

Security Target

ST introduction

The reference of this ST is **TESS V7.1 FeliCa-CryptoLibrary Security Target version 1.0**

TOE

The TOE is an IC Platform composed with the FeliCa Crypto Library. Designed to meet the security functionality of the package “FeliCa Crypto Library” defined in Mobile FeliCa Applet Protection Profile[MFAPP].

TOE reference

The TOE is referred to as **TESS V7.1** and is named and uniquely identified as follows:

Platform identification data (TESS v7.1 OS v1.19)

OS Ident. command Get Data command (tag FE)

Expected value FE15060A2B060104012A026E01030607D0027115DA0113

Field	Value
Javacard version	2B060104012A026E0103
OS information	
- PDM counter	D0027115DA
- OS release	0113 (=v1.19)

Patch Ident. command Get Data command (tag FD)

Expected value FD0400010000

Field	Value
- Patch major revision	0001
- Patch minor revision	0000

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
IC	SENSN6H	(diced) wafer/module/card	ICCN0304	2023-08-31
JavaCard	TESS V7.1	Embedded onto the IC	PCN0215	2024-12-06
Crypto libraries	V2.6.0	Embedded onto the IC	PCN0215	2024-12-06
FeliCa Crypto library		Embedded onto the IC	CCP-SEL2-063	2024-12-19
Security Guidance		Documentation (*)	n/a	n/a

(*) Documentation

D1516176 (v4.1)	Guidance for Secure application development on Thales Embedded Secure Solutions, December 2024
D1619041 (v1.0)	Operational guidance on CC platforms - TESS V7.1, June 2024
D1620259 (v1.0)	Operational guidance for VA - TESS V7.1, June 2024
D1619304 (v1.0)	Evaluated_API_TESS_V7.1, November 2024
GPC_GUI_050 (v2.0)	Composition Model – Security Guidelines for Basic Applications

The TOE claims the following FeliCa Crypto library packages of the [MFAPP] section 6:

DES1 DES2 DES3 AES1 AES2

Information for Composite Evaluations

[CL-ETRFC] has to be assessed as part of any composite evaluation using this Crypto Library.

Conformance claims

This ST does not claim compliance to any PP but it is based on [MFAPP] as it uses the FeliCa Crypto Library packages defined in [MFAPP] Section 6.

This ST claims to be conformant to the Common Criteria version 3.1, revision 5.

This ST is CC Part 2 conformant:

- Exactly, the SFRs of the [MFAPP] Section 6 are included by reference.

The ST is CC Part 3 conformant:

- The assurance package is **EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.**

The rationale behind these claims is the requirement that the FeliCa Approval for Security and Trust (FAST) scheme requires compliance to this [MFAPP] for this TOE type (FeliCa products).

Security Problem Definition

Refer to [MFAPP] Section 6.

Objectives

Refer to [MFAPP] Section 6 and TOE FeliCa Crypto Library algorithms selected in section “TOE overview”.

Extended components definition

Refer to [MFAPP] Section 6.

Security Requirements

Security Functional Requirements

Refer to [MFAPP] Section 6 and TOE FeliCa Crypto Library algorithms selected in section “TOE overview”.

Security Assurance Requirements and Rationale

See section “Conformance claims”.

TOE Summary Specification

The TOE implements the SFRs in accordance to the FeliCa CL specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

References

[FeliCa-CL-Tool]	FAST FeliCa Crypto Library API Checker tool list version 1.0
[MFAPP]	FeliCa Networks, Inc. Mobile FeliCa Applet Protection Profile, version 1.0
[CL-ETRFC]	25-RPT-062 v2.0, FeliCa-Evaluation Technical Report for Composition of
Thales TESS v7.1	

ST revision history

0.1	Creation with v1.0 template
1.0	16/01/2024 Update: TOE reference (identification), TOE overview (certificate)