Certification Report

PWPW SmartApp-ID 5.0 (SIGN configuration)

Sponsor and developer:	***Polska Wytwórnia Papierów Wartościowych S.A*** **ul. Sanguszki 1** **00-222 Warszawa** **Poland**
Evaluation facility:	***TÜV Informationstechnik GmbH*** **Am TÜV 1** **45307 Essen** **Germany**
Report number:	**NSCIB-CC-2300120-01-CR2**
Report version:	**2**
Project number:	NSCIB-**2300120-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**25 April 2025**
Number of pages:	**12**
Number of appendices:	**0**

CONTENTS

Foreword **3**

Recognition of the Certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **6**

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 8
2.6.1 Testing approach and depth 8
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 9
2.8 Evaluated Configuration 9
2.9 Evaluation Results 9
2.10 Comments/Recommendations 9

3 Security Target **10**

4 Definitions **10**

5 Bibliography **11**

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the PWPW SmartApp-ID 5.0 (SIGN configuration). The developer of the PWPW SmartApp-ID 5.0 (SIGN configuration) is Polska Wytwórnia Papierów Wartościowych S.A located in Warszaw, Poland and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE provides the functionality of a secure signature creation device (SSCD). It is intended for the usage in cryptographic cards and other products providing the SSCD functionality. The digital signature created by the SSCD may be used to create an advanced electronic signature as defined in Article 26 of *[EU-REG]*.

The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 25 April 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the PWPW SmartApp-ID 5.0 (SIGN configuration), the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the PWPW SmartApp-ID 5.0 (SIGN configuration) are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ATE_DPT.2 (Testing: security enforcing modules), ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by TÜV Informationstechnik GmbH included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

This document was re-issued as version 2 to correct an error in the evaluation completion date.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the PWPW SmartApp-ID 5.0 (SIGN configuration) from Polska Wytwórnia Papierów Wartościowych S.A located in Warszaw, Poland.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) registered under the reference BSI-DSZ-CC-1149-V3-2023	R1/R2/R3
Platform	JCOP 4.5 P71, registered under the reference NSCIB-CC-2300127-01	
Software	PWPW SmartApp-ID (SIGN configuration)	5.0

To ensure secure usage a set of guidance documents is provided, together with the PWPW SmartApp-ID 5.0 (SIGN configuration). For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]* or *[ST-Lite*, Chapter 1.3.5.

2.2 Security Policy

The TOE is a Java Card configured to provide a contact and contactless integrated-circuit (IC) chip containing components to securely create, use and manage signature-creation data (SCD) with key generation. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to establish a secure channel for the signature PIN.

The TOE provides the following functionalities:

1. generate signature creation data (SCD) and the correspondent signature verification data (SVD),
2. export the SVD for certification,
3. import signature creation data (SCD),
4. receive and store certificate info,
5. switch the TOE from a non-operational state to an operational state,
6. if in an operational state, to create digital signatures for data with the following steps:
    a. select an SCD if multiple is present in the SSCD,
    b. authenticate the signatory and determine its intent to sign,
    c. receive data to be signed or a unique representation thereof (DTBS/R),
    d. apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R;
7. present personal data of its holder to authorized terminals,
8. prove the identity as SSCD to external entities,
9. protect confidentiality and integrity of data sent to/from the TOE.

PWPW SmartApp-ID 5.0 (SIGN configuration) supports also following security protocols:

1. Password Authenticated Connection Establishment
    a. Generic Mapping,
    b. Chip Authentication Mapping (PACE-CAM),

