PREMIER MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CSPN-2026/06

MICROSESAME & TILLYS-CUBE HIGH SECURE

Version MICROSESAME V2025.2.1, TILLYS-CUBE V8.0.1, MLP2 V8.0.1

Paris, le 17/6/2026 | 17:57 CEST

Vincent Strubel

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2026/06

Nom du produit

MICROSESAME & TILLYS-CUBE HIGH SECURE

Référence/version du produit

Version MICROSESAME V2025.2.1, TILLYS-CUBE V8.0.1, MLP2 V8.0.1

Catégorie de produit

Système de contrôle d'accès physique

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

HIRSCH
Parc du Golf, 350 rue de la Lauzière
13592 Aix-en-Provence Cedex 3, France

Développeur

HIRSCH
Parc du Golf, 350 rue de la Lauzière
13592 Aix-en-Provence Cedex 3, France

Centre d'évaluation

THALES / CNES
290, allée du Lac
31670 Labège, France

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Authentification et contrôle d'accès des exploitants et opérateurs
Etablissement d'un canal protégé serveur MS – Postes Client
Protection en transmission du code PIN
Protection des données échangées entre le serveur MS et les UTL TILLYS-CUBE
Protection des données échangées entre les TILLYS-CUBE 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	Non

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 cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « MICROSESAME & TILLYS-CUBE HIGH SECURE, Version MICROSESAME V2025.2.1, TILLYS-CUBE V8.0.1, MLP2 V8.0.1 » développé par HIRSCH.

Ce produit constitue une solution intégrée permettant une gestion centralisée et en temps réel des accès physiques.

La solution est composée :

- d'une partie « GAC » (Gestion des Accès Contrôlés) intégrant :
  - un serveur de base de données ;
  - un serveur hébergeant les applications de paramétrage et d'exploitation du contrôle d'accès ;
  - un serveur de certificat (non fourni) ;
  - un serveur RADIUS (non fourni) ;
  - des postes clients pour l'exploitation de la solution.
- d'une partie « UTL » (Unité de Traitement Logique) et « Lecteurs et badges » intégrant les équipements de terrain :
  - alimentation secourue avec batterie ;
  - modules de base TILLYS-CUBE ;
  - modules d'extension MLP2 (pour la gestion de deux lecteurs de badge), pouvant être déportés via des bus RS485 (MLV3) ;
  - lecteurs de badge avec et sans clavier ;
  - badges d'accès (MIFARE DESFire EV3).

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 2025
	Applicatifs	Application de gestion MICROSESAME 2025.2.1	
	Fonctions cryptographiques	TLS 1.3 OpenSSL 3.4.0	
	Bases de données et annuaires		Microsoft SQL Server 2022
UTL	Système d'exploitation	TILLYS-CUBE : Linux 6.12.41 MLP2 : FreeRTOS 11.1.0	
	Applicatifs	TILLYS-CUBE : 8.0.1 MLP2 : 8.0.1	
	Fonctions cryptographiques	TLS 1.3.3 OpenSSL 3.4.2	
	SAM		HSM WiseKey Vault IC420

Lecteurs	Lecteurs simples	STID ARC-W33-A/Ph5-7ADyZ23	
	Lecteurs-clavier	STID ARC-W33-B/Ph5-7ADyZ23	
Badges			MIFARE DESFire EV3

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 malveillants
☐	3	Pare-feu
☐	4	Passerelle-multiniveau
☐	5	Effacement de données
☐	6	Administration et supervision de la sécurité
☐	7	Moyen d'authentification numérique
☒	**8**	**Système de contrôle d'accès physique**
☐	9	Communication sécurisée
☐	10	Messagerie sécurisée
☐	11	Stockage sécurisé
☐	12	Environnement d'exécution sécurisé
☐	13	Matériel avec logiciel embarqué
☐	14	SCADA
☐	15	Automate programmable industriel
☐	16	Système de vidéoprotection
☐	99	Autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	**MICROSESAME & TILLYS-CUBE HIGH SECURE**
Numéro de la version évaluée	**Version MICROSESAME V2025.2.1, TILLYS-CUBE V8.0.1, MLP2 V8.0.1**

La version certifiée du produit peut être identifiée de la manière suivante :

- pour l'application de gestion MICROSESAME : se connecter à l'application et dans le menu principal, aller dans la section « A propos » ou « ? » et sélectionner le programme « se_menu.exe » pour afficher la version :

