

Security Target

ST introduction

The reference of this ST is **FeliCa-CryptoLibrary-ST - Combo_CE_4.2.3_v1.2** 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 **Combo CE 4.2.3 v1.2** and is named and uniquely as follows:

Platform:

- Identification data: GET DATA command using tag 00FE
- Value for this product: FE15060A2B060104012A026E01030607D0023F15460110 (see below for interpretation)

Field	Value
Java Card version	2B060104012A026E0103
OS information	
- PDM counter	D0023F1546
- OS release	0110 (meaning OS Release / Check Point 1.10)

TOE overview

The TOE consists of the following components:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
IC	ST54J Rev C & D ST54K Rev D	(diced) wafer/module/card	ICCN0260X (*)	September 20, 2024 (*)
Java Card	Combo CE 4.2.3 v1.2	Embedded onto the IC	PCN0179.02 (**)	August 7, 2020
Crypto libraries	ST54J v3.5.0.0 CP 1.82.1.21	Embedded onto the IC	PCN0179.02 (**)	August 7, 2020
FeliCa Crypto library		Embedded onto the IC	CCP-SEL2-036	July 1 st , 2022
Security Guidance		Documentation (***)	n/a	n/a

(*) ICCN0260 expired November 30, 2024, but the Extension Recognition Letter has been issued on November 28, 2024, with a date of reassessment on September 20, 2024

(**) PCN0179.02 valid until August 7, 2025

(***) Documentation

- D1516176, v2.0 – Guidance for Secure application development on Thales Embedded Secure Solutions
- D1516178, v1.0 – Operational guidance of Thales Embedded Secure Solutions for VA
- D1516180, v1.0 – Operational guidance of Thales Embedded Secure Solutions
- D1546158, v1.1 – Security Technical Note for the guides

- D1563865, v1.0 – Evaluated API – Combo CE 4.2.3 v1.2
- GPC_GUI_050, v2.0 – Composition Model Security Guidelines For Basic Application

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 with 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]	24-0889_FAST-2500028-01_F-ETRfc_v1.0

ST revision history

- 0.1 Creation (February 3, 2025)
- 0.2 Correction following the Evaluation lab remarks (February 4, 2025)
 - Typos
 - Correction of information from Extension Recognition Letter
- 0.3 Correction following the Evaluation lab remarks (February 5, 2025)
 - Typo in file name
 - Removing useless reference
- 1.0 Corrections following the official template (March 11, 2025)
 - Add the documentation references to the TOE components table
 - Update ETRfc reference to its final version