PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2022/04

MICRO-SESAME

Version M.S. V2021.1.0.11539, TILLYS-CUBE V5.1.2.8556, MLP2 V5.0.0.1757

Paris, le 26 avril 2022

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-2022/04**
Nom du produit **MICRO-SESAME**
Référence/version du produit **Version M.S. V2021.1.0.11539, TILLYS-CUBE V5.1.2.8556, MLP2 V5.0.0.1757**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **TIL TECHNOLOGIES** Parc du Golf 350, rue de la Lauzière 13592 Aix-en-Provence Cedex 3
Développeur **TIL TECHNOLOGIES** Parc du Golf 350, rue de la Lauzière 13592 Aix-en-Provence Cedex 3
Centre d'évaluation **Thales SIX GTS** 290 allée du Lac 31670 Labège
Fonctions de sécurité évaluées Authentification et contrôle d'accès des exploitants et opérateurs Etablissement d'un canal protégé serveur MS – Postes Client Protection de la transmission du code PIN Protection des données échangées entre le serveur MS et les UTL TILLYS-CUBE Protection des données échangées entre les UTL et les modules déportés MLP2 Sécurisation des UTL TILLYS-CUBE Sécurisation des modules déportés MLP2 Sécurisation du lecteur-clavier Signature du *firmware*
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est «MICRO-SESAME, Version M.S. V2021.1.0.11539, TILLYS-CUBE V5.1.2.8556, MLP2 V5.0.0.1757» développé par TIL TECHNOLOGIES.

MICRO-SESAME est une solution intégrée permettant une gestion centralisée et en temps réel des accès physiques.

Les fonctions d'accès sont gérées par une application métier « MS Serveur », qui permet :

- de référencer de façon unique les usagers dans la base de données côté « Serveur » ;
- de donner des droits d'accès au personnel de l'entreprise/société et aussi aux visiteurs ;
- de référencer les éléments de sécurité SI (droits d'administration, droits d'accès au SI,…).

Pour répondre à ces besoins, la solution MICRO-SESAME repose sur :

- des équipements côté application métier :
  - un serveur et base de données centrale ;
  - des postes clients pour l'exploitation.
- des équipements de terrain :
  - des coffrets UTL (enveloppe métallique) avec le module de base TILLYS-CUBE et un système d'alimentation en énergie (alimentation secourue) ;
  - des modules d'extension MLP2 qui peuvent être situés dans le coffret (jusqu'à 4 modules d'extension), ou déportés (jusqu'à 4 unités déportées) ;
  - des lecteurs de badges (TIL EVOLUTION) ;
  - des badges d'accès (MIFARE DESFire EV2).

Le tableau ci-dessous synthétise le périmètre de l'évaluation :

Composant du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE), supposé de confiance
GAC	Système d'exploitation		Microsoft Windows Server 2019
	Applicatifs	Application métier MS Serveur	
	Fonctions cryptographiques	OpenSSL version 1.1.1h	
	Bases de données et annuaires		Microsoft SQL
UTL : Modules TILLYS-CUBE + MLP2	Système d'exploitation	Linux 5.4.77	
	Applicatifs	Microsesame	
	Fonctions cryptographiques	OpenSSL version 1.1.1g FreeRTOS 10.0.0 PolarSSL 0.14.0[1]	
	SAM		HSM WiseKey VaultIC420
Lecteurs	Lecteurs simples	TIL EVOLUTION EVO ST, réf. LEC05XF5200-NB5	
	Lecteurs-clavier	TIL EVOLUTION EVO KB, réf. LEC05XF5240-NB5	
Badges			MIFARE DESFire EV2

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

[1] Cette version de PolarSSL n'est plus maintenue, ce qui aurait pu mener à un échec de certification. Cependant, le produit n'utilise, de cette librairie, que des primitives cryptographiques AES. Le code source de ces mécanismes a été revu intégralement par le CESTI, qui n'a pas identifié de vulnérabilité exploitable pour le niveau d'attaquant visé.

☐ 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*

Produit	
Nom du produit	MICRO-SESAME
Numéro de la version évaluée	M.S. V2021.1.0.11539 TILLYS-CUBE V5.1.2.8556 MLP2 V5.0.0.1757

La version certifiée du logiciel de gestion peut être identifiée via les propriétés de l'exécutable « se_menu.exe » dans le répertoire d'installation du logiciel MICRO- SESAME :

