

# Security Target

## ST introduction

The reference of this ST is **FeliCa-CryptoLibrary-ST-template-v1.0 - COMBO\_CE\_4.2.3\_V1.1** 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 v1.1 and is named and uniquely identified as follows ([IDENT-CONF]):

### **Platform :**

Identification data                      Get Data command (tag FE)

Value for this product                      FE15060A**2B060104012A026E0103**0607**D0023F15240112**

Field	Value
Javacard version	2B060104012A026E0103
OS information	
- PDM counter	D0023F1524
- OS release	0112 (1.12)

## TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
IC	ST54J Rev C & D ST54K RevD	(diced) wafer/module/card	ICCN0260 (*)	Nov.30,.2018
JavaCard	COMBO CE 4.2.3 v1.1	Included in the PCN	PCN0179.01 (**)	Aug.7 2020
Crypto libraries	CP 1.82.1.21	Included in the PCN	PCN0179.01 (**)	Aug.7 2020
FeliCa Crypto library		Included in the PCN	CCP-SEL2-038	July 1st 2022

(\*) ICCN0260 renewal completed, and valid until Nov.30 2024

(\*\*) PCN0179.01 valid until Aug.7 2024

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] FeliCa Evaluation Technical Report for Composition – 24-0260 Project –  
FAST-2400047-01 – Combo CE 4.2.3 v1.1 on STMicroelectronics ST54J rev.C &D/K rev.D, version  
1.0 (Ref. : 24-0260\_F-ETRFC\_v1.0)  
[IDENT-CONF] D1539040\_Platform\_IdentificationConfigurability v1.1 for Combo CE  
4.2.3 V1.1

## ST revision history

- 0.1 Creation (March 1st 2024)
- 1.0 Updated with ETRfc reference (May 14 2024)