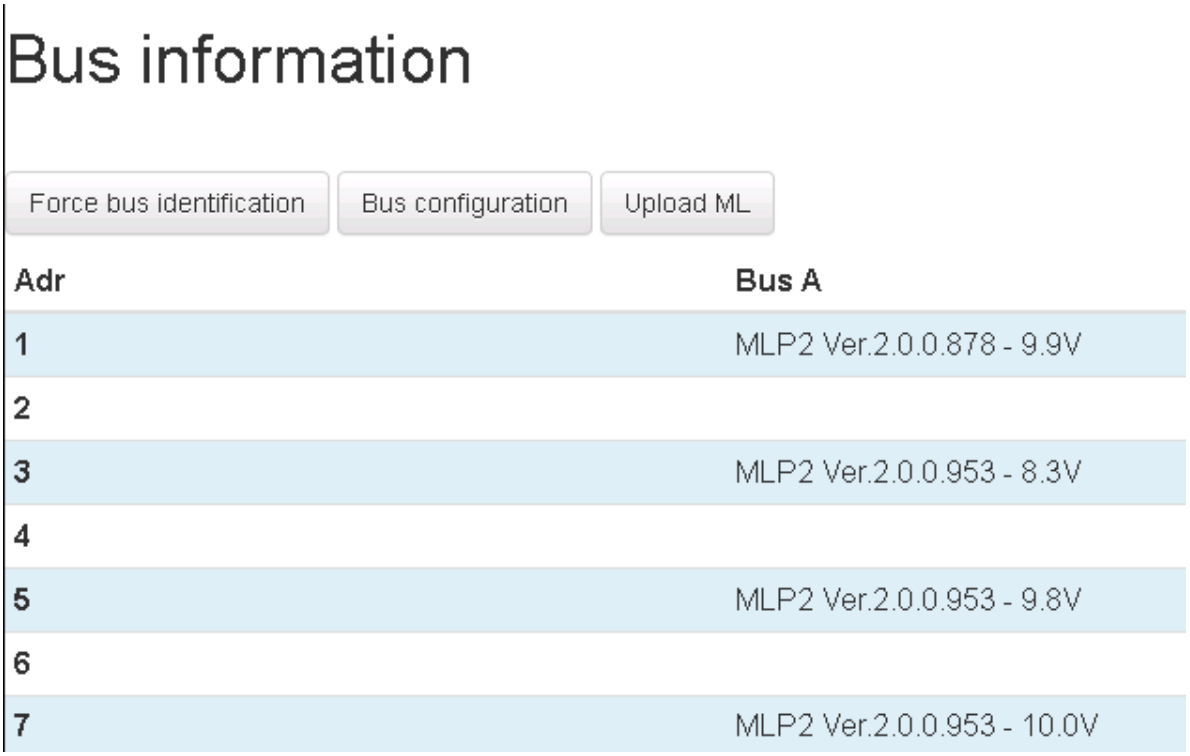

Figure 4 : Identification de la version des modules déportés

L'identification des lecteurs de badge se fait par lecture de l'étiquette située à l'intérieur du lecteur. Cela ne peut donc se faire que lors de l'installation ou de la maintenance.

1.2.3. **Fonctions de sécurité**

Les fonctions de sécurité évaluées du produit sont :

- protection en transmission du code PIN ;
- protection des données échangées entre serveur et coffrets (UTL) ;
- protection des données échangées entre coffrets (UTL) et modules déportés (ML-P2) ;
- sécurisation des coffrets (UTL) ;
- sécurisation des modules déportés (ML-P2) ;
- sécurisation du lecteur-clavier ;
- signature du firmware.

1.2.4. **Configuration évaluée**

Le module TILLYS NG permet plusieurs configurations :

- TILLYS-NG + Configuration 1 bus ;
- TILLYS-NG + Configuration 2 bus ;
- TILLYS-NG + Configuration 3 bus.

La configuration évaluée est la configuration « TILLYS-NG + configuration 1 bus ».

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

Le produit (ULT, modules déportés et lecteurs) a été relié à une maquette de test.

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

L'installation du produit a été effectuée avec l'aide des équipes du développeur. Le socle logiciel nécessaire à la TOE a été livré préconfiguré sur un PC dédié.
L'évaluateur n'a pas eu besoin d'installer et configurer la TOE et recommande de se faire assister par le développeur durant cette phase.

2.3.1.3. Durée de l'installation

Le temps total d'installation et de configuration a duré une demi-journée.

2.3.1.4. Notes et remarques diverses

Sans objet.

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 eu accès au code source dans le cadre de l'analyse des mécanismes cryptographiques.

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

Des vulnérabilités potentielles connues ont été identifiées sur le produit, et les briques tierces qu'il utilise. Cependant, elles sont considérées comme non exploitables dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

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

Un entretien avec les développeurs durant une journée a été effectué afin d'installer la TOE. Cette entrevue a permis d'apporter des éclaircissements concernant l'architecture matérielle et logicielle de la TOE.

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 a identifié un point de configuration pouvant mener à un affaiblissement de la sécurité du système, qui donne lieu à recommandations dans la section suivante.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Le certificat de la console web du boîtier TILLYS NG est auto signé lors de la livraison de l'environnement. Il est recommandé de mettre à jour ce certificat avant toute configuration de la TOE et de s'assurer que l'on n'est pas en zone hostile lors de cette manipulation. Ce point constitue une restriction d'usage (voir section 3.2).
Plus généralement, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées.

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

Le CESTI a relevé que l'administrateur du produit aura besoin de l'assistance du développeur lors de l'installation et de la configuration 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

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. L'évaluateur n'a pas relevé de vulnérabilité exploitable, dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.5. Analyse du générateur d'aléas

L'évaluateur n'a pas relevé de vulnérabilité exploitable, dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré, concernant les générateurs d'aléa mis en œuvre par le produit.

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 « MICRO-SESAME, version V2018.1.2.25223 » 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 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).
La sécurité du produit est fortement dépendante de sa bonne installation et de sa bonne configuration initiale, qui ne sont pas garanties par l'évaluation du produit. Il est donc impératif que ces phases soient réalisées par des intégrateurs compétents et de confiance.
Par ailleurs, l'administrateur ou installateur du produit devra installer un certificat signé en lieu et place du certificat auto-signé de la console web du coffret TILLYS-NG (UTL). Cette manipulation doit avoir lieu avant toute configuration de la TOE, et être effectuée en zone non hostile.
Enfin, le présent rapport de certification ne se prononce pas sur la résistance des UTLs à une attaque physique – il est donc impératif que les concentrateurs d'accès soient installés et manipulés en zone non hostile, par des personnels compétents et de confiance.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité –Contrôle des accès - MICRO-SESAME V2018.1* Référence : N/A ; Version : *3.4* ; Date : *9 juillet 2018*
[RTE]	*Rapport Technique d'Evaluation CSPN MICRO-SESAME3* Référence : OPPIDA/CESTI/MICRO-SESAME3/RTE ; Version : 1.2 (référencé OPPIDA/CESTI/MICRO-SESAME3/RTE/2) ; Date : *17 septembre 2018*

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 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.