Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0694-2012

for

SmartApp SIGN 2.2

from

Polska Wytwórnia Papierów Wartościowych S.A.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0694-2012

SmartApp SIGN 2.2

from	Polska Wytwórnia Papierów Wartościowych S.A.
PP Conformance:	Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 6 February 2012

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp.E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

This evaluation contains the components ALC_DVS.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SmartApp SIGN 2.2 has undergone the certification procedure at BSI.

The evaluation of the product SmartApp SIGN 2.2 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21. December 2011 The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the developer, sponsor and applicant is: Polska Wytwórnia Papierów Wartościowych S.A..

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

[6] Information Technology Security Evaluation Facility

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5 Publication

The product SmartApp SIGN 2.2 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Polska Wytwórnia Papierów Wartościowych S.A.
ul. R. Sanguszki 1
00-222 Warszawa
Poland

This page is intentionally left blank

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the SmartApp SIGN 2.2. It is a smartcard product implementing a secure signature creation device as described in [7] that can generate a signing key (signature creation data, SCD) and operates to create electronic signatures with the generated key. SmartApp SIGN 2.2 extends the scope of the protection profile [7] by a trusted channel secure communication with a signature creation application and a certificate generation application.

The PWPW (short for the company name Polska Wytwórnia Papierów Wartościowych S.A.) SmartApp SIGN 2.2 comprises of the platform (NXP J2A080 v2.4.1 Revision 3), which consist of the integrated circuit (NXP P5CC080 V0B), the operating system (JCOP 2.4.1 Revision 3) and the cryptographic library (V2.6), the applet containing the SSCD functionality (SmartApp SIGN 2.2), and the associated guidance documentation [9] and [10].

The main functionalities of SmartApp SIGN 2.2 cover following areas:

- cryptographic key generation and secure management;
- secure signature generation with secure management of data to be signed;
- identification and authentication of trusted users and applications;
- data storage and protection from modification or disclosures, as needed;
- secure exchange of sensitive data between the TOE and a trusted application;
- secure exchange of sensitive data between the TOE and a trusted human interface device.

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the appropriate policies considering the life cycle state, user role and security state.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionalities:

TOE Security Functionality	Addressed issue
SF.ACCESS	Access control/Storage and protection of data; Security and life cycle management
SF.CRYPTO	Cryptographic functions support
SF.TRUST	PACE protocol, Secure messaging

TOE Security Functionality	Addressed issue
SF.USER	Identification and Authentication mechanisms
SF.RANDOM	Random number generation
SF.PROTECTION	Protection against interference, logical tampering and bypass

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

The TOE is delivered in one configuration, consisting of:

- platform (NXP J2A080 v2.4.1 Revision 3), that is the integrated circuit (NXP P5CC080 V0B), the operating system (JCOP 2.4.1 Revision 3) and the cryptographic library (V2.6);
- applet containing the SSCD functionality (SmartApp SIGN 2.2);
- guidance documentation [9] and [10].

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

SmartApp SIGN 2.2,

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	integrated circuit (in the form of module) with the embedded operating system and SmartApp SIGN 2.2 applet	2.2.1.0	Secure physical delivery.
2	DOC	Guidances Operational user guidance [10]	2.2.16.0	Secure electronic delivery.
3	DOC	Guidances Preparative Procedures [9]	2.2.13.0	Secure electronic delivery.

No	Type	Identifier	Release	Form of Delivery
4	KEYS	Transport key – this key allows to access most parts of the EEPROM (including JCRE configuration area) to preconfigure the card, Verification key – this key allows to verify authenticity of the IC via internal JCOP authentication mechanism	n/a	Secure electronic delivery.

Table 2: Deliverables of the TOE

The unique TOE identification process is described in [10], chapter 6.1, and [9], chapter 6.1.2 and can be verified using the GET DATA: GET INFO command with the parameters according to the aforementioned references.

The response data field of this command will be: ’02 02 01 00’ which is applet version 2.2.1.0.

The TOE is delivered to a SSCD provisioning services between initialisation (SSCD production) and personalisation (SSCD preparation) as illustrated in Figure 1.3 of the Security Target [6].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It is defined according to the “Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009” by the Security Objectives and Requirements for the Secure Signature Creation Device (SSCD) based on the requirements and recommendations in this Protection Profile and extended with a signature creation application and a certificate generation application according the the Security Target [6].

