JPKI Applet SAR Application Note v1.00

1. Introducing the documentation

Digital Agency, the scheme owner of the JPKI Security Certification scheme for Mobile Devices (JPKI-MD) and manager of the risks to JPKI systems, decided that for evaluations against the PP [JPKIPP], the following application notes shall be applied.

At the beginning of the evaluation, the evaluator shall check if a JPKI Applet Intermediate Report (JAIR) exists for the JPKI Applet version under evaluation. In case it does not exist, it is required to generate such document as part of the outcome from the evaluation. This document can later be used to reuse part of the JPKI Applet evaluation results in a similar way an ETRfc is used during a composite evaluation. The ETRfc template should be used as a basis to create this document.

In case a JAIR exists, then evaluator shall reuse the evaluation work presented in the JAIR as it is explained in the following sections. JAIR reuse is only possible within the same Lab.

Application note ASE

The JPKI-MD 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. It is required that the JPKI Applet is identified individually.

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.

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.

1.1 Application note AGD

AGD evidences are covered by the pre-compiled evidences explained in this section. The developer does not need to provide any additional evidences.

[JPKI-UM] and [JPKI-Spec] are the sole and complete preparative and operational guidance for the JPKI Applet part of the TOE on the contactless interface and on the contact interface in the operational state.

The evaluator and certifier should consider the [JPKI-UM] and [JPKI-PRE], and of the JPKI 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 the contact interface in the operational state. In case there is any additional guidance required to identify the underlying platforms (IC and OS), the evaluator shall check this guidance is listed in the ST, it is clear, it works as it is expected, and matches with the identification of the TOE defined in the ST.

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.

1.2 Application note ADV

1.2.1 Application note ADV_FSP

ADV_FSP evidences are covered by the pre-compiled evidences explained in this section. The developer does not need to provide any additional evidences.

The JPKI specification [JPKI-Spec] is the sole and complete specification of the functionality of the JPKI Applet part of the TOE on the contactless interface and on the 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 the contact interface in the operational state. No other specification shall be deemed relevant by the evaluators. If only [JPKI-Spec] is 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 and JAIR.

JAIR reuse: The evaluator only needs to check that the JPKI Applet Intermediate Report (JAIR) confirms that the above requirements have been successfully verified. The evaluator shall report this verification with a simple statement in the ETR.

1.2.2 Application note ADV_TDS

ADV_TDS evidences are covered by the pre-compiled evidences explained in this section. The developer does not need to provide any additional evidences.

The JPKI design specification [JPKI-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 only minor discrepancies 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 and JAIR.

JAIR Reuse: The evaluator shall check that the JPKI Applet Intermediate Report (JAIR) confirms that as part of the ADV_IMP activities, the JPKI Applet source code fits the design as described above.

1.2.3 Application note ADV_ARC

ADV_ARC evidences are covered by the pre-compiled evidences explained in this section. The developer does not need to provide any additional evidences.

The JPKI security architecture [JPKI-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 and JAIR.

JAIR Reuse: The evaluator shall check that the JPKI Applet Intermediate Report (JAIR) confirms that as part of the ADV_IMP activities, the JPKI Applet source code fits the design as described above.

1.2.4 Application note ADV_IMP

The source code of JPKI Applet has been provided with the evaluator and evaluated in advance.

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

- The code matches the standard design identified in the ST.
- The JPKI 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 (see also ADV_COMP).

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

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

JAIR Reuse: The evaluator only shall check that the JPKI Applet Intermediate Report (JAIR) confirms that the relevant points from above were covered as part of the ADV_IMP activities.

1.2.5 Application note ADV_COMP

The evaluator shall analyse that the source code is compliant with the user guidance documents of the respective underlying platforms certified by CC or EMVCo.

Although this activity cannot be carried out at applet level independently from the specific platform to be used on the final TOE, it is expected that the JPKI Applet Intermediate Report (JAIR) contains valuable information regarding ADV_IMP and AVA activities, which are expected to speed up this activity.

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

1.3 Application note ATE

The JPKI test suites [JPKI-ATE] are considered to meet the ATE_COV.2, ATE_DPT.1 and ATE_FUN.1 requirements for JPKI functionality as defined in [JPKIPP] and [JPKI-Specs]. The evaluator shall verify that all test suites have been successfully applied to the current TOE by JPKI Applet developer. The developer needs to ask JPKI Applet developer to provide test results for the evaluator. 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 and ATE_COMP.

The evaluator shall determine in ADV_IMP that the JPKI functional testing exercises all relevant behaviour 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 and JAIR.

JAIR Reuse: The evaluator only shall check that the JPKI Applet Intermediate Report (JAIR) confirms that the above check was successfully verified.

1.4 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.

This needs to be reported both in ETR and JAIR.

Regarding ALC_COMP, the evaluator has to confirm that all the TOE composite components can be properly identified as it was required in ASE section. The evaluator shall check the JPKI Applet developer acceptance procedures are clear and add a summary of them in the JAIR.

JAIR Reuse: The evaluator shall check that the JPKI Applet Intermediate Report (JAIR) covered the above requirements, and explicitly verify:

1. The validity of the involved sites is not expired (ALC_DVS).

2. There is no major discrepancy between the underlying platform acceptance and installation procedures and the JPKI Applet procedures described in JAIR (ALC_COMP).

1.5 Application note AVA

In case there is no available JAIR for the JPKI Applet under evaluation, the initial vulnerability analysis shall be done independently from any potential underlying platform used together with the Applet. In case, it is detected something is missing in the JAIR, the Lab shall update the JAIR and submit it to the certifier. The analysis shall contain the list of potential vulnerabilities found and any related requirement from the underlying platform required to cover such vulnerabilities.

Any protocols and guidance not listed in the JPKI specification [JPKI-Specs] should be evaluated that do not add any additional threat, as they are not covered by the security analysis document.

The evaluator shall report their analysis, including the versions of the JIL Application of Attack Potential and JIL Attack Methods for Smartcards and Similar Devices in the ETR and JAIR.

This analysis shall be done together with the analysis from ADV_COMP, from the underlying Platform ETRfc's and the JAIR input. The Lab needs to confirm that the whole VA is covering the current state of the art. In case, it is detected something is missing in the JAIR, the Lab shall update the JAIR and submit it to the certifier.

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 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)
[JPKI-ARC]	Commercial Applet for Mobile JPKI Projects Security Design Document v0.6 Security Design Document Appendix1 Security Design Document Appendix2
[JPKI-ATE]	JPKI Applet Test Overview v0.5 JPKI Applet Test Specification 0.5 ATE Analysis ARC and Test mapping v0.5 ATE Analysis SFR and Test mapping v0.5
[JPKI-PRE]	JPKI Applet Delivery and Acceptance procedure v0.6
[JPKI-Specs]	Commercial Applet for Mobile JPKI Projects External Interface Specification v1.0 SFR and TSFI mapping v0.61
[JPKI-TAT]	JPKI Applet Build procedure v0.6
[JPKI-TDS]	Commercial Applet for Mobile JPKI Projects Basic Design Document v0.5 Commercial Applet for Mobile JPKI Projects Detailed Design Document v0.5
[JPKI-UM]	Commercial Applet for Mobile JPKI Projects External Interface Specification v1.0 JPKI Applet User guidance v0.7 JPKI Applet Installation Procedure v0.6
[PP84]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0
[JPKIPP]	JPKI Applet Protection Profile version 1.10