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-2021-33

COSMOS (UTL SYRIUS 2P2L-EXT version 1661z, UTL ORION 4P-8L-EXT version 1661z)

Version 4.6.0.96

Paris, le 14 janvier 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-2021/33**
Nom du produit **COSMOS** **(UTL SYRIUS 2P2L-EXT version 1661z,** **UTL ORION 4P-8L-EXT version 1661z)**
Référence/version du produit **Version 4.6.0.96**
Catégorie de produit **identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **ELSYLOG** 10-12 rue Marcel Paul Parc d'activités Les Berges de Seine 3 95070 Bezons France
Développeur **ELSYLOG** 10-12 rue Marcel Paul Parc d'activités Les Berges de Seine 3 95070 Bezons France
Centre d'évaluation **OPPIDA** 6 avenue du Vieil Etang 78180 Montigny le Bretonneux France
Fonctions de sécurité évaluées Protection des communications entre le lecteur et l'UTL Protection des communications entre l'UTL et le GAC COSMOS Protection des communications entre l'UTL et COMET Protection des communications entre COMET et le GAC COSMOS Protection du code PIN Protection contre l'arrachement de l'UTL Détection d'ouverture et d'arrachement de la tête de lecture du lecteur de Proximité Protection du *firmware* de l'UTL Détection de court-circuit ou de coupure de boucle de la fonction associée au bouton poussoir de sortie Détection de court-circuit ou coupure de boucle de la surveillance de l'accès l'entrée Protection des données utilisateur pour l'authentification Cloisonnement entre les différents comptes utilisateurs Échanges clients/serveur Cosmos Protection de l'accès à la base de données Protection de la communication avec le composant Lantronix
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « COSMOS (UTL SYRIUS 2P2L-EXT version 1661z, UTL ORION 4P-8L-EXT version 1661z), Version 4.6.0.96 » développé par ELSYLOG. Son but est de contrôler les accès des personnes à un site, un bâtiment ou un local.

Le système de contrôle d'accès COSMOS se compose :

- du gestionnaire des accès contrôlés (GAC) Cosmos assurant la gestion des UTL[1] et la saisie des différents paramètres nécessaires au fonctionnement sécurisé du système ;
- d'UTL SYRIUS assurant la sécurisation de deux portes distinctes ou d'une porte permettant l'entrée et la sortie ;
- d'UTL ORION assurant la sécurisation de quatre portes distinctes ;
- de badges MIFARE DESFIRE EV1/EV2, norme ISO 14443 ;
- de lecteurs de Proximité MIFARE DESFIRE (Modèle SYL123-S-ARCDES), compatibles avec tous les badges MIFARE : MIFARE CLASSIC, MIFARE PLUS, MIFARE DESFIRE EV1/EV2 ;
- du PC industriel exécutant l'application COMET qui assure l'interconnexion entre l'application COSMOS et les UTL.

Les UTL sont équipés d'une carte SAM AV2/AV3 NXP permettant la gestion et la sécurisation des clés utilisées dans le cadre des communications chiffrées avec le badge, ainsi que celles nécessaires à la communication chiffrée avec le serveur COSMOS.

[1] Unités de Traitement Logique.

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

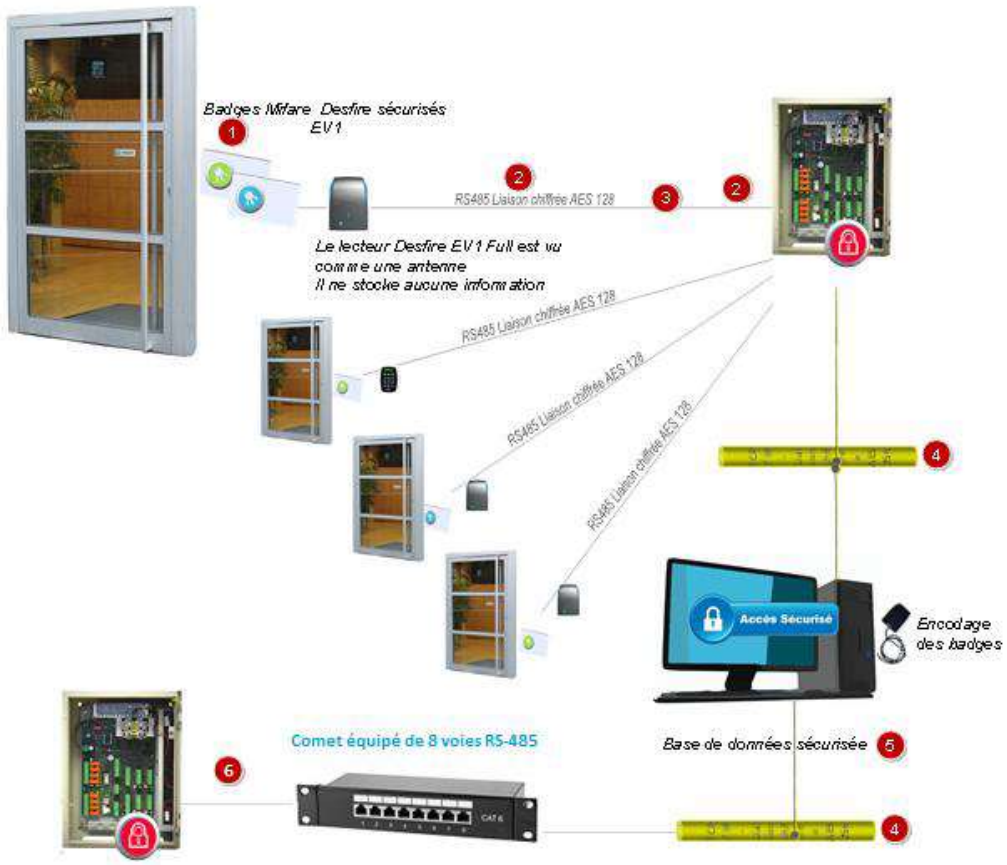

Figure 1 – Architecture du produit.

