PREMIÈRE 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-2023/16

Logiciel multi-tenant Rainbow EDGE en tant que service (SaaS), en hébergement Cloud privé sur socle IaaS

Version 114, Client web 2.114.x

Paris, le 10 Novembre 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

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-2023/16**
Nom du produit **Logiciel multi-tenant Rainbow EDGE en tant que service (SaaS), en hébergement Cloud privé sur socle IaaS**
Référence/version du produit **Version 114, Client web 2.114.x**
Catégorie de produit **Communication sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **ALE International** 260 rue Léon Foucault 67400 Illkirch-Graffenstaden, France
Développeur **ALE International** 260 rue Léon Foucault 67400 Illkirch-Graffenstaden, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Authentification de l'utilisateur Contrôle d'accès de l'utilisateur Rattachement de l'utilisateur à une entité bénéficiaire Protection de la session et des messages instantanés Protection des flux point-à-point Protection des flux multipoints Chiffrement des données stockées Chiffrement des mots de passe stockés
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 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 7
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Travaux d'évaluation 9
2.2.1 Installation du produit 9
2.2.2 Analyse de la documentation 9
2.2.3 Revue du code source (facultative) 9
2.2.4 Analyse de la conformité des fonctions de sécurité 9
2.2.5 Analyse de la résistance des mécanismes des fonctions de sécurité 10
2.2.6 Analyse des vulnérabilités (conception, construction, etc.) 10
2.2.7 Analyse de la facilité d'emploi 10
2.3 Analyse de la résistance des mécanismes cryptographiques 10
2.4 Analyse du générateur d'aléa 10
3 La certification 11
3.1 Conclusion 11
3.2 Recommandations et restrictions d'usage 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Logiciel multi-tenant Rainbow EDGE en tant que service (SaaS), en hébergement Cloud privé sur socle IaaS, Version 114, Client web 2.114.x » développé par ALE International.

Le service de collaboration Rainbow dans sa version Rainbow EDGE est hébergé sur un *Cloud* privé ou dans un *data center*, installé et maintenu par Alcatel-Lucent Enterprise. Il fournit à ses clients un service de collaboration avancé et sécurisé leur permettant de communiquer en voix, vidéo ou messages. Ces communications peuvent être point à point ou multipoints et les données échangées peuvent avoir différents formats : images, vidéo, texte, partage d'écran.

Les abonnés au service Rainbow utilisent une application client Rainbow déployée sur leur ordinateur et/ou sur leur téléphone mobile, et qui établit des flux d'échange avec le serveur Rainbow.

Le présent certificat porte sur la confidentialité des informations échangées lors de communications établies avec Rainbow, dans un déploiement en *Cloud* privé sur socle IaaS et accédé par client web.

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

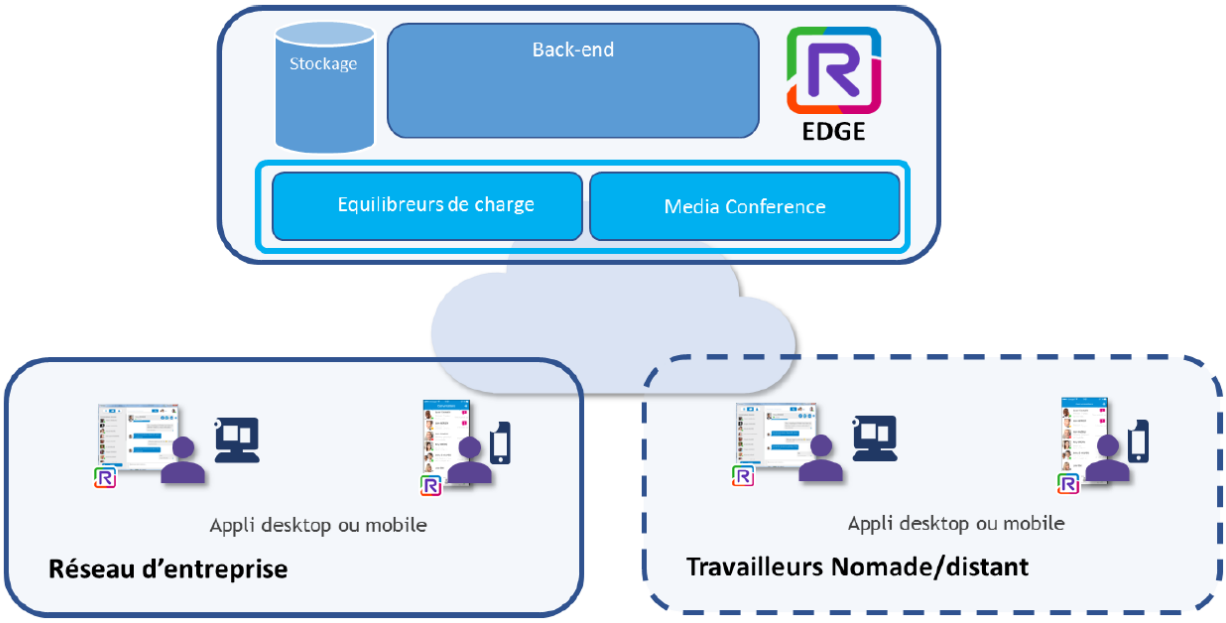

Figure 1 - Architecture Produit.

