



**PREMIÈRE  
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-2023/18

## **MICRO-SESAME**

**Version M.S. V2023.2.1.0, TILLYS-CUBE V6.0.2, MLP2 V6.0.1**

Paris, le 19 Janvier 2024

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

Vincent STRUBEL

[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 présumées 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](mailto:certification@ssi.gouv.fr)

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

|                                       |   |
|---------------------------------------|---|
| Référence du rapport de certification | <b>ANSSI-CSPN-2023/18</b>   |
| Nom du produit                        | <b>MICRO-SESAME</b>   |
| Référence/version du produit          | <b>Version M.S. V2023.2.1.0, TILLYS-CUBE V6.0.2, MLP2 V6.0.1</b>  |
| Catégorie de produit                  | <b>Identification, authentification et contrôle d'accès</b>   |
| Critère d'évaluation et version       | <b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU<br/>(CSPN)</b>   |
| Commanditaire                         | <b>TIL TECHNOLOGIES</b><br>Parc du Golf<br>350, rue de la Lauzière<br>13592 Aix-en-Provence Cedex 3, France   |
| Développeur                           | <b>TIL TECHNOLOGIES</b><br>Parc du Golf<br>350, rue de la Lauzière<br>13592 Aix-en-Provence Cedex 3, France   |
| Centre d'évaluation                   | <b>THALES / CNES</b><br>290, allée du Lac<br>31670 Labège, France   |
| Fonctions de sécurité évaluées        | <b>Authentification et contrôle d'accès des exploitants et opérateurs</b><br><b>Etablissement d'un canal protégé serveur M.S. – Postes Client</b><br><b>Protection en transmission du code PIN</b><br><b>Protection des données échangées entre le serveur M.S. et les UTL TILLYS-CUBE</b><br><b>Protection des données échangées entre les UTL et les modules déportés MLP2</b><br><b>Sécurisation des UTL TILLYS-CUBE</b><br><b>Sécurisation des modules déportés MLP2</b><br><b>Sécurisation du lecteur-clavier</b><br><b>Signature du <i>firmware</i></b> |
| Fonctions de sécurité non évaluées    | <b>Sans objet</b>   |
| Restriction(s) d'usage                | <b>Non</b>  |

## 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.cyber.gouv.fr](http://www.cyber.gouv.fr).

## TABLE DES MATIERES

|           |  |    |
|-----------|--|----|
| 1         | Le produit.....  | 6  |
| 1.1       | Présentation du produit.....   | 6  |
| 1.2       | Description du produit évalué.....                                     | 7  |
| 1.2.1     | Catégorie du produit.....  | 7  |
| 1.2.2     | Identification du produit.....   | 8  |
| 1.2.3     | Fonctions de sécurité.....   | 9  |
| 1.2.4     | Configuration évaluée.....   | 9  |
| 2         | L'évaluation.....  | 10 |
| 2.1       | Référentiels d'évaluation.....   | 10 |
| 2.2       | Travaux d'évaluation.....  | 10 |
| 2.2.1     | Installation du produit.....   | 10 |
| 2.2.2     | Analyse de la documentation.....                                       | 10 |
| 2.2.3     | Revue du code source (facultative).....                                | 10 |
| 2.2.4     | Analyse de la conformité des fonctions de sécurité.....                | 10 |
| 2.2.5     | Analyse de la résistance des mécanismes des fonctions de sécurité..... | 10 |
| 2.2.6     | Analyse des vulnérabilités (conception, construction, etc.).....       | 11 |
| 2.2.7     | Analyse de la facilité d'emploi.....                                   | 11 |
| 2.3       | Analyse de la résistance des mécanismes cryptographiques.....          | 12 |
| 2.4       | Analyse du générateur d'aléa.....                                      | 12 |
| 3         | La certification.....  | 13 |
| 3.1       | Conclusion.....  | 13 |
| 3.2       | Recommandations et restrictions d'usage.....                           | 13 |
| ANNEXE A. | Références documentaires du produit évalué.....                        | 14 |
| ANNEXE B. | Références liées à la certification.....                               | 15 |

