FeliCa Approval for Security and Trust scheme Application Note for FeliCa Crypto Library v1.0

1. Introducing the documentation

FeliCa Networks, the scheme owner of the FeliCa Approval for Security and Trust (FAST) scheme and manager of the risks to FeliCa systems and the FeliCa brand, decided that for evaluations against the PP[MFAPP], the following application notes shall be applied.

1.1 Application note ASE

The FAST scheme provides a ST template that can be used and fulfils the ASE requirements efficiently (if the ST template is not used, then the Evaluator shall perform the full ASE evaluation and report its result)

The TOE identification must include a clear and explicit reference to the identification method.

The identification method shall be clearly and completely described to the customers of the product, and shall be sufficiently practical to be applied by the customer and any entity determining whether a product is the evaluated product when a product is taken from the field.

The method of identification may consist of several identification steps. For example, the verification of the hardware part may differ from the verification of the software parts.

Note that this method of product identification shall be used to verify the platform identifier during any subsequent composite activity, and in situations where it is contested that a product found in the field is the evaluated product.

The evaluator shall determine that the product identification is consistent with the product identification method. The evaluator shall determine that any underlying platform identification steps relevant for the product identification are performed or consistently communicated to the user of the product as needing to be verified.

The evaluator shall verify that the samples can be used according to the TOE identification method. Any divergence for testing purposes (such as test patches or configuration settings) must be documented in the ETR, including an analysis why this has no negative impact on the assurance gained.

As per application note, the Security Target should also identify which of the TOE designs is applicable.

Correctness of the ST template operations from the PP shall be verified by the evaluator.

The evaluator shall report this verification with a simple statement in the ETR.

1.2 Application note AGD

[FeliCa-CL-Spec] is the sole and complete operational guidance for the FeliCa part of the TOE in the operational state. FeliCa Crypto Library is included in the binary code of the Java Card platform, so any (pre-)personalization guidance are considered to be in the scope of AGD_PRE.1 of the platform.

The evaluator and certifier should consider the [FeliCa-CL-Spec] to fulfil the requirements of AGD_OPE.1. And the evaluators should verify that no other manual is referred to by the developer for the contactless interface and the contact interface in the operational state.

The evaluator shall check that any additional preparative guidance, executed by experienced personalizers, is clear and leads to the TOE as tested by the evaluator. The evaluator shall report this verification with a simple statement in the ETR.

1.3 Application note ADV

1.3.1 Application note ADV_FSP

The FeliCa Crypto Library specifications [FeliCa-CL-Spec] are the sole and complete specification of the functionality of the FeliCa part of the TOE.

The evaluators should verify that no other specification is referred to by the developer. No other specification shall be deemed relevant by the evaluators. If only [FeliCa-CL-Spec] are referred to, the evaluator and certifier should consider the requirements of ADV_FSP to be fulfilled.

The evaluator shall report this verification with a simple statement in the ETR.

1.3.2 Application note ADV_TDS

The evaluator should gather the understanding of the design specification during the ADV_IMP activities (as allowed under “Collection of Developer evidence”).

The evaluator shall report this understanding of the security architecture in a short summary in the ETR

1.3.3 Application note ADV_ARC

The evaluator should gather the understanding of the security architecture during the ADV_IMP activities (as allowed under “Collection of Developer evidence”).

The evaluator shall report this understanding of the security architecture in a short summary in the ETR.

1.3.4 Application note ADV_IMP

During the code review, the evaluator shall also verify that:

- The code matches the standard design identified in the ST.
- The FeliCa functional testing will exercise all relevant code paths and behaviour of the TOE. This may be determined by code review, code coverage tools, or other means.

- All relevant guidance of the underlying platform is applied.

- The scope of the evaluation of the underlying platform includes at least AES, DES and RNG functionality, and in the case of an open platform separation between the applications and the FeliCa functionality.

The evaluator shall report this verification with a simple statement in the ETR.

1.3.5 Application note ADV_COMP

The developer shall analyse that the source code is compliant with the user guidance of the underlying platform certified by CC or EMVCo.

The evaluator shall report the verification of the analysis with a detailed analysis in the ETR.

1.4 Application note ATE

The FeliCa Crypto Library functional testing is mandatory for all platform vendors. The evaluator and certifier shall consider the SE L2 certification of Mobile FeliCa Chipset Certification Program to fulfil the requirements of ATE_COV, ATE_FUN and ATE_IND. If the developer doesn't have the SE L2 certification, the developer shall provide the result of the API Checker tool [FeliCa-CL-Tool] provided from FeliCa Networks and the evaluator shall check the result. The evaluator shall report the SE L2 certification ID of Mobile FeliCa Chipset Certification Program or the result of the API Checker in the ETR.

The evaluator shall determine in ADV_IMP that the FeliCa functional testing exercises all relevant behavior of the TOE, considering especially whether there are execution paths unlikely to be exercised. The evaluator and certifier shall consider this to fulfil the requirements of ATE_COV and ATE_DPT.

The evaluator shall report the result of this check with a simple statement in the ETR.

1.3 Application note ALC_LCD/CMC/CMS/DVS/DEL/TAT

The development and production life-cycle is expected to follow the [PP84] life cycle.

All sites involved in the development and production must be audited in compliance to the applicable requirements from those Common Criteria or EMVCo requirements. The site audits can be reused from the date of the site audit according to the current SOG-IS approach. Sites may be re-used on the basis of both site and product certifications.

The evaluator shall report this verification with an overview of the sites, their role, the applicable audit report and validity date, and a statement that the evaluator has verified that the combination of sites together is likely able to develop and produce the complete product securely.

1.4 Application note AVA

The evaluator's vulnerability analysis shall use the relevant FeliCa security analysis [FeliCa-SA] and [FeliCa-CL-SG] for the definition of the assets and for a minimum set of possible attacks to be considered. This analysis shall be done together with the analysis of the underlying Platform ETRfc.

Any protocols and guidance not listed in the FeliCa specification [FeliCa-CL-Spec] should be evaluated additionally, as they are not covered by the security analysis document.

Rating shall be done according to the latest version of JIL Application of Attack Potential to Smartcards [AM] and JIL Attack Methods for Smartcards and Similar Devices [AP].

The evaluator shall report his/her analysis, including the versions of the [FeliCa-SA], JIL Application of Attack Potential and JIL Attack Methods for Smartcards and Similar Devices in the ETR.

The evaluator shall generate the CL ETRfc. This document is required to be based on [ETR-tmpl].

2. Reference documentations

[AM]	Joint Interpretation Library Attack Methods for Smartcards and Similar Devices, version 2.4
[AP]	Joint Interpretation Library Application of Attack Potential to Smartcards, version 3.2, dated November 2022
[FeliCa-SA]	FeliCa Security Analysis, FN15-F002-E01-40, version 1.40
[FeliCa-CL-Spec]	FAST FeliCa Crypto Library Specifications for AES1, version 1.0 FAST FeliCa Crypto Library Specifications for AES2, version 1.0 FAST FeliCa Crypto Library Specifications for DES1, version 1.0 FAST FeliCa Crypto Library Specifications for DES2, version 1.0 FAST FeliCa Crypto Library Specifications for DES3, version 1.0
[FeliCa-CL-Tool]	FAST FeliCa Crypto Library API Checker tool list version 1.0
[FeliCa-CL-SG]	Security guidelines for the FeliCa crypto library AES, dated 2016-05-26 Security guidelines for the FeliCa crypto library DES, dated 2016-05-26
[PP84]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0
[MFAPP]	Mobile FeliCa Applet Protection Profile version 1.0