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-2020/41

Odisia Broker utilisé avec Odisia Desktop

Versions 1.0.15 et 1.3.7

Paris, le 1er décembre 2020

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

Guillaume POUPARD

[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-2020/41**
Nom du produit **Odisia Broker utilisé avec Odisia Desktop**
Référence/version du produit **Versions 1.0.15 et 1.3.7**
Catégorie de produit **Autre : API de signature numérique**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **LEX Persona** Technopôle de l'Aube en Champagne 2, rue Gustave Eiffel, 10430 Rosières-près-Troyes, France
Développeur **LEX Persona** Technopôle de l'Aube en Champagne 2, rue Gustave Eiffel, 10430 Rosières-près-Troyes, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Protection des communications entre l'application métier et Odisia Broker Protection des communications entre Odisia Broker et le poste du signataire Gestion de la transaction avec un identifiant unique Identification de manière unique les applications métiers appelant Odisia Broker Création d'une signature numérique des documents Vérification de la signature numérique des documents
Fonctions de sécurité non évaluées Néant
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 « Odisia Broker, version 1.0.15 » utilisé avec le produit Odisia Desktop, version 1.3.7, développés par LEX Persona.

Odisia Enterprise, une solution développée par LEX Persona, propose une architecture de signature électronique. *Odisia Broker* et *Odisia Desktop* s'inscrivent dans cette architecture en remplissant des rôles distincts :

- *Odisia Broker* est un *webservice* REST permettant l'intermédiation entre une application métier qui nécessite une signature électronique et un signataire utilisateur de l'application métier ;
- *Odisia Desktop* est une application cliente qui permet de réaliser la signature électronique depuis le poste de l'utilisateur final.

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

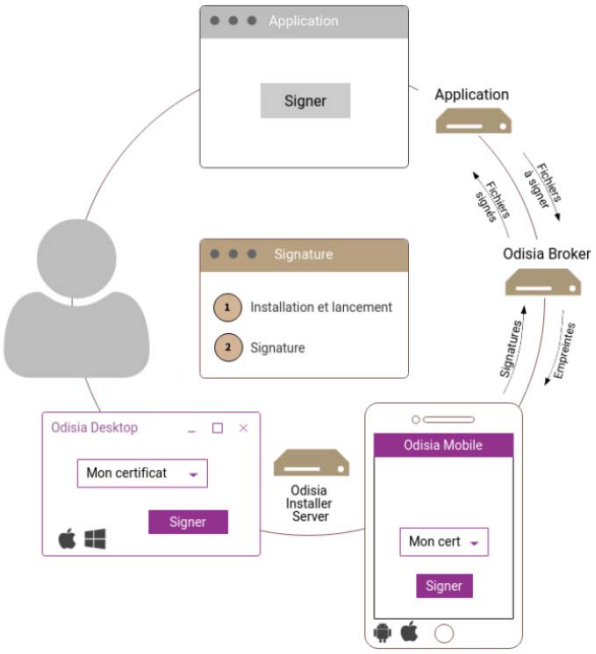

Figure 1 - Architecture Produit.

Dans le cadre de cette évaluation, seuls *Odisia Broker et Odisia Desktop* pour Windows font partie du périmètre d'évaluation.

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 : API de signature numérique**

1.2.2 *Identification du produit*

Produit	
Nom du produit	*Odisia Broker*
Numéro de la version évaluée	1.0.15
Nom du produit	*Odisia Desktop*
Numéro de la version évaluée	1.3.7

La version certifiée du produit peut être identifiée de la manière suivante :
- au démarrage du serveur, la version d'*Odisia Broker* apparait dans les *logs* ;
- en cliquant dans la partie inférieure de la fenêtre d'*Odisia Desktop* une nouvelle fenêtre apparait, mentionnant la version du produit.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- la protection des communications entre l'application métier et *Odisia Broker* ;
- la protection des communications entre *Odisia Broker* et le poste du signataire ;
- la gestion de la transaction avec un identifiant unique ;
- l'identification de manière unique des applications métiers appelant *Odisia Broker* ;
- la création d'une signature numérique des documents ;
- la vérification de la signature numérique des documents.

1.2.4 *Configuration évaluée*

La plateforme de test est constituée des éléments suivants :
- un PC exécutant *Windows* 10 sur lequel est installé :
  - *Odisia Desktop* pour Windows en version 1.3.7 ;
- un PC exécutant *Windows* 10 sur lequel est installé :
  - *Odisia Broker* en version 1.0.15,

- *Tomcat* en version 9.0.35 et
- *Java* en version 8u251.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe B.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 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].

2.3.1 *Installation du produit*

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4, avec la version Windows d'*Odisia Desktop*.

Les composants suivants doivent être présents sur le serveur :

- *Tomcat* en version 9.0.35 ;
- *Java* en version 8u251.

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

La documentation d'installation ([GUIDES]) est correctement rédigée et permet une installation rapide de la TOE.

2.3.1.3 Durée de l'installation

L'installation de la partie serveur prend une trentaine de minutes.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

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

2.3.3 *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.

2.3.4 *Analyse de la conformité des fonctions de sécurité*

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

2.3.5 *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.

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

2.3.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2 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.

2.3.7 *Accès aux développeurs*

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

2.3.8 *Analyse de la facilité d'emploi*

2.3.8.1 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.

2.3.8.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.8.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas, mais s'appuie sur Java pour la génération d'identifiants uniques. Celui-ci a fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

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 « Odisia Broker utilisé avec Odisia Desktop, Versions 1.0.15 et 1.3.7 » 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.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité CSPN Odisia Broker & Desktop Version : 1.1 ; Date : 4 septembre 2020.
[RTE]	Rapport Technique d'Évaluation CSPN LEX PERSONA ODISIA - Odisia Broker & Odisia Desktop Référence : OPPIDA/CESTI/LEX PERSONA ODISIA/RTE/1.2 ; Version : 1.2 ; Date : 9 novembre 2020.
[GUIDES]	*Odisia Broker installation* Date : 11 avril 2019. *Odisia Broker API* Date : 11 avril 2019.

ANNEXE B. Références 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-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.