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « MICRO-SESAME, Version M.S. V2023.2.1.0, TILLYS-CUBE V6.0.2, MLP2 V6.0.1 » 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 « Serveur Micro-Sésame », 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 Serveur Micro-Sésame :
  - o un serveur et base de données centrale ;
  - o des postes clients pour l'exploitation.
- des équipements de terrain :
  - o des coffrets UTL (enveloppe métallique) avec le module de base TILLYS-CUBE et un système d'alimentation en énergie (alimentation secourue) ;
  - o 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) ;
  - o des lecteurs de badges (TIL EVOLUTION) ;
  - o 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<br>Microsoft Windows 10 (64 bits) |
|   | Applicatifs                   | Application métier<br>Serveur Micro-Sésame        |   |
|   | Fonctions cryptographiques    | OpenSSL version 1.1.1t                            |   |
|   | Bases de données et annuaires |   | Microsoft SQL   |
| UTL :<br>Modules<br>TILLYS-CUBE<br>+ MLP2 | Système d'exploitation        | Linux 5.15.91                                     |   |
|   | Applicatifs                   | Micro-Sésame                                      |   |
|   | Fonctions cryptographiques    | FreeRTOS 10.0.0                                   |   |
|   | SAM                           |   | HSM WiseKey Vault IC420   |
| Lecteurs                                  | Lecteurs simples              | TIL EVOLUTION EVO<br>ST, réf. LEC05XF5200-<br>NB5 |   |
|   | Lecteurs-clavier              | TIL EVOLUTION EVO<br>KB, réf. LEC05XF5240-<br>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

|                                     |    |   |
|-------------------------------------|----|---|
| <input type="checkbox"/>            | 1  | détection d'intrusions                                      |
| <input type="checkbox"/>            | 2  | anti-virus, protection contre les codes malicieux           |
| <input type="checkbox"/>            | 3  | pare-feu  |
| <input type="checkbox"/>            | 4  | effacement de données                                       |
| <input type="checkbox"/>            | 5  | administration et supervision de la sécurité                |
| <input checked="" type="checkbox"/> | 6  | <b>identification, authentification et contrôle d'accès</b> |
| <input type="checkbox"/>            | 7  | communication sécurisée                                     |
| <input type="checkbox"/>            | 8  | messaging sécurisée   |
| <input type="checkbox"/>            | 9  | stockage sécurisé   |
| <input type="checkbox"/>            | 10 | environnement d'exécution sécurisé                          |
| <input type="checkbox"/>            | 11 | terminal de réception numérique (Set top box, STB)          |
| <input type="checkbox"/>            | 12 | matériel et logiciel embarqué                               |
| <input type="checkbox"/>            | 13 | automate programmable industriel                            |
| <input type="checkbox"/>            | 99 | autre   |

### 1.2.2 Identification du produit

| Produit                      |   |
|------------------------------|---|
| Nom du produit               | MICRO-SESAME  |
| Numéro de la version évaluée | M.S. V2023.2.1.0<br>TILLYS-CUBE V6.0.2<br>MLP2 V6.0.1 |

