



**PREMIER
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 2022/05

**Strong Customer Authentication for Apple Pay on iPhone with
iPhone SE (2nd generation) running iOS 14.5.1
Version 18E212**

Paris, January 19th 2022

COURTESY TRANSLATION

WARNING

This report is intended to provide people who request evaluations with a document to certify the level of security provided by the product under the usage or operating conditions defined in this report for the version which was evaluated. It is also intended to provide potential acquirer of the product with the conditions under which they may use the product to ensure that they meet the conditions for which the product was 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 hypotheses and 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 relating to this report must 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

Reproduction of this document without alteration or division is authorized.

Certification Report reference	ANSSI-CC 2022/05
Product name	Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) running iOS 14.5.1
Product reference/version	Version 18E212
Evaluation criteria and version	Common Criteria version 3.1 revision 5
Evaluation level	EAL 2 augmented with ADV_FSP.3, ALC_FLR.3
Developer	APPLE INC. 7 place d'Iena 75016 Paris, France
Sponsor	APPLE INC. 7 place d'Iena 75016 Paris, France
Evaluation facility	THALES / CNES 290 allée du Lac, 31670 Labège, France
Applicable recognition agreements	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;"><p>This certificate is recognized at the level EAL2 augmented with FLR.3.</p></div><div style="text-align: center;"><p>This certificate is recognized at the level EAL2 augmented with FLR.3.</p></div></div>

FOREWORD

Certification of the security provided by information technology products and systems is governed by amended decree 2002-535 of 18th April 2002. This decree indicates that:

- The *Agence nationale de la sécurité des systèmes d'information* establishes certification reports. These reports specify the characteristics of the security objectives proposed. They may contain any warnings that their authors consider are worth mentioning for security reasons. The people who order the reports may choose whether or not to communicate them to third parties or to make them public (article 7).
- The certificates awarded by the *directeur général de l'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 current rules and standards, with the required levels of competence and impartiality (article 8).

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

TABLE OF CONTENTS

1	The product	6
1.1	Presentation of the product.....	6
1.2	Product description	6
1.2.1	Introduction.....	6
1.2.2	Security services	6
1.2.3	Architecture	6
1.2.4	Product identification.....	7
1.2.5	Life cycle	8
1.2.6	Evaluated configuration	8
2	The evaluation.....	9
2.1	Evaluation standards	9
2.2	Evaluation work.....	9
2.3	Cryptographic mechanisms analysis according to the ANSSI's technical reference bases.....	9
2.4	Random number generator analysis	9
3	The certification	10
3.1	Conclusion	10
3.2	Usage restrictions.....	10
3.3	Recognition of the certificate	10
3.3.1	European recognition (SOG-IS).....	10
3.3.2	International Common Criteria recognition (CCRA)	11
ANNEXE A.	Document references of the evaluated product	12
ANNEXE B.	Reference related to the certification.....	13

1 The product

1.1 Presentation of the product

The evaluated product is «Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) running iOS 14.5.1, version 18E212» developed by APPLE INC.

Apple Pay is a mobile payment solution developed by Apple. After registering a bank card in their Apple device, users can make payments with their device. For the payment to succeed, users must sign in on the device through a password, a digital fingerprint, or facial recognition. This device can be an iPhone, an iPad, an Apple Watch, or a Mac device.

For the evaluation, the only Apple hardware taken into account is iPhone SE (2nd generation) with the chip A13 Bionic, running iOS 14.5.1 (18E212) with fingerprint (Touch ID) and password as a means of user authentication.

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 (enrolment, authentication, etc.);
- secure use of Apple Pay and Apple Cash (provisioning of cards, management of transactions including anti-replay).
- protection of stored data (data encryption, secure erasure);
- protection of data in transit (biometric sensor to SEP, SEP to SE);
- secure software update.

1.2.3 Architecture

The TOE corresponds to the following elements of *iPhone SE (2nd generation)* running *iOS 14.5.1 (18E212)*, which are involved in the implementation of the services covered by this evaluation:

- *System on Chip A13 Bionic* including:
 - o the *Application Processor (AP)*: application processor running the operating system and user applications;
 - o the *Secure Enclave Processor (SEP)*: secure processor executing a secure operating system (SEPOS) and secure applications in a dedicated environment;
- the screen allowing, among other things, the user to type in their password to authenticate.

The product also relies on:

- the fingerprint matching system called Touch ID, which is connected to the SoC and used to authenticate the user ;
- a *Secure Element* (SE) to carry out banking transactions and ensure the cryptographic protection of sensitive information.

Figure 1 describes the product architecture.