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	Logiciel multi-tenant Rainbow EDGE en tant que service (SaaS), en hébergement Cloud privé sur socle IaaS
Numéro de la version évaluée	Version 114, Client web 2.114.x

La version certifiée du produit peut être identifiée directement via l'URL d'accès au client web :

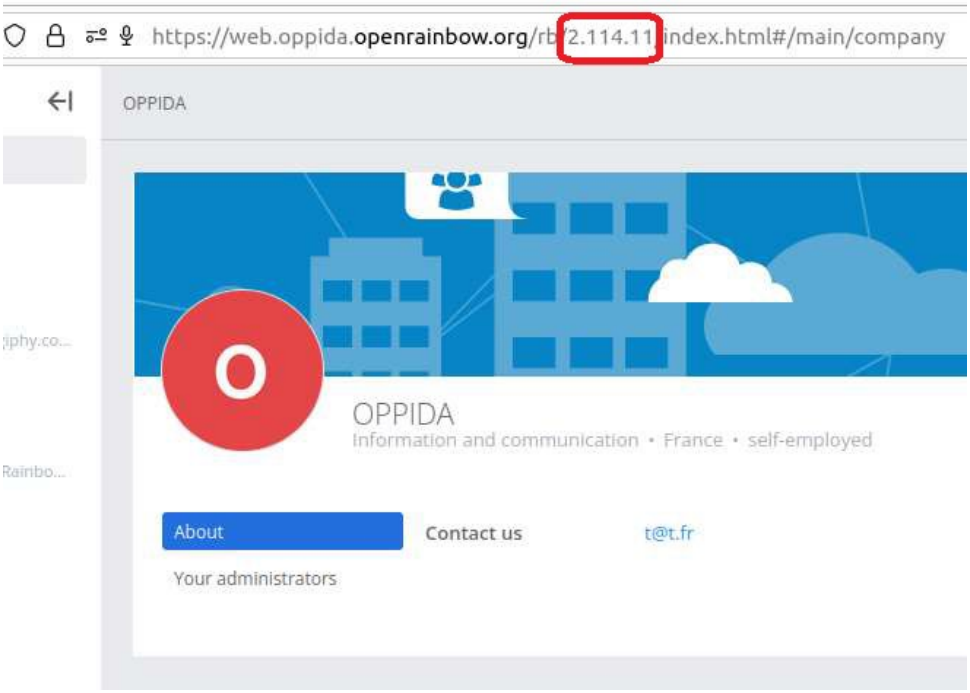

Figure 2 – Identification de la version certifiée du produit.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification de l'utilisateur ;
- le contrôle d'accès de l'utilisateur ;
- le rattachement de l'utilisateur à une entité bénéficiaire ;
- la protection de la session et des messages instantanés ;
- la protection des flux point-à-point ;
- la protection des flux multipoints ;
- le chiffrement des données stockées ;
- le chiffrement des mots de passe stockés.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à un hébergement de la solution en *cloud* privé sur socle IaaS et accédé par le client web. Seule la communication avec les clients fait partie du périmètre d'évaluation.

La plateforme de test est constituée de navigateurs compatibles (tels que définis le site du développeur *support.openrainbow.com*) et d'un accès SSH dédié (fourni exceptionnellement au CESTI afin qu'il puisse avoir accès au système d'exploitation sous-jacent de la cible 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-06].

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 de la cible d'évaluation a été faite par le développeur, et ce dernier a fourni à l'évaluateur, comme points d'entrée pour l'évaluation : le lien https://web.oppida.openrainbow.org ainsi qu'un accès SSH à distance.

L'évaluateur n'ayant pas pu réaliser lui-même une installation locale du produit comme demandé par la [NOTE-06], il a donc audité et testé le processus d'installation et configuration automatisée de la cible d'évaluation par le *playbook* Ansible.

L'évaluateur confirme que l'installation respecte les bonnes pratiques de configuration.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

Le développeur n'a fourni aucun guide de configuration ou d'utilisation dans le cadre de cette évaluation.

Il existe cependant une aide en ligne décrite dans [GUIDES].

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité 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 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 et 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 évalué est orienté grand public et son utilisation reste très intuitive et ne nécessite pas de documentation ou de formation spécifique.

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 [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 « Logiciel multi-tenant Rainbow EDGE en tant que service (SaaS), en hébergement Cloud privé sur socle IaaS, Version 114, Client web 2.114.x » 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 : - RAINBOW EDGE par ALCATEL-LUCENT ENTERPRISE - ANSSI Cible - CSPN Ed 1.3.1, référence OD-405320, version 1.3.1, 16 janvier 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Rainbow EDGE – RAINBOW3, référence OPPIDA/CESTI/2022/RAINBOW3/RTE, version 1.3, 26 octobre 2023.
[GUIDES]	Aide en ligne disponible à l'adresse suivante : https://support.openrainbow.com/hc/fr

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 2022. 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, 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-06]	Note d'application - Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, référence ANSSI-CSPN-NOTE-06, version 1.0, 2 mars 2021.