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.SVD_Auth: Authenticity of the SVD
- OE.CGA_QCert: Generation of qualified certificates
- OE.SSCD_Prov_Service Authentic: SSCD provided by SSCD Provisioning Service
- OE.HID_VAD: Protection of the VAD
- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.DTBS_Protect: SCA protects the data intended to be signed
- OE.Signatory: Security obligation of the Signatory
- OE.CGA_SSCD_Auth: Preinitialisation of the TOE for SSCD authentication
- OE.CGA_TC_SVD_Imp: CGA trusted channel for SVD import

- OE.HID_TC_VAD_Exp: Trusted channel of HID for VAD export
- OE.SCA_TC_DTBS_Exp: Trusted channel of SCA for DTBS export

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The following subsystems can be distinguished inside the applet. The list contains basic responsibilities of each subsystem:

- SUB.Access – initializing the TOE, receiving user requests, verification of access conditions, triggering actions of other subsystems, sending responses to the user;
- SUB.Const – storing global data defined by the developer;
- SUB.Files – managing transparent files, their parameters and contents;
- SUB.Trust – establishment and usage of trusted path and trusted channel;
- SUB.Crypto – managing SCD/SVD and security attributes, generating digital signature of DTBS representation;
- SUB.User – authentication of Signatory and Administrator, managing RAD;
- SUB.Random – generating random challenge values.

The TOE subsystems are divided into two separate components. SmartApp SIGN and SmartApp LIB. Interactions among TSF subsystems are limited to calls from SUB.Access to SmartApp LIB and responses to those calls. There are no interactions among subsystems grouped in the SmartApp LIB component. The only exception to this rule is SUB.Const, which stores global data defined by the developer and can be accessed in read-only mode by other subsystems.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

Developer Tests:

The TOE consists of the SmartApp SIGN 2.2 smartcard product implementing a secure signature creation device application installed on NXP J2A080 v2.4.1 Revision 3 chip platform. For communication with the TOE over the ISO 7816 interface a SCM Microsystems SDI010 reader was used for the tests. The developer used a self-developed script application for implementing all tests. With the application also test reports and test logs were created. A test run automatically compares expected and actual results. The test script application allows binding of dynamic libraries that provide specific functionality, e.g. cryptographic computations.

Testing was performed on the final TOE, consisting of the platform as specified and the SmartApp SIGN 2.2 application (JavaCard applet) accessed through a card reader.

The scenarios for performing the functional tests are structured by the main functionality of the TOE, divided into two main test campaigns, one called Core Functionality and the other Extended Functionality which is focused on secure messaging. The scenarios use so called test primitives which constitute the lowest test level although they may consist of several test steps. All test scenarios start with applet selection which means that testing of the functionality includes successful execution of all previously necessary and preparative steps. This also makes the tests easier to repeat.

Negative tests are also implemented for the whole functionality of the TOE. For some main functionalities separate scenarios for positive and negative tests were provided. Some parameter tests, e.g. CLA / INS parameter tests of APDU commands, were not performed for the whole set of used APDU commands but only representatively for some commands.

To run the test campaign the card was prepared as described in the guidance document [9]. The card preparation is implemented as a script by the developer and can be run by the test script application. The card preparation contains some platform-related configuration settings and the applet instance creation with some functionality related configuration settings. The test files are contained in two directories according to the two campaigns. All keys and further data used in the tests are either loaded by plug-ins and pre-configured or are implemented directly in the test scripts. All test items have unique identifiers. The purpose of each test is also reproduced in the resulting test reports. The test reports include details and comments of the used command structure and the expected results. The test prerequisites, test steps, and expected results adequately test each TSFI, and they are consistent with the descriptions of the TSFI in the functional specification. The test plan includes all the details about the set-up procedures, input parameters, the privileges to run, the test procedure and information about the execution of the tests. They are suitable to test the TSF portion mediated by the related interface adequately.

The interfaces are represented by and correspond to TSFI, i.e. APDU commands. All TSF subsystems and SFR-enforcing module behaviour is covered by the tests. All TSFI are present and mapped to tests. The actual test results correspond to the expected test results. The TOE has passed all tests so that all TSF have been successfully tested. The developer’s testing results demonstrate that the TSF perform as specified.