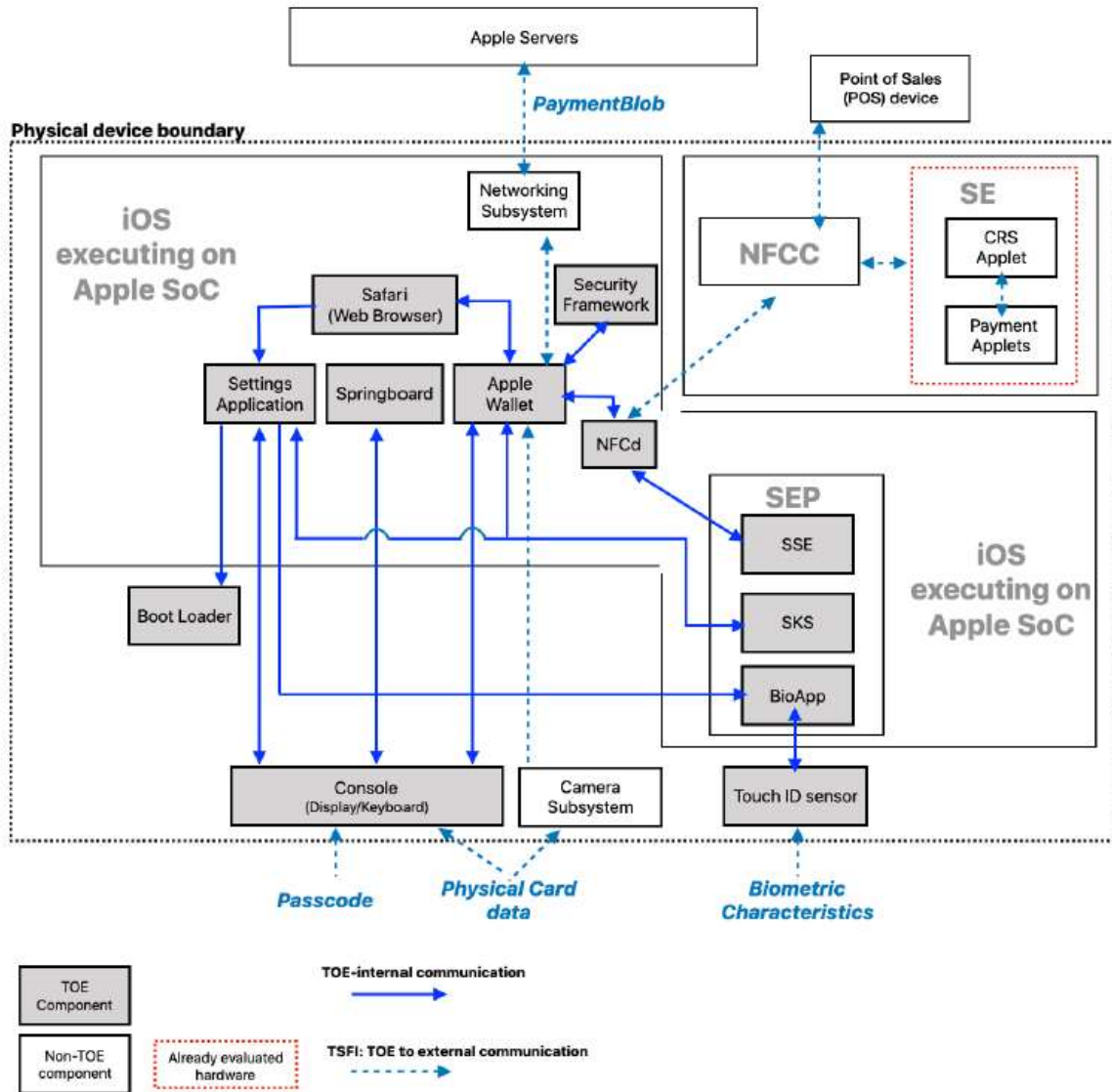


Figure 1 : Product architecture

1.2.4 Product identification

The product’s constituent elements are identified in the configuration list [CONF].

The certified version of the product can be identified by the elements of the table below, described in detail in terms of the security target [ST] in section 2.1 “Target of Evaluation Definition.”

Configuration elements		Source
Model	iPhone SE 2 nd generation	APPLE INC.

SoC	A32 Bionic	
<i>Touch ID version</i>	Gen 3	
<i>Secure Enclave (SEP)</i>	SEPOS part of iOS 14.5.1	
OS version	iOS 14.5.1 (18E212)	

In the phone settings, the section « *Settings* » then « *General* » and « *About* » display the operating system version under « *Software Version* ». By tapping « *Software Version* », the user will see build number 18E212 appear.

Note:

The *iOS version* (18E212 in this case) determines not only the operating version but also the system applications included therein, such as the Apple Pay application and the SEPOS version.

1.2.5 Life cycle

The product's life cycle is as follows:

- design: design of hardware and software;
- fabrication: fabrication of hardware and implementation of software;
- integration: integration of software and device;
- issuance: the product is delivered to the customer, ready to be initialized with the customer's user data.

