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-CC-2023/07

API GATEWAY
version 7.7.20210530, Patch24803, Patch24985, Patch25644, Patch25454

Paris, le 16 Février 2023

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 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-CC-2023/07

Nom du produit

API GATEWAY

Référence/version du produit

7.7.20210530, Patch24803, Patch24985, Patch25644, Patch25454

Version : 7.7.20210530, Build : 2021-06-02, rev. : 4c84fa4
APIGateway_7.7.20210530_Patch24803_6b68457e_allOS_BN20210708
APIGateway_7.7.20210530_Patch24985_c185313c_allOS_BN20210723
APIGateway_7.7.0_Patch25454_95d32974_linux-x86-64_BN20211028
APIGateway_7.7.0_Patch25644_c6c4d330_allOS_BN20211019

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté
AVA_VAN.4, ALC_FLR.3

Développeur

AXWAY SOFTWARE
8-34 Percy Place
Dublin 4, Ireland

Commanditaire

AXWAY SOFTWARE
Tour W
102 Terrasse Boieldieu
92085 Paris La Défense Cédex, France

Centre d'évaluation

OPPIDA
4-6 avenue du vieil étang, Bâtiment B,
78180 Montigny le Bretonneux, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3.

SOG-IS

Ce certificat est reconnu au niveau EAL4 augmenté de FLR.3.

PREFACE

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 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 « API GATEWAY, version 7.7.20210530, Patch24803, Patch24985, Patch25644, Patch25454 » développé par AXWAY SOFTWARE.

Ce produit est une plateforme de gestion d'API qui permet de gérer de manière centralisée le contrôle d'accès aux services web et aux ressources connexes d'une entreprise. Plus précisément, il s'agît d'une plateforme complète pour la gestion centralisée, et la sécurisation des API.

Les principaux composants du produit sont les trois éléments suivants :

- API Gateway (passerelle) : l'utilisateur des services se connecte au travers d'API Gateway de manière transparente pour accéder aux données et applications ;
- API Gateway Manager (*monitoring*) : l'opérateur réalise ses opérations de surveillance via la console d'administration web API Gateway Manager ;
- Policy Studio (définition de politiques) : le développeur de politiques va pouvoir virtualiser des services et développer des politiques de sécurité grâce à Policy Studio. C'est un outil qui permet de créer, modifier ou supprimer des politiques de manière graphique.

