Security Target

ST introduction

The reference of this ST is **FeliCa-CyptoLibrary-ST on TESS v5.2 Rev 02, TESS v5.2 Rev 03, TESS v5.2.1 Rev 01 and TESS v5.2.1 Rev 02** version **v1.1**

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 v5.2 Rev 02, TESS v5.2 Rev 03, TESS v5.2.1 Rev 01 and TESS v5.2.1 Rev 02**, and is named and uniquely identified using the GetVersion command as follows:

Platform identification data (TESS v5.2 and TESS v5.2.1)

Identification data Get Data command (tag FE)

Value for this product FE15060A2B060104012A026E01030607D0026115C60115

Field	Value
Javacard version	2B060104012A026E0103
OS information - PDM counter - OS release	 D0026115C6 0115 (1.21)

Four patches configurations are available:

Configuration 1: TESS v5.2 Rev 02

Identification data Get Data command (tag FD)

Value for this product FD0400090000

Field	Value
- OS Patch revision	00090000

Configuration 2: TESS v5.2 Rev 03

Identification data Get Data command (tag FD)

Value for this product FD04000A0000

Field	Value
- OS Patch revision	000A0000

Configuration 3: TESS v5.2.1 Rev 01

Identification data Get Data command (tag FD)

Value for this product FD04000B0000

Field	Value
- OS Patch revision	000B0000

Configuration 4: TESS v5.2.1 Rev 02

Identification data Get Data command (tag FD)

Value for this product FD04000C0000

Field	Value
- OS Patch revision	000C0000

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	**S3NSEN6 Rev2**	**(diced) wafer/module/card**	**ICCN0291 valid until 20 June, 2026**	**2022-06-20**
Java Card	**TESS v5.2 Rev02, TESS v5.2 Rev03, TESS v5.2.1 Rev01, TESS v5.2.1 Rev02**	**Embedded in the above**	**PCN0203.03 PCN0203.04 PCN0203.05 PCN0203.06 valid until 24 Feb 2027**	**2023-02-24**
FeliCa Crypto library		**Embedded in the above**	**N/A**	**N/A**

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] 25-0317_FAST-2400149-02_F-ETRfC_v1.3

ST revision history

1.0 Creation with v1.0 template

1.1 Minor updates