Independent Testing according to ATE_IND:

The TOE consists of the SmartApp SIGN application installed on NXP J2A080 Secure Smart Card Controller, Revision 3. The APDU tests were performed using a card reader, a standard PC, test software provided by the developer as well as evaluator’s test software. The LFI tests were performed using Card Reader, Oscilloscope, Delay Generator, probe-station, Motor Control Unit, Laser, microscope.

The selected tests cover tests of the TSFI related to

- Manufacturing (applet loading, installing and selection)
- Identification and Authentication (interfaces of different authentication mechanisms),
- Protection against interference, logical tampering and bypass (disturbance of interface execution),
- Secure Messaging (test of interface commands using secure messaging)
- Preparative procedures, performed by the evaluator according to the guidance [9]

The choice of the subset of interfaces used for testing has been done according to the following approach:

- Augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces are both used for setting up test cases
- Besides augmentation and supplementation of developer’s tests the tests are also selected by the complexity and the susceptibility to vulnerabilities of interfaces and related functionality.
- The APDU interfaces are essential for the TOE and therefore in the focus of testing.

All TOE security functionality is included within the subset of tests. All cryptographic functionality was provided by the platform and sufficiently tested during platform evaluation. The TOE was tested with core and with extended functionality. The cryptographic keys and personalization data used in the test configurations were in general the same for all functional tests.

The test reports for the APDU tests are automatically generated by the test tool used. The test logs and the test documentation include details and comments on the test configuration, on the test equipment used, on the used command structure and the expected results. The test prerequisites, test steps, and expected results adequately test the related TSFI, and they are consistent with the descriptions of the TSFI in the functional specification.

The test results have not shown any deviations between the expected test results and the actual test results.

Penetration Testing:

The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the ITSEF.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential High was actually successful.

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised attack scenarios for penetration tests. In addition. the evaluators performed applet code review to verify the implementation of the requirements of the platform's ETR for composition and guidance as well as of the security mechanisms of the applet in general. The results of these activities led to confidence in the security of the TOE as a whole.

- pertubation attacks, i.e. program flow disturbance and authentication bypass;
- bypass authentication or access control;
- reaching limits of resources or maximum values of parameters.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE’s operational environment as defined in [6] provided that all measures required by the developer are applied.

8 Evaluated Configuration

The TOE is delivered in one configuration, consisting of:

- platform (NXP J2A080 v2.4.1 Revision 3), that is the integrated circuit (NXP P5CC080 V0B), the operating system (JCOP 2.4.1 Revision 3) and the cryptographic library (V2.6);
- applet containing the SSCD functionality (SmartApp SIGN 2.2);
- guidance documentation [9] and [10].

The unique TOE identification process is described in [10], chapter 6.1, and [9], chapter 6.1.2 and can be verified using the GET DATA: GET INFO command with the parameters according to the aforementioned references.

The response data field of this command will be: ’02 02 01 00’ which is applet version 2.2.1.0.

The TOE is delivered to a SCSD provisioning services between initialisation (SSCD production) and personalisation (SSCD preparation) as illustrated in Figure 1.3 of the Security Target [6].

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- Application of Attack Potential to Smart Cards
- Functionality classes and evaluation methodology for deterministic random number generators (for JCOP)
- Functionality classes and evaluation methodology for physical random number generators (for the hardware platform)
- Composite product evaluation for Smart Cards and similar devices. According to this concept the relevant documents ETR for Composition from the platform evaluations (i.e. on hardware, crypto library and JCOP) have been provided to the composite evaluator and used for the TOE evaluation.

(see [4], AIS 20, AIS 25, AIS 26, AIS 31, AIS 34, AIS 35, AIS 36, AIS 38 were used)

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009 [7]
- for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 extended
EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for the TOE Security Functionality SF.CF and is detailed in the following table.

The table lists the cryptographic algorithms that are used by the TOE to enforce its security policy.

Algorithm	Bit Length	Purpose	Security Function	Standard of Implementation	Standard of Application
3DES (112 and 168 bit keys) for en-/decryption (CBC and ECB) and MAC generation and verification (Retail-MAC and CBCMAC)	112 and 168	Used by the TOE for: PACE protocol encryption/decryption, MAC calculation, administrator authentication.	SF.CRYPTO	ISO 11568-2	ICAO Technical Report: Machine Readable Travel Documents – Supplemental Access Control for Machine Readable Travel Documents; Version 1.01; November 11, 2010
RSA CRT	2048	Signature generation and verification	SF.CRYPTO	PKCS#1, v1.5	-
RSA CