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-2023/17

Strong Customer Authentication pour Apple Pay sur Apple Watch avec S7 exécutant watchOS 8.5.1 (Version 8.5.1 (build 19T252))

Paris, le 27 Mars 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-2023/17**
Nom du produit **Strong Customer Authentication pour Apple Pay sur Apple Watch avec S7 exécutant watchOS 8.5.1**
Référence/version du produit **Version 8.5.1 (build 19T252)**
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'Iéna 75016 Paris, France
Commanditaire **APPLE INC.** 7 place d'Iéna 75016 Paris, France
Centre d'évaluation **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.3. **SOG-IS**

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 avec S7 exécutant watchOS 8.5.1*, *Version 8.5.1 (build 19T252)* » 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 cette évaluation, le matériel *Apple* pris en compte est l'*Apple Watch* contenant la puce S7 exécutant la version 8.5.1 (*build 19T252*) du système d'exploitation *watchOS* avec comme moyen d'authentification utilisateur le 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.) ;
- 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 (chiffrement des données, effacement sécurisé) ;
- la protection des données en transit (entre *Secure Enclave et Secure Element*) ;
- la mise à jour sécurisée du logiciel.

1.2.3 *Architecture*

La TOE correspond à l'ensemble des éléments suivants, qui interviennent dans la mise en œuvre des services objets de la présente évaluation :
- le *System on Chip* (SoC) S7 incluant :
  - l'*Application Processor* (AP) : processeur applicatif exécutant le système d'exploitation et les applications utilisateurs ;
  - le *Secure Enclave* (SEP) : processeur sécurisé exécutant dans un environnement dédié un système d'exploitation sécurisé (*sepOS*) et des applications sécurisées ;
- la console, c'est-à-dire le matériel et les drivers permettant de gérer l'écran et le clavier, en particulier pour permettre à l'utilisateur de taper son mot de passe afin de s'authentifier ;

Le produit s'appuie également sur :

- un *Secure Element* (SE) pour réaliser les transactions bancaires et assurer la protection cryptographique des éléments sensibles.

La Figure 1 décrit l'architecture du produit :

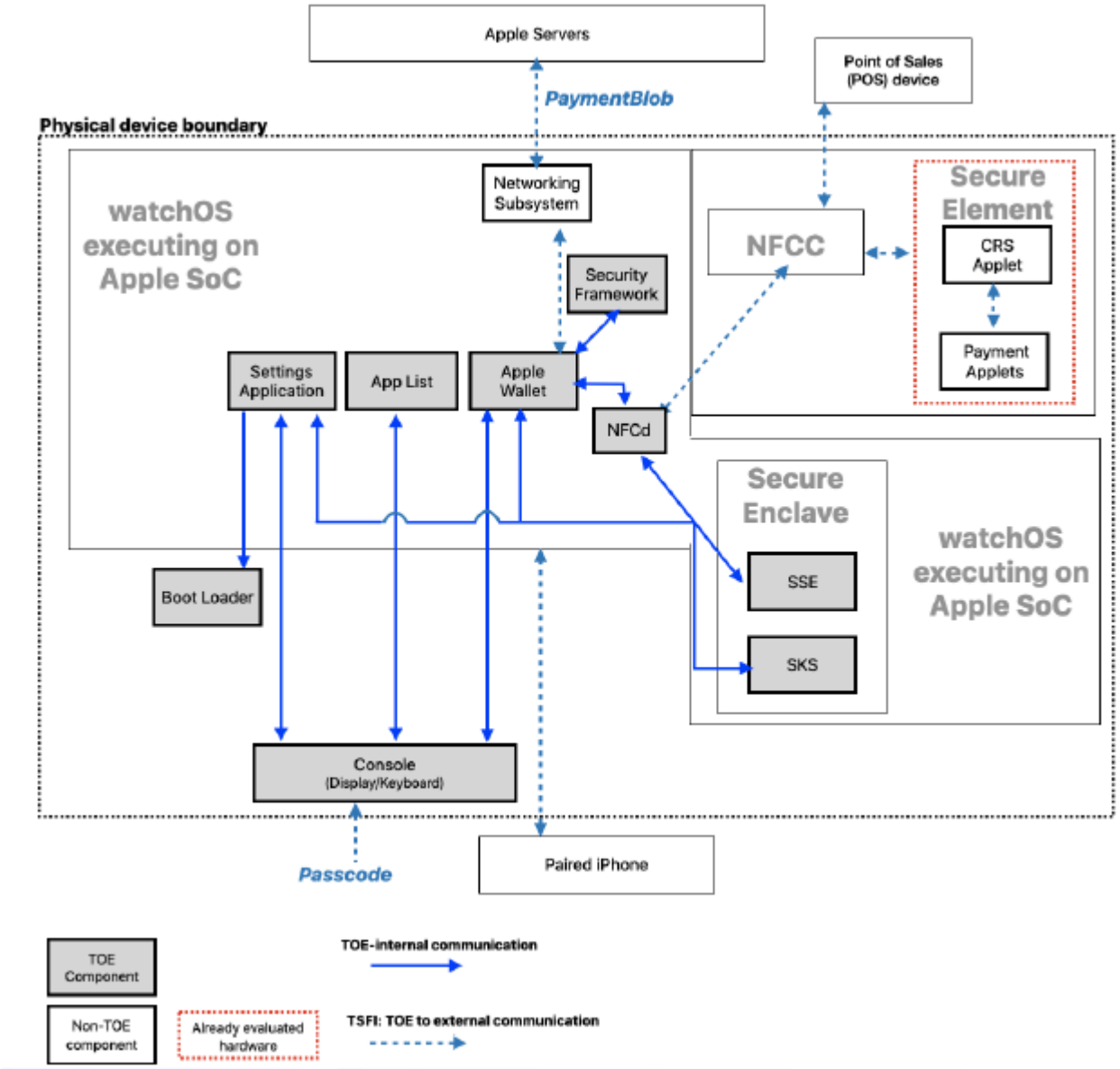

Figure 1 : Architecture du produit

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 Reference* ».

Eléments de configuration		Origine
Modèle des appareils	*Apple Watch Series 7*	APPLE INC.
SoC	S7	
Secure Enclave (SEP)	*sepOS* de *watchOS* 8.5.1	
Version du système d'exploitation	*watchOS* 8.5.1 (*build* 19T252)	

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 19T252, 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 INC.

Apple Park Way,
Cupertino, CA 95014
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 les produits tels que décrit au paragraphe 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 13 janvier 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].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

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.

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, pour certains équipements matériels avec boîtiers sécurisés, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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.

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 :

[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 S7 running watchOS 8.5.1 Security Target*, version 1.4, 11 novembre 2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – PSD2 OS 2021 – WEXFORD3, référence WEXFORD3_ETR*, version 2.0, 13 janvier 2023.
[CONF]	Liste de configuration du produit : - *Strong Customer Authentication for Apple Pay on Apple Watch with S7 running watchOS 8.5.1 Configuration Item List*, version 1.2, 11 novembre 2022.
[GUIDES]	Guide d'utilisation du produit : - *Strong Customer Authentication for Apple Pay on Apple Watch with S7 running watchOS 8.5.1 Guidance*, version 1.4, 11 novembre 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.