The product was developed on the following site:

APPLE

Apple Park Way,
Cupertino, CA95014
United States

For the evaluation, the evaluator considered the end user as the product's sole user.

1.2.6 Evaluated configuration

The certificate relates to the products as described in the paragraph "1.2.4 Product identification."

2 The evaluation

2.1 Evaluation standards

The evaluation was carried out in accordance with the Common Criteria version 3.1 revision 5 [CC] and the evaluation methodology defined in the manual [CEM].

2.2 Evaluation work

The evaluation technical report [ETR] delivered to the ANSSI on November 23rd, 2021 details the work performed by the evaluation facility and certifies that all evaluation tasks are “**successful.**”

2.3 Cryptographic mechanisms analysis according to the ANSSI's technical reference bases

The cryptographic mechanisms implemented by the security functions of the product (see [ST]) were analysed in accordance with the procedure [CRY-P-01] and the results were recorded in the report [RTE].

This analysis did not identify any non-compliance with the [ANSSI Crypto] requirements. The independent vulnerability analysis performed by the evaluator did not show any exploitable vulnerability for the targeted attack potential.

2.4 Random number generator analysis

The product contains a random number generator which has been analysed in accordance with procedure [CRY-P-01].

This analysis did not identify any non-compliance with the [ANSSI Crypto] requirements.

This analysis did not reveal any blocking statistical biases. This does not make it possible to affirm that the data generated are really random but ensures that the generator does not suffer from major design flaws. As stated in the document [ANSSI Crypto], it is recalled that, for cryptographic use, the output of a hardware random number generator must imperatively undergo cryptographic algorithmic reprocessing, even if the analysis of the physical random generator did not reveal any weakness.

The independent vulnerability analysis performed by the evaluator did not show any exploitable vulnerability for the targeted attacker level.

3 The certification

3.1 Conclusion

The evaluation was carried out in accordance with applicable rules and standards and with the expertise and impartiality required from licensed evaluation facility. All the evaluation work carried out allows the issuance of a certificate in accordance with Decree 2002-535.

This certificate certifies that the «*Strong Customer Authentication for Apple Pay on iPhone SE 2nd generation running iOS 14.5.1, Version 18E212*» product submitted for evaluation meets the security characteristics specified in its security target [ST] for the evaluation level EAL 2 augmented with ADV_FSP.3 and ALC_FLR.3.

3.2 Usage restrictions

This certificate pertains to the product specified in chapter 1.2 of this Certification Report.

The user of the certified product must ensure the compliance with the security objectives for the operating environment, as specified in the security target [ST], and follow the recommendations in the provided guides [GUIDE].

3.3 Recognition of the certificate

3.3.1 European recognition (SOG-IS)

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

The 2010 SOG-IS European recognition agreement enables recognition of the ITSEC and Common Criteria certificates by the countries which have signed the agreement¹. European recognition applies up to ITSEC E3 Elementary and CC EAL4 level. The certificates that are recognised in the context of this agreement are issued with the following mark:

Certificates recognized under this agreement are issued with the following mark:



¹ The list of signatory countries of the SOG-IS agreement is available on the website www.sogis.org.

3.3.2 International Common Criteria recognition (CCRA)

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

The "Common Criteria Recognition Arrangement" enables recognition of the Common Criteria certificates by the signatory countries².

Recognition applies to CC EAL2 level assurance components and the ALC_FLR family. The certificates that are recognised in the context of this agreement are issued with the following mark:



² The list of signatory countries of the CCRA arrangement is available on the website www.commoncriteriaportal.org.

ANNEXE A. Document references of the evaluated product

[ST]	Security Target for the evaluation : <ul style="list-style-type: none">- Strong Customer Authentication for Apple Pay on iPhoneSE (2nd generation) with A13 Bionic running iOS 14.5.1 Security Target, version 1.6, 23 Novembre 2021.
[RTE]	Evaluation Technical Report: <ul style="list-style-type: none">- Evaluation Technical Report Flamingo, version 1.2, 23 Novembre 2021.
[CONF]	Product configuration list : <ul style="list-style-type: none">- Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) with A13 Bionic running iOS 14.5.1 Configuration Item List, version 1.3, 23 Novembre 2021.
[GUIDE]	Product User Guide : <ul style="list-style-type: none">- Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) with A13 Bionic running iOS 14.5.1 Guidance, version 1.3, 23 Novembre 2021.

ANNEXE B. Reference related to the certification

Decree 2002-535 of April 18, 2002, as amended, relating to the evaluation and certification of the security offered by information technology products and systems.	
[CER-P-01]	<i>Procédure ANSSI-CC-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, ANSSI.</i>
[CRY-P-01]	<i>Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, ANSSI.</i>
[CC]	Common Criteria for Information Technology Security Evaluation: <ul style="list-style-type: none">- 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.
[ANSSI Crypto]	<i>Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.</i>
[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.