PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Certification report ANSSI-CC-2023/60

Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOS 9.4 (watchOS 9.4 (build 20T253))

Paris, the

COURTESY TRANSLATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01.71.75.82.82

WARNING

This report is intended to provide people who request evaluations with a document allowing them to confirm the level of security offered by the product under the usage or operating conditions defined in this report for the evaluated version. It is also intended to provide a potential acquirer of the product with the circumstances under which they may operate or use the product in accordance with the operating conditions for which the product has been evaluated and certified; this is why the certification report must be read in conjunction with the evaluated usage and administration guides and with the product's security target, which describes the pre-supposed threats, environmental assumptions and presumed usage conditions so that the user can judge whether the product is suitable for their needs in terms of security objectives.

The certification does not in itself constitute a product recommendation by the Agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is completely free of vulnerabilities that can be exploited.

All correspondence relative to this report should be sent to:

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

Certification report reference	**ANSSI-CC-2023/60**
Product name	**Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOS 9.4**
Product reference/version	**watchOS 9.4 (build 20T253)**
Compliance with a protection profile	N/A
Evaluation criterion and version	**Common Criteria version 3.1 revision 5**
Evaluation level	**EAL2 augmented** ADV_FSP.3
Developer	**APPLE INC.** 7 place d'Iéna 75016 Paris, France
Sponsor	**APPLE INC.** 7 place d'Iéna 75016 Paris, France
Evaluation facility	**THALES/CNES** 290 allée du Lac 31670 Labège, France
Applicable recognition agreements	**CCRA** **SOG-IS** This certificate is recognized at level EAL2.

FOREWORD

The certification of security offered by information technology products and systems is governed by amended Decree 2002 535 dated April 18, 2002. This decree states that:

- the Agence nationale de la sécurité des systèmes d'information drafts certification reports. These reports specify the characteristics of the proposed security objectives. They may contain any warnings that their authors consider are worth mentioning for reasons of security. The people who order the reports may choose whether or not to communicate them to third parties or make them public (Art. 7);
- the certificates awarded by the Director General of the Agence nationale de la sécurité des systèmes d'information certify that the individual product or system submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out according to the current rules and standards, with the required level of competence and impartiality (Art. 8).

The certification procedures are available on the website www.cyber.gouv.fr.

TABLE OF CONTENTS

1 Product

1.1 Product Presentation

The evaluated product is "Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOS 9.4, watchOS 9.4 (build 20T253)", developed by APPLE INC..

Apple Pay is a mobile payment solution developed by the company APPLE INC. After users register a bank card in their *Apple* device, they can use it to make payments. For the payment to be successful, users must authenticate themselves on the device using a passcode, a fingerprint or facial recognition.

For this evaluation, the *Apple* device used is the *Apple Watch* containing the S8 chip running version 9.4 (*Build* 20T253) of the *watchOS* operating system, using a passcode as user authentication means.

1.2 Product Description

1.2.1 *Introduction*

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operating environment.

1.2.2 *Security Services*

The main security services provided by the product are:
- user authentication management (passcode);
- security functions to ensure *Apple Pay* transactions;
- protection of stored data (bank information, transaction history) in particular using cryptographic features which allow data encryption and secure erasure;
- protecting data in transit (between the *Secure Enclave and the Secure Element*);
- secure software update.

1.2.3 *Architecture*

The target of evaluation (TOE) consists of the following *Apple Watch S8* hardware elements:

- *Apple SoC (System on Chip) S8* including:
  - Running the watchOS 9.4 operating system.
  - The *Secure Enclave* (SEP) running a secure operating system and secure applications such as SSE (*Secure Enclave-Secure Element*) and SKS (*Secure Key Store*) in a dedicated physical environment.
  - The NFCd allowing communication between the *Apple Wallet* and the *Secure Element* (not belonging to the TOE).
- The *Apple Watch S8* touch screen allowing passcode authentication.

Other elements which are not part of the TOE are necessary for the operation of a product like an *iPhone* (supporting *Apple Pay* with the *Apple Watch* application) paired with the watch, the NFC controller (allowing transactions between the *Apple Watch* and an external bank terminal) or even the Secure Element.