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

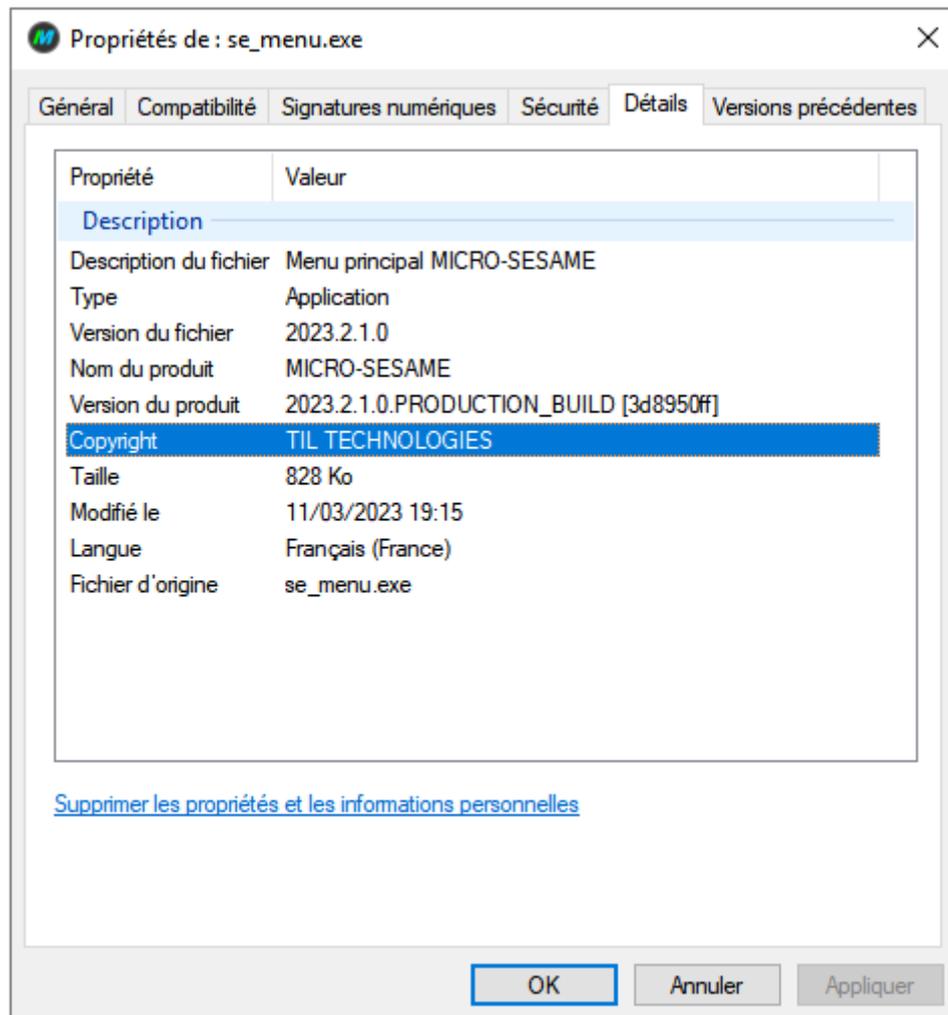


Figure 1 : Identification de la version du logiciel de gestion MICRO-SESAME

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 le serveur M.S. et les postes client ;
- la protection de la transmission du code PIN ;
- la protection des données échangées entre le serveur M.S. 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 Installation du produit

##### 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 du présent rapport de certification .

##### 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.

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 inexploitable 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 inexploitable 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

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

### 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. V2023.2.1.0, TILLYS-CUBE V6.0.2, MLP2 V6.0.1 » 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].

## ANNEXE A. Références documentaires du produit évalué

|           |   |
|-----------|---|
| [CDS]     | Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none"><li>- Cible de sécurité CSPN Contrôle des accès physiques MICRO-SESAME &amp; TILLYS CUBE HIGH SECURE, version 4.7, 5 septembre 2023.</li></ul>   |
| [RTE]     | Rapport technique d'évaluation : <ul style="list-style-type: none"><li>- Rapport Technique d'Evaluation CSPN MSTC2, référence MSTC2_CSPN_RTE_FR, version 1.3, 8 décembre 2023.</li></ul>  |
| [ANA_CRY] | Rapport d'expertise cryptographique : <ul style="list-style-type: none"><li>- Analyse des mécanismes cryptographiques MSTC2, référence MSTC2 CRY, version 1.2, 22 novembre 2023.</li></ul>  |
| [GUIDES]  | Guides d'utilisation, administration et installation du produit : <ul style="list-style-type: none"><li>- Guide Administration et Sécurité MICRO-SESAME 2023, version 1.9, 7 septembre 2023 ;</li><li>- Guide de mise en place des certificats TLS, version 1.49, 13 mars 2023</li><li>- Architecture Informatique MICRO-SESAME, version 1.21, 13 mars 2023 ;</li><li>- Guide d'installation, migration et restauration MICRO-SESAME, version du 1.7, 13 mars 2023 ;</li><li>- Prérequis d'installation MICRO-SESAME CUBE, version 1.22, 13 mars 2023 ;</li><li>- Guide de mise en sécurité des lecteurs transparents, version 1.14, 13 mars 2023</li><li>- Guide de paramétrage d'une applet, version 1.13, 6 septembre 2023</li></ul> |

## **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 5.0, 12 janvier 2023.<br><br>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.<br><br>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, 26 janvier 2021.   |
| [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.  |