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-2023/13

Strong customer authentication pour Apple Pay sur Apple Watch série 4 exécutant watchOS 7.4.1 (Version 18T201)

Paris, le 1er Mars 2023

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

Emmanuel NAEGELEN

[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-2023/13

Nom du produit

Strong customer authentication pour Apple Pay sur Apple Watch série 4 exécutant watchOS 7.4.1

Référence/version du produit

Version 18T201

Conformité à un profil de protection

Sans objet

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL2 augmenté
ADV_FSP.3, ALC_FLR.3

Développeur

Apple Inc.
7 place d'Iena
75016 Paris, France

Commanditaire

Apple Inc.
7 place d'Iena
75016 Paris, France

Centres d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

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 ALC_FLR.3.

SOG-IS

Ce certificat est reconnu au niveau EAL2 augmenté de ADV_FSP.3 et ALC_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 « Strong customer authentication pour Apple Pay sur Apple Watch série 4 exécutant watchOS 7.4.1, Version 18T201 » développé par Apple Inc..

Apple Pay est une solution de paiement mobile développée par la société Apple Inc. Après avoir enregistré une carte bancaire dans son équipement Apple, l'utilisateur peut faire des paiements au travers de celui-ci. Pour que le paiement aboutisse, l'utilisateur doit s'authentifier sur l'équipement en utilisant un mot de passe, une empreinte digitale ou en utilisant la reconnaissance faciale. Ces équipements peuvent être un iPhone, un iPad, une Apple Watch ou un équipement de type Mac.

Dans le cadre de l'évaluation le seul matériel Apple pris en compte est l'Apple Watch, exécutant la version 7.4.1 (18T201) du système d'exploitation watchOS avec comme moyen d'authentification utilisateur le mot de passe. L'appairage avec un iPhone permet également un déverrouillage rapide sans saisie du mot de passe.

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 :

- la gestion de l'authentification de l'utilisateur (enrôlement, authentification, etc.) ;
- le déverrouillage utilisant un iPhone appairé au produit ;
- l'utilisation sécurisée d'Apple Pay et Apple Pay Cash (provisionnement des cartes, gestion des transactions dont le non rejeu) ;
- la protection des données stockées ;
- la mise à jour sécurisée du logiciel.

1.2.3 *Architecture*

Le produit est constitué :

- du *System on Chip* (*SoC*) S4 incluant
  - l'*Application Processor* (AP) : processeur applicatif exécutant le système d'exploitation et les applications utilisateurs,
  - le *Secure Enclave Processor* (SEP) : processeur sécurisé exécutant dans un environnement dédié un système d'exploitation sécurisé (SEPOS) et des applications sécurisées ;
- l'écran permettant, entre autres, à l'utilisateur de taper son mot de passe pour s'authentifier.

Le produit s'appuie sur un *Secure Element* (SE), hors périmètre de l'évaluation, pour réaliser les transactions bancaires et assurer la protection cryptographique des éléments sensibles.

Le produit permet enfin l'appairage avec un iPhone, également hors-périmètre de l'application, permettant le déverrouillage sans saisie du mot de passe.

La Figure 1 décrit l'architecture du produit.

