FeliCa Approval for Security and Trust scheme Application Note for FeliCa Card v1.1

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[PTPP], 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-UM] and [FeliCa-SRMs] are the sole and complete preparative and operational guidance for the FeliCa part of the TOE on the contactless interface and on the optional contact interface in the operational state. Any (pre-)personalization guidance such as [FeliCa-PAP] are considered to be in the scope of AGD_PRE.1

The evaluator and certifier should consider the [FeliCa-UM], [FeliCa-SRMs] and [FeliCa-PAP], and of the FeliCa specification, to fulfil the requirements of AGD_OPE.1 and AGD_PRE.1 respectively. And the evaluators should verify that no other manual is referred to by the developer for the contactless interface and optional 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 up to ADV_FSP.5

The FeliCa specification [FeliCa-Specs],[FeliCa-SRMs] and the standards such as ISO 18092 they refer to, are the sole and complete specification of the functionality of the FeliCa part of the TOE on the contactless interface and on the optional contact interface in the operational state.

The evaluators should verify that no other specification is referred to by the developer for the contactless interface and optional contact interface in the operational state. No other specification shall be deemed relevant by the evaluators. If only [FeliCa-Specs] and all standards referred from these such as ISO 18092, are referred to, the evaluator and certifier should consider the requirements of ADV_FSP to be fulfilled as all are industry standards well known to meet these requirements.

Any specifications referred to for the administrative interfaces not covered by the above, shall be evaluated in accordance to ADV_FSP.

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

1.3.2 Application note ADV_TDS up to ADV_TDS.5

The FeliCa design specification [FeliCa-TDS] is sole and complete design specification and provides a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

The evaluator shall verify, as part of the ADV_IMP activities, that the source code fits the design as described above.

If the source code fits the design as described above and the evaluator can perform the ADV_IMP activities with little confusion on the structure of the TOE, the requirements of ADV_TDS are considered fulfilled (as allowed under “Collection of Developer evidence”).

The evaluator shall report the verification that the source code fits the design with a simple statement in the ETR.

1.3.3 Application note ADV_ARC

The FeliCa security architecture [FeliCa-ARC] explains how the implemented security mechanisms contribute to the security properties.

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_INT up to ADV_INT.3

The FeliCa internal structure [FeliCa-INT] explains that the entire TSF is well structured.

The evaluator shall verify, as part of the ADV_IMP activities, that the source code is well structured as described above.

If the source code is well structured as described above and the evaluator can perform the ADV_IMP activities with little confusion on the structure of the TOE, the requirements of ADV_INT are considered fulfilled (as allowed under “Collection of Developer evidence”).

The evaluator shall report the verification that the source code fits the design with a simple statement in the ETR.

In case of ADV_INT.3, the developer shall provide an internal description which demonstrate that the entire TSF is not overly complex.

The evaluator shall confirm that information provided meets all requirements for content and presentation of evidence and perform an internal analysis on the entire TSF.

The evaluator shall report this result of the internal analysis in a short summary in the ETR.

1.3.5 Application note ADV_IMP up to ADV_IMP.2

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 (hardware, any crypto libraries, any OS) is applied.
- The scope of the evaluation of the underlying platform includes at least AES 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.

1.3.6 Application note ADV_SPM

The developer shall provide a formal security policy model. For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.

The developer shall provide a formal proof of correspondence between the model and any formal functional specification and a demonstration of a correspondence between the model and the functional specification.

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

The evaluator shall report the result of the confirmation in a short summary in the ETR.

1.3.7 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 test suites [FeliCa-ATE] are considered to meet the ATE_COV.3, ATE_DPT.3 and ATE_FUN.2 requirements for FeliCa functionality as defined in [PTPP] and [FeliCa-Spec]. The evaluator shall verify that all test suites have been successfully applied to the current TOE by the developer. The evaluator and certifier shall consider the testing is performed completely there is no useful additional functional test, and as the testing is performed by the developer already there is no useful additional independent testing to fulfil the requirements of ATE_IND.2.

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.

1.5 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.

1.6 Application note AVA

The evaluator's vulnerability analysis shall use the relevant FeliCa security analysis [FeliCa-SA] for the definition of the assets and for a minimum set of possible attacks to be considered.

Any protocols and guidance not listed in the FeliCa specification [FeliCa-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.

2. Reference documentations

[AM]	Joint Interpretation Library Attack Methods for Smartcards and Similar Devices, (latest version)
[AP]	Joint Interpretation Library Application of Attack Potential to Smartcards, (latest version)
[FeliCa-ARC]	FeliCa OS Version 5 Security Architecture, OS5-ARC-E01-00, version 1.0
[FeliCa-ATE]	FeliCa OS Version 5 Test coverage and depth analysis, OS5-COV-E01-10, version 1.10 FeliCa OS Version 5 Test Specification, OS5-ATE-E01-00, version 1.00
[FeliCa-INT]	FeliCa OS Version 5 Internal Structure of TSF, OS5-INT-E00-90, version 0.9
[FeliCa-PAP]	Product Acceptance Procedure, M985-E01-10, version 1.1
[FeliCa-SA]	FeliCa Security Analysis, FN15-F002-E01-70, version 1.70
[FeliCa-Specs]	FeliCa OS Version 5 Functional Specification, OS5-FSP-E01-00, version 1.0
[FeliCa-SRM]	FAST Security Reference Manuals for AES1 v1.0 FAST Security Reference Manuals for AES2 v1.0
[FeliCa-TDS]	FeliCa OS Version 5 TOE Design Specification, OS5-TDS-E01-00, Version 1.0

[FeliCa-UM]	FeliCa Card User's Manual, M660-E01-41, version 1.41
[PP84]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0
[PTPP]	Public Transportation IC Card Protection Profile, version 1.12