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*

Produit	
Nom du produit	COSMOS UTL SYRIUS 2P2L-EXT UTL ORION 4P-8L-EXT
Numéro de la version COSMOS évaluée	4.6.0.96
Version du *firmware* des UTL	1661z
Version de COMET	4.1.0.86

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

- le numéro de la version du GAC COSMOS peut être visualisé sur la mire d'authentification de l'application ;
- le numéro de la version de COMET peut être retrouvé dans l'application COSMOS, dans le menu de configuration des TERMINAUX ;
- le numéro de la version du *firmware* des UTL apparaît également dans le menu de configuration des TERMINAUX de l'application COSMOS ;
- le numéro de version de la carte-mère des UTL se retrouve sur les composants en question.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection des communications entre le lecteur et l'UTL ;
- la protection des communications entre l'UTL et le GAC COSMOS ;
- la protection des communications entre l'UTL et COMET;
- la protection des communications entre COMET et le GAC COSMOS ;
- la protection du code PIN ;
- la protection contre l'arrachement de l'UTL ;
- la détection d'ouverture et d'arrachement de la tête de lecture du lecteur de Proximité ;
- la protection du *firmware* de l'UTL ;
- la détection de court-circuit ou de coupure de boucle associée au bouton poussoir de sortie;
- la détection de court-circuit ou coupure de boucle de la surveillance de l'entrée ;
- la protection des données utilisateur pour l'authentification ;
- le cloisonnement entre les différents comptes utilisateurs ;
- les échanges clients/serveur Cosmos ;
- la protection de l'accès à la base de données ;
- la protection de la communication avec le composant Lantronix.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond :

- aux UTL SYRIUS (SYRIUS-2P2L-IP-EXT v1661z) et ORION (ORION-4P8L-EXT v1661z) raccordés au serveur COSMOS via un bus de terrain RS485 ou un réseau IP ;
- aux lecteurs de proximité MIFARE DESFIRE (SYL123-S-ARCDESF - ARC A et SYL123-S-ARCDESF-C - ARC B) raccordées sur des UTL SYRIUS/ORION via une liaison RS485 ;
- à un ensemble de badges MIFARE DESFIRE EV1/EV2, norme ISO 14443 ;
- à un serveur hébergeant les différentes machines virtuelles constituant le système COSMOS : Serveur web, serveur RADIUS, contrôleur de domaine, base de données ;
- à un poste client permettant d'accéder à l'application COSMOS ;
- à un PC industriel exécutant l'application COMET. Cette application assure l'interconnexion entre l'application COSMOS et les UTL.

La carte SAM dans les UTL, les badges DESFIRE, le serveur RADIUS, le contrôleur de domaine, le poste client hébergeant l'application COSMOS et l'interface de communication entre le badge et la tête de lecture ne font pas partie du périmètre d'évaluation.

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 **Erreur ! Source du renvoi introuvable.**.

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'environnement d'évaluation a été fourni par ELSYLOG sous forme de maquette prête à l'emploi. L'évaluateur ne peut donc pas se prononcer sur cet aspect de l'évaluation.

2.2.1.3 Notes et remarques diverses

Néant.

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 ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré 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 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 globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le **Erreur ! Source du renvoi introuvable.**.

2.3 Analyse de la résistance des mécanismes cryptographiques

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

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 « COSMOS (UTL SYRIUS 2P2L-EXT version 1661z /UTL ORION 4P-8L-EXT version 1661z), version 4.6.0.96 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité **Erreur ! Source du renvoi introuvable.** 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 **Erreur ! Source du renvoi introuvable.**, et suivre les recommandations se trouvant dans les guides fournis **Erreur ! Source du renvoi introuvable.**.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité gamme COSMOS (Cosmos / Syrius / Orion), version 1.7, 2 décembre 2021.
[RTE]	Rapport technique d'évaluation : - Titre du Rapport Technique d'Evaluation CSPN CORNAC – COSMOS, version 1.2, 1 décembre 2021.
[GUIDES]	Guide de configuration du produit : - Configuration CSPN Cosmos, version 1.1, 2 décembre 2021 ; - Cosmos – Prérequis, version 1.1, 2 décembre 2021 ; - SqlServer 2016 Installation ; - Cosmos Installation ; - DocManager Installation ; - Cosmos Démarrage Contrôle Accès ; - Configuration Xport Edge ; - Diagnostic de mise en route – Niveau 0 ; - Certificat UTL ; - Activer chiffrement UTL ; - Radiux 802.1x ; - Configuration IIS ; - DAT_MaquetteANSSI.

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 3.0, 12 avril 2021. 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.