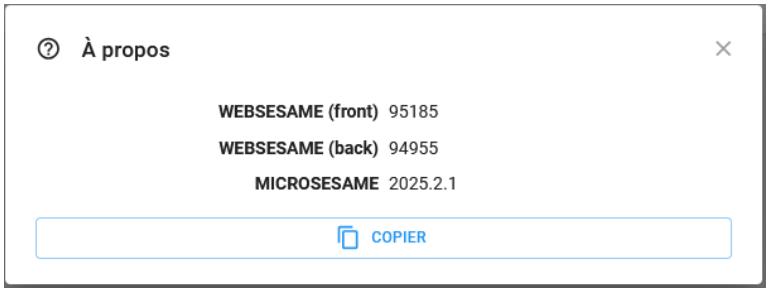

Figure 1 : Version application de gestion MICRO-SESAME

- pour les UTL TILLYS-CUBE : se connecter à l'interface de gestion et aller dans la section « Version et numéro de série » :

Figure 2 : Version application UTL TILLYS-CUBE

- pour les modules déportés MLP2 : se connecter à l'interface de gestion et aller dans la section « Matériel » et « Diagnostic du bus » :

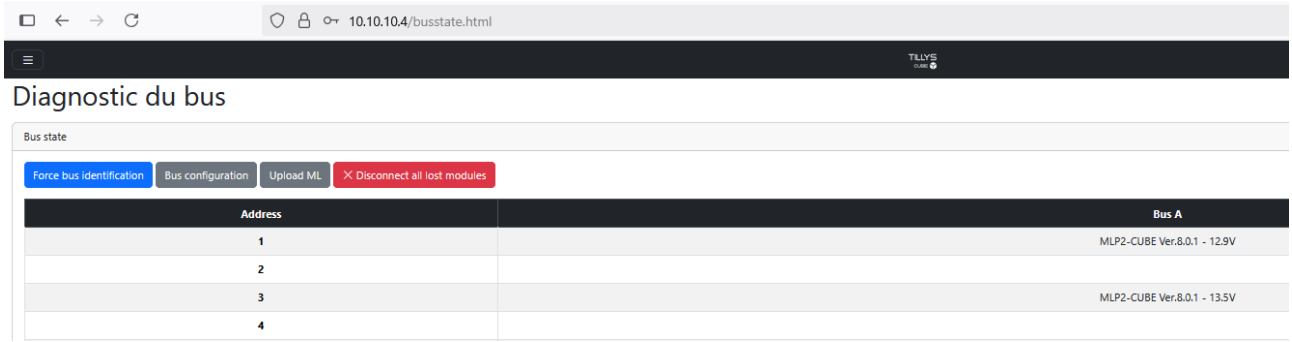

Figure 3 : Version modules déportés MLP2

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 MS et les Postes Client ;
- la protection en 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 TILLYS-CUBE 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 MICROSESAME) ;
- installation complète autonome (avec serveur MICROSESAME) ;
- installation complète intégrée au sein du réseau d'entreprise (annuaire d'entreprise, base de données externe) ;

et trois niveaux de sécurité : élémentaire, standard, renforcé.

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

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.

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

L'installation du produit a été réalisé par le développeur avec un suivi des procédures par l'évaluateur.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

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 inexploitables 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

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

2.2.7 *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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi 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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont 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 « MICROSESAME & TILLYS-CUBE HIGH SECURE, Version MICROSESAME V2025.2.1, TILLYS-CUBE V8.0.1, MLP2 V8.0.1 » 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].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (*Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN – Contrôle des accès physiques – MICROSESAME & TILLYS-CUBE HIGH SECURE, version 4.10, 29/09/ 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Cible de sécurité CSPN – Contrôle des accès physiques – MICROSESAME & TILLYS-CUBE HIGH SECURE, version 4.11, 22/05/2026.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN, référence CSPN_MICROSESAME_2024, version 1.3, 21/05/2026.
[ANA_CRY]	Rapport d'expertise cryptographique : - Analyse des mécanismes cryptographiques – MICROSESAME CUBE, référence CSPN_MICROSESAME_2024_CRY, version 1.1, 11/05/2026.
[GUIDES]	Guides d'utilisation, d'administration et d'installation du produit : - Administration et sécurité d'un système MICROSESAME, référence GU-15007-FR, 2 décembre 2025 ; - Installation, migration et restauration de MICROSESAME, référence GU-10020-FR, 25 juillet 2025 ; - Guide de paramétrage applet pour ML 5.x et UTL 6.x, référence GU-10017-FR, 4 juillet 2026 ; - Guide de référence MICROSESAME 2025, référence GR-10014-FR, 29 octobre 2025 ; - Guide de référence TILLYS-CUBE 7.0, référence GR-10012-FR, version 7.0, 2 juillet 2025.

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 7.0,12 mai 2026. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2024 Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 juillet 2024.
[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 2.2, 28 octobre 2025.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement*,version 3.0, mai 2026.