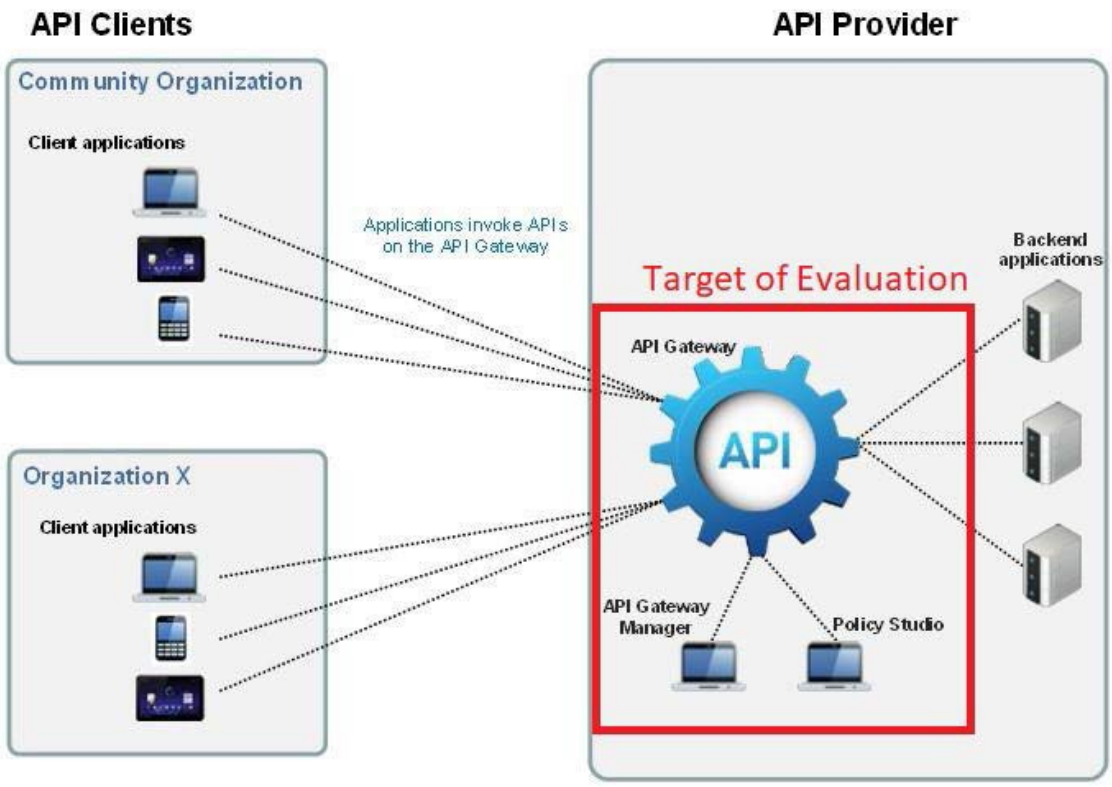

Figure 1: Architecture d'API Gateway

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits dans la section 6 de la cible de sécurité [ST].

1.2.3 *Architecture*

Le produit est déployé sous la forme d'un composant logiciel composé de trois éléments principaux :

- *Policy Studio* : il est utilisé pour élaborer des politiques et administrer le produit. Plus précisément, il s'agit d'une application *GUI* qui fournit à l'utilisateur l'interface administrative principale de la passerelle ;
- *API Gateway* : une ou plusieurs instances du logiciel API Gateway qui appliquent des politiques pour contrôler les services *web* ;
- *API Gateway Manager* : une interface *web* pour surveiller le trafic de la passerelle en temps réel et configurer la politique globale des accès, les événements d'audit et d'autres événements de ce type.

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans le guide d'installation [GUIDES].

La version certifiée du produit (Version : 7.7.20210530, Build : 2021-06-02, rev. : 4c84fa4) peut être identifiée sur différentes interfaces :

- en utilisant l'interface *web* du produit ;
- en utilisant *Policy Studio*.

Les patchs suivants sont également nécessaires :

- APIGateway_7.7.20210530_Patch24803_6b68457e_allOS_BN20210708 ;
- APIGateway_7.7.20210530_Patch24985_c185313c_allOS_BN20210723 ;
- APIGateway_7.7.0_Patch25454_95d32974_linux-x86-64_BN20211028 ;
- APIGateway_7.7.0_Patch25644_c6c4d330_allOS_BN20211019.

La version certifiée du produit et les patchs appliqués peuvent être identifiés en utilisant *Managedomain* (`./managedomain -- version`).

1.2.5 *Cycle de vie*

Le développement et la maintenance du produit sont faits sur les sites suivants (voir [SITES]) :

Dublin AXWAY IRELAND LIMITED 1st Floor, 8-34 Percy Place Dublin 4 Ireland	**Phoenix** PX1 – 2500 W. Union Hills Drive Phoenix AZ 85027 United States of America
Saint Denis Interxion 11-13 avenue des Arts et Métiers 93200 Saint Denis France	

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit tel que présenté plus haut aux paragraphes 1.2.2 et 1.2.4.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 20 décembre 2022, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

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 [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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Cependant, 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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

3.3 Reconnaissance du certificat

3.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - API Gateway v7.7 Security Target, référence API_CC_ST_01, version 2.7, novembre 2021.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report API GW*, référence OPPIDA/CESTI/API GW/RTE, version 1.1, 20 décembre 2022.
[ANA_CRY]	*Cryptographic Analysis report API GW*, référence OPPIDA/CESTI/API GW/CRYPTO, version 1.1, 24 octobre 2022.
[GUIDES]	Guide d'installation du produit : - Guide d'installation, référence AGD_PRE, version 0.3, 8 novembre 2021. Guide d'administration et d'utilisation du produit : - *API Gateway User Guidance*, référence AGD_OPE, version 0.6, 28 septembre 2021.

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.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[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.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[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.