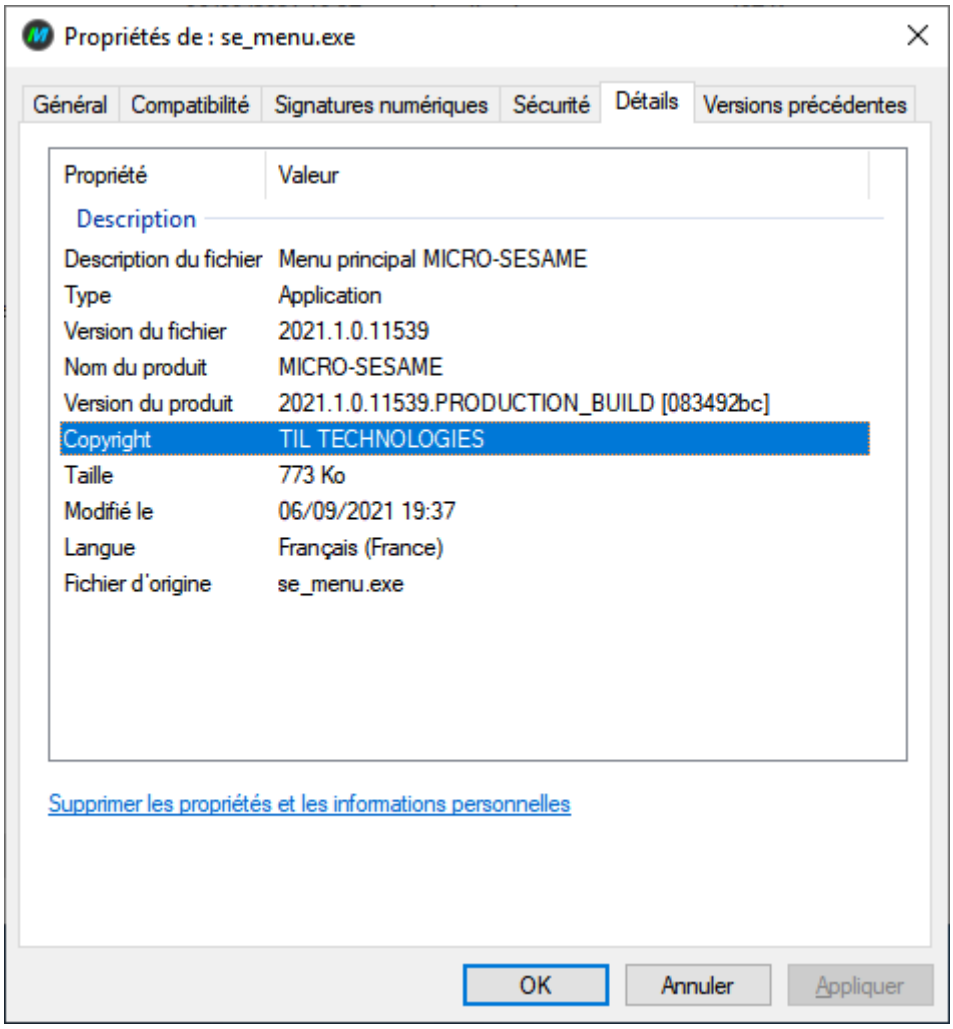

Figure 1 : Identification de la version : composant M.S. V2021.1.0.11539

La version de l'UTL TILLYS CUBE et la version des modules MLP2 peuvent être identifiées via l'interface de gestion.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification et le contrôle d'accès des exploitants et opérateurs ;
- l'établissement d'un canal protégé entre serveur MS et postes Client ;
- la protection de la transmission du code PIN ;
- la protection des données échangées entre le serveur MS et les UTL TILLYS-CUBE ;
- la protection des données échangées entre les UTL et les modules déportés MLP2 ;
- la sécurisation des UTL TILLYS-CUBE ;
- la sécurisation des modules déportés MLP2 ;
- la sécurisation du lecteur –clavier ;
- la signature du *firmware*.

1.2.4 *Configuration évaluée*

La solution offre plusieurs cas d'installation possibles :

- installation simple autonome (sans serveur MICRO-SESAME) ;
- installation complète autonome (avec serveur MICRO-SESAME) ;
- installation complète, intégrée au sein du réseau d'entreprise (annuaire d'entreprise, base de données externe).

Le cas évalué est une **installation complète autonome**.

L'installation a été réalisée en suivant les procédures et directives décrites dans [GUIDES].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-07].

2.2 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].

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Le développeur a installé le produit dans les locaux de l'évaluateur et a expliqué son fonctionnement.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit et fourni les résultats de l'analyse dans le rapport d'analyse cryptographique [ANA_CRY].

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS]

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations et des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est complet et comporte de nombreuses fonctionnalités permettant de s'adapter à la majorité des situations, ce qui rend également sa prise en main complexe.

Néanmoins, les documents [GUIDES] sont clairs en ne conduisent pas à une utilisation non sécuritaire du produit.

2.2.7.3 Notes et remarques diverses

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

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 M.S. V2021.1.0.11539, TILLYS-CUBE V5.1.2.8556, MLP2 V5.0.0.1757 » 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 Recommandations et 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 suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- 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 ;
- 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-CUBE (UTL). Cette manipulation doit avoir lieu avant toute configuration de la TOE et être effectuée en zone non hostile.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité MICRO-SESAME et TILLYS CUBE, version 4.4 du 8 mars 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation CSPN, Projet : MICRO-SESAME et TILLYS CUBE, référence MSTC_CSPN_RTE, version 2.1 du 1er avril 2022.
[ANA_CRY]	Rapport d'expertise cryptographique : - Analyse des mécanismes cryptographiques MICRO-SESAME et TILLYS CUBE, référence MSTC_CRY, version 1.1 du 16 juin 2021.
[GUIDES]	Guides d'utilisation, administration et installation du produit : - Guide Administration et Sécurité, version 2.6 du 17 décembre 2020 ; - Guide de mise en place des certificats TLS, version du 21 décembre 2020 - Architecture Informatique MICRO-SESAME 2020, version du 12 novembre 2020 ; - Guide sur le contrôle d'accès basique, version 1.3 du 6 Janvier 2021 ; - Guide d'installation, migration et restauration MICRO-SESAME, version du 17 décembre 2020 ; - Prérequis d'installation MICRO-SESAME CUBE, version 1.0 du 23 décembre 2020 ; - Protocole MLv3, version 1.2 ; - Spécification TILLYS NG des échanges *multi-cast*, version 1.0 ; - Protocole de communication SSCP V2 Firmware Z14, version 1.8 ; - Guide de configuration TILLYS CUBE 5.x, version du 14 janvier 2021. Guides cryptographiques : - Guide KeySecureManager NG ; - Guide de création et de mise en place d'une ligne de communication TLS, version 1.2 du 14 décembre 2020 ;

ANNEXE B. Références liées 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, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 20022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-07]	Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version 1.0, 7 juillet 2020.