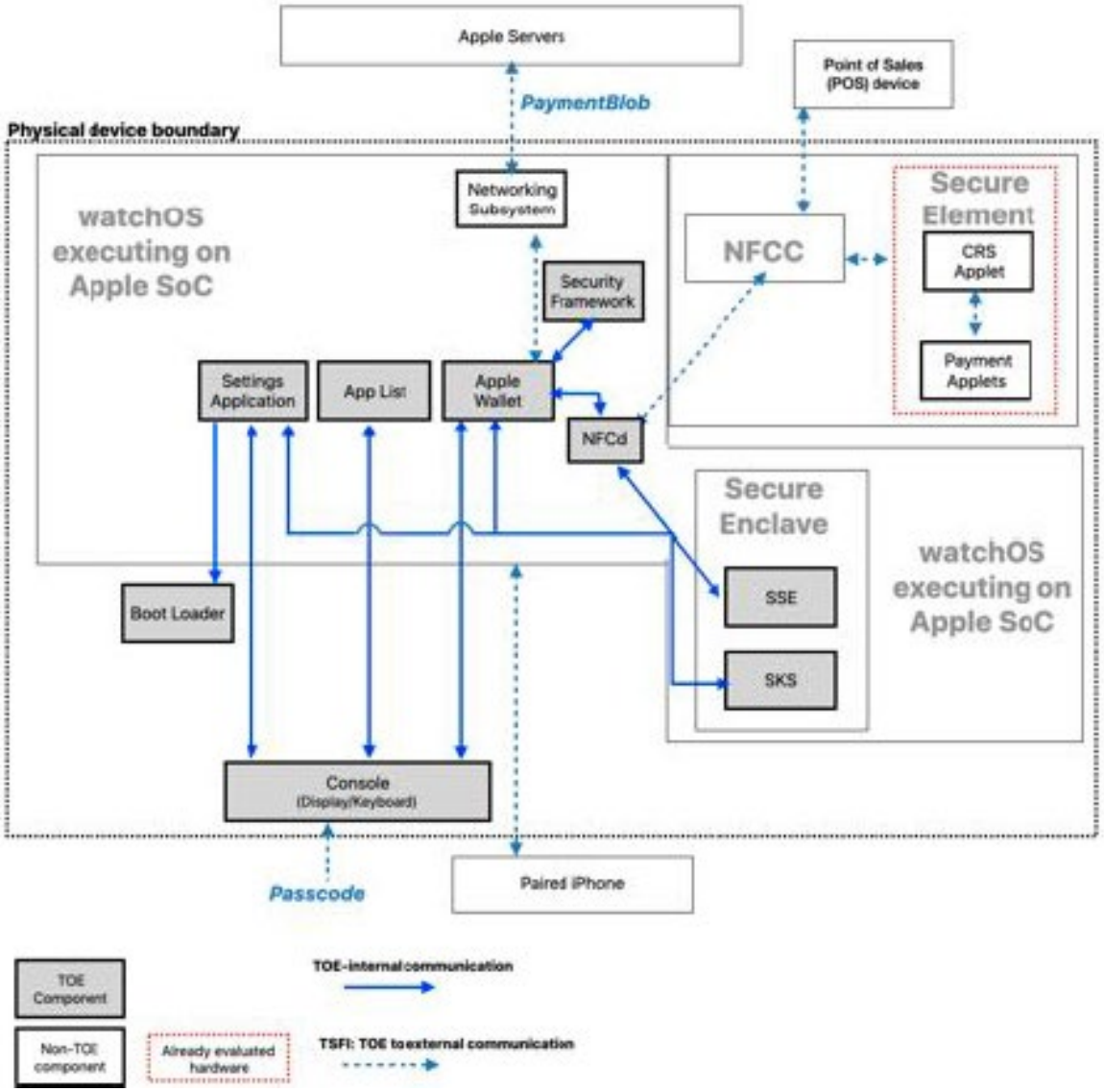

Figure 1 : Architecture du produit

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] à la section 2.1 « *Target of Evaluation Definition* ».

Eléments de configuration		Origine
Modèle	Apple Watch série 4	Apple Inc.
Version du système d'exploitation	watchOS 7.4.1 (18T201)	
SoC	S4	

Le numéro de modèle peut se vérifier à l'intérieur des rainures où le bracelet s'attache sur le produit (nécessite de détacher le bracelet). Dans les paramètres du produit, la section générale, puis « à propos » expose la version du système d'exploitation sous la mention « Version ».

Remarque :

La version de watchOS, ici 18T201, fige non seulement la version du système d'exploitation mais également les applications système qui y sont contenues, telle que l'application Apple Pay, ainsi que la version de SEPOS.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :

- design : la conception du matériel et du logiciel ;
- fabrication : la fabrication du matériel et l'implémentation du logiciel ;
- intégration : l'intégration du logiciel et du matériel ;
- mise en circulation : le produit est remis au client, prêt à être initialisé avec ses données utilisateurs.

Le produit a été développé sur le site suivant :

Apple

Apple Park way,
Cupertino, CA95014
Etats Unis

Pour l'évaluation, l'évaluateur a considéré l'utilisateur final comme seul utilisateur du produit.

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit décrit au paragraphe « 1.2.4 Identification du produit ».

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [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 3 février 2023, 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 [RTE].

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.

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].

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.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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.

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 :

[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.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Strong Customer Authentication for Apple Pay on Apple Watch with S4 running watchOS 7.4.1 - Security Target, version 1.5, 10 mai 2022.
[RTE]	Rapport technique d'évaluation : - *WEXFORD2 Project: Evaluation Technical Report*, référence WEXFORD2_ETR, version 1.1, 3 février 2023.
[CONF]	Liste de configuration du produit : - *Strong Customer Authentication for Apple Pay on Apple Watch with S4 running watchOS 7.4.1 - Configuration Item List*, version 1.8, 10 mai 2022.
[GUIDES]	*Strong Customer Authentication for Apple Pay on Apple Watch with S4 running watchOS 7.4.1 – Guidance*, version 1.3, 10 mai 2022.

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 5.0.
[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.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.