Figure 1 of the security target describes the product architecture:

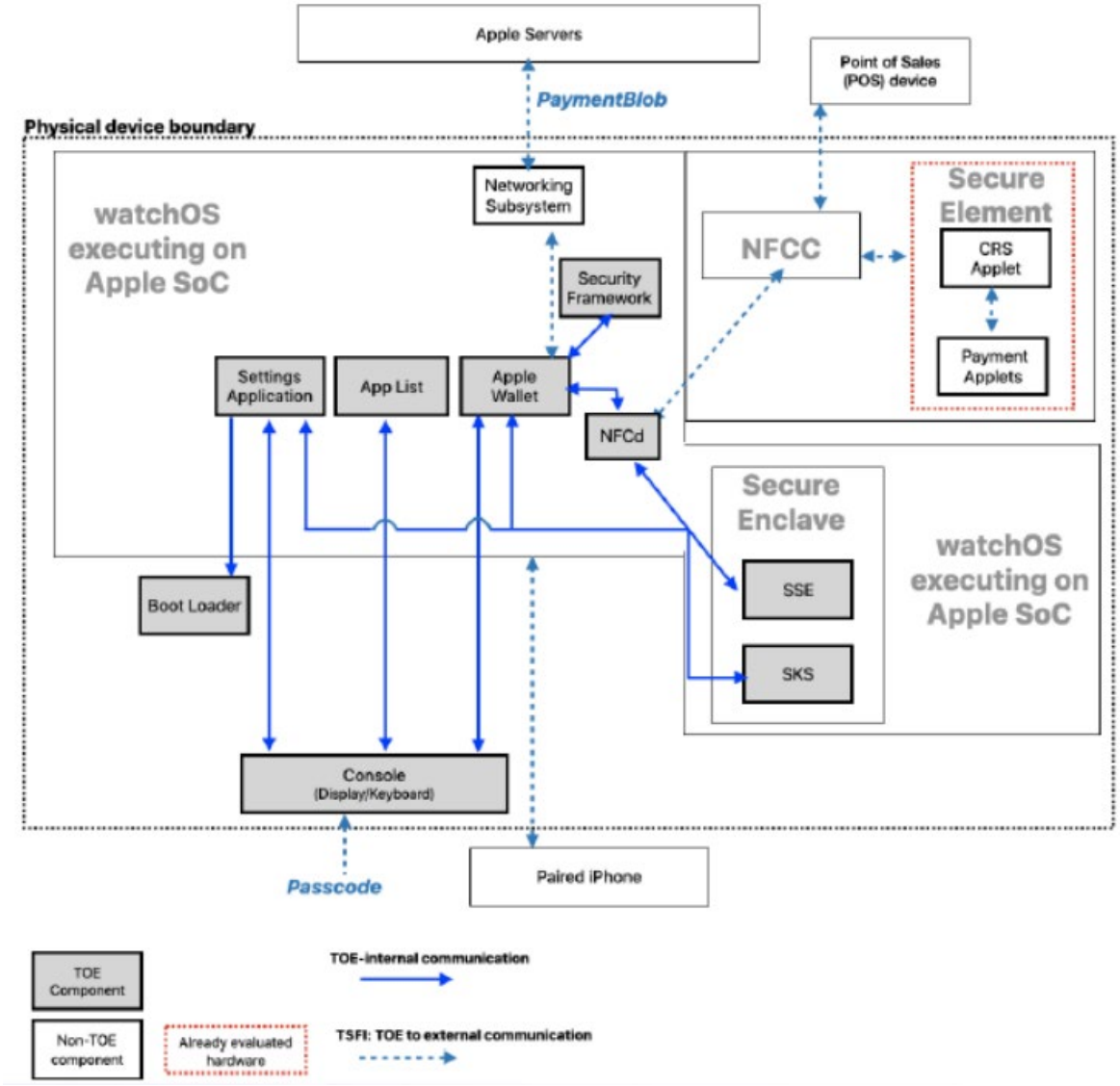

Figure 1: Product Architecture

1.2.4 Product Identification

The component elements of the product are identified in the configuration list [CONF].

The certified version of the product can be identified by the elements in the table below, which are outlined in the security target [ST] in section 2.1 “Target of Evaluation Reference.”

Configuration Elements		Origin
Device model	*Apple Watch* S8	APPLE INC.
SoC *(Application Processor)*	S8	
Operating System Version	watchOS 9.4 (*build* 20T253)	
Secure Enclave (SEP)	*sepOS part of* watchOS 9.4	

The *Apple Watch* user can at any time see the operating system version under "Version" label following the next steps: go to the "*Settings*" application, then to "*General*" and "*About*".

1.2.5 *Life Cycle*

The life cycle of the product is as follows:

- *Design*: hardware, firmware and software;
- *Fabrication:* production of hardware and software implementation;
- *Integration*: integration on Apple Watch: assembly, *trust provisioning*, firmware integration, installation of software and applets;
- *Device Issuance*: delivery of the Apple Watch to the user;
- *Initialization*: product initialization with user data;
- *Enrollment/Provisioning*: the user configures an authentication method (passcode). Later, a bank card is added through Apple Pay.
- *Usage:* use of the device and transaction made with *Apple Pay*, using passcode authentication.
- *Termination:* physical destruction of the device, *watchOS* re-initialisation, erasing data related to *Apple Pay*.