2. Chip Authentication.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

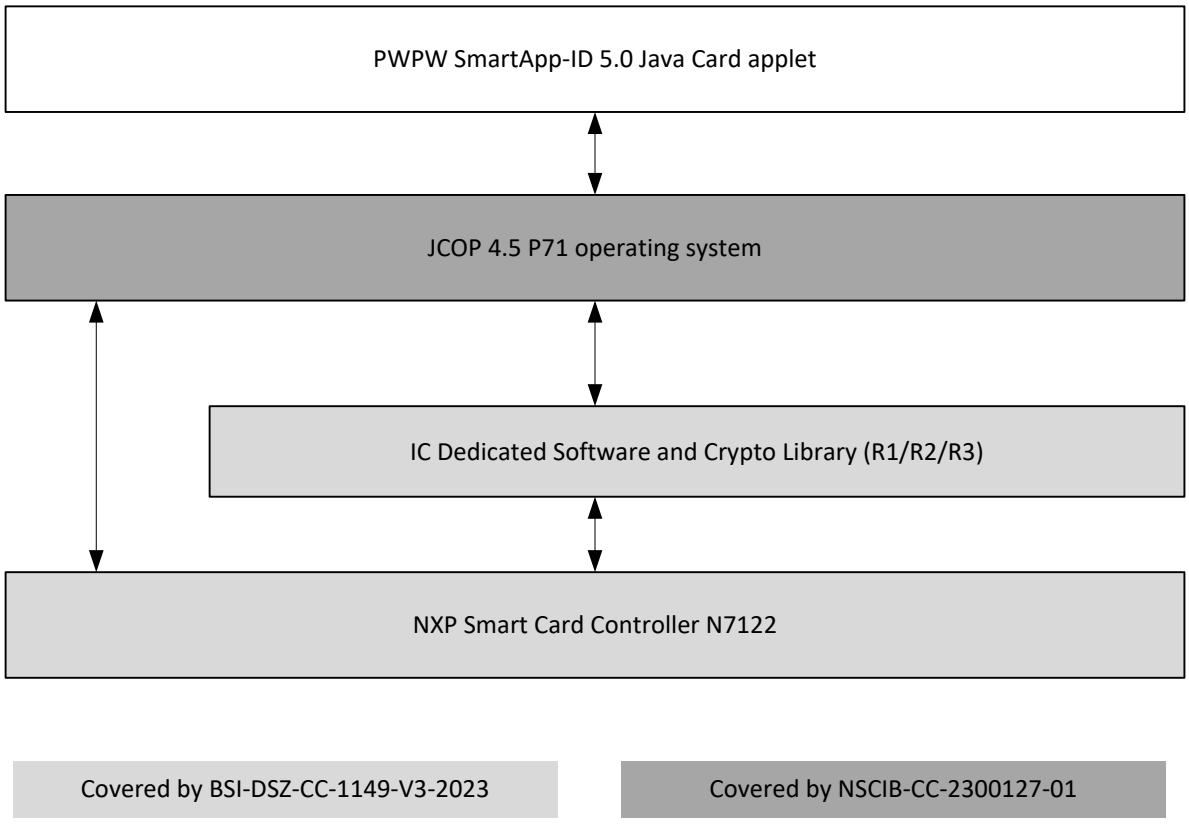
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]* or *[ST-Lite]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE architecture can be depicted as follows



The TOE is a composite product comprising the application implementing the security functionality of the TOE by relying of the underlying certified OS functionalities coming from the JCOP OS running on the HW IC. For each of the security functionalities, the application implements a subsystem with the according functionality. Those subsystems interact together to ensure the TOE functionality in terms of TOE architecture.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
PWPW SmartApp-ID 5.0 (SIGN configuration): Preparative procedures	5.0.5.0
PWPW SmartApp-ID 5.0 (SSCD configuration): Operational user guidance	5.0.4.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created during vulnerability analysis, the evaluators derived the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment. While doing this, also the aspects of the security architecture were considered for penetration testing.

Source code reviews of the provided implementation representation accompanied the development of test cases were used to find input for testing. The code inspection also supported the testing activities because it enabled the evaluator to verify implementation aspects that could hardly be covered by test cases.

The total test effort expended by the evaluators was 22 days. During that test campaign, 30% of the total time was spent on Perturbation attacks, and 70% on logical tests.

2.6.3 Test configuration

The following configuration was used for testing:

- PWPW SmartApp-ID 5.0 (SIGN configuration)

There is only one configuration of the TOE.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number PWPW SmartApp-ID 5.0 (SIGN configuration).

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the PWPW SmartApp-ID 5.0 (SIGN configuration), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ’strict’ conformance to the Protection Profile *[EN419211-2]*, *[EN419211-3]* *[EN419211-4]*, *[EN419211-5]* and *[EN419211-6]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The PWPW SmartApp-ID 5.0 (SIGN configuration) Security Target, Version 5.0.7.0, Dated 22 May 2024 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

DCAP	eIDAS Dutch Conformity Assessment Process
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SCD	Signature Creation Device
SVD	Signature Verification Device
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[HW-CERT]	Certification Report BSI-DSZ-CC-1149-V3-2023 for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 1.0, 13 December 2023
[HW-ETRfC]	Evaluation Technical report for Composite Evaluation (ETR COMP) for NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Version 2, 1 December 2023
[HW-ST]	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3 Security Target Lite, version 1.8, dated 1 December 2023
[PLAT-CERT]	Certification Report JCOP 4.5 P71, NSCIB-CC-2300127-01-CR, version 1, dated 16 January 2024
[PLAT-ETRfC]	Evaluation Technical Report for Composition “NXP JCOP 4.5 P71” – EAL6+, 23-RPT-1350, version 2.0, Dated 20 December 2023
[PLAT-ST]	JCOP 4.5 P71 Security Target Lite, Rev 2.6, Dated 11 December 2023
[eIDAS-REP]	Annex E of [ETR]
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02.
[EN419211-3]	EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01
[EN 419211-4]	EN 419211-4:2013: Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application; BSI-CC-PP-0071-2012-MA-01
[EN419211-5]	EN 419 211-5:2013, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01
[EN419211-6]	EN 419211-6:2014: Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application; BSI-CC-PP-0076-2013-MA-01
[ETR]	EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY) 8120833745 / NSCIB-2300120-01, Version 4, Dated 18 March 2025

[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2024 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	PWPW SmartApp-ID 5.0 (SIGN configuration) Security Target, Version 5.0.7.0, Dated 22 May 2024
[ST-lite]	PWPW SmartApp-ID 5.0 (SIGN configuration) Security Target Lite, Version 5.0.1.0, Dated 05 November 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)