The life cycle is described in chapter 2.7 of the [ST] and only the initial three phases are fully carried out under the control of APPLE INC.

For the evaluation, the evaluator considered the end user to be the sole user of the product.

1.2.6 *Evaluated Configuration*

The certificate is for the product as described in chapter 1.2 of this report.

2 Evaluation

2.1 Evaluation Standard

The evaluation was carried out in accordance with the Common Criteria [CC] and the evaluation methodology defined in the manual [CEM].

2.2 Evaluation Work

The evaluation technical report [ETR], which was delivered to the ANSSI on November 27, 2023, details the work performed by the evaluation facility and certifies that all evaluation tasks are "**successful**."

2.3 Rating of Cryptographic Mechanisms According to ANSSI Technical Benchmarks

The cryptographic mechanisms implemented by the product's security functions (see [ST]) were analyzed in accordance with procedure [CRY-P-01], and the results were recorded in the [ETR] report.

This analysis did identify non-compliances with respect to benchmark [ANSSI Crypto]. They were taken into account in the independent vulnerability analysis conducted by the evaluator and did not show any exploitable vulnerabilities for the targeted attack potential.

2.4 Random Number Generator

The product includes a random number generator that was analyzed in accordance with procedure [CRY-P-01].

This analysis did not identify any non-compliances with respect to benchmark [ANSSI Crypto].

The independent vulnerability analysis carried out by the evaluator did not show any exploitable vulnerabilities for the targeted attack potential.

3 Certification

3.1 Conclusion

The evaluation was carried out in accordance with the rules and standards in force, with the requisite expertise and impartiality for an accredited evaluation facility. The overall evaluation work performed allows the issuance of a certificate in accordance with Decree 2002-535.

This certificate certifies that the evaluated product satisfies the security characteristics set out in its security target [ST] for the specified evaluation level.

3.2 Usage Restrictions

This certificate covers the product specified in chapter 1.2 of this certification report.

Users of the product must ensure the compliance with the security objectives regarding the operating environment, as specified in the security target [ST], and to follow the recommendations found in the provided guides [GUIDES].

3.3 Recognition of the Certificate

3.3.1 *European Recognition (SOG-IS)*

This certificate is issued under the terms of the SOG-IS agreement [SOG-IS].

The 2010 SOG-IS European Recognition Agreement allows the recognition, by the signatory countries of the agreement[1], of ITSEC and Common Criteria certificates. European recognition applies up to level ITSEC E3 Basic and CC EAL4 when CC dependencies are satisfied. Certificates recognized under this agreement are issued with the following mark:

3.3.2 *Common Criteria Recognition Arrangement (CCRA)*

This certificate is issued under the terms of the CCRA agreement [CCRA].

The Common Criteria Recognition Arrangement agreement allows the recognition of Common Criteria certificates by the signatory countries[2].

The recognition applies up to the CC EAL2 level assurance as well as to the ALC_FLR family. Certificates recognized under this agreement are issued with the following mark:

[1] The list of signatory countries of the SOG-IS agreement is available at the agreement's website: www.sogis.eu.

[2] The list of signatory countries of the CCRA is available at the agreement's website: www.commoncriteriaportal.org.

ANNEXE A. Documentary References for the Evaluated Product

[ST]	Reference security target for the evaluation: - *Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOs 9.4 Security Target*, version 1.4, October 27, 2023.
[ETR]	Evaluation technical report: - *Evaluation Technical Report PSD2 OS 2022 – WEXFORD4*, reference: WEXFORD4_ETR_1.1, version 1.1, November 27, 2023.
[CONF]	Product configuration list: - *Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOs 9.4 Configuration Item List, version 1.3, October 27, 2023.*
[GUIDES]	Product user guide: - *Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOs 9.4 Guidance*, version 1.2, October 17, 2023.

ANNEXE B. Reference related to the certification

Decree 2002-535 dated April 18, 2002 as modified relative to the evaluation and certification of the security offered by information technology products and systems.	
[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*, April 2017, version 3.1, revision 5, reference CCMB-2017-04-001; - *Part 2: Security functional components*, April 2017, version 3.1, revision 5, reference CCMB-2017-04-002; - *Part 3: Security assurance components*, April 2017, version 3.1, revision 5, reference CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, April 2017, version 3.1, revision 5, reference CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, July 2, 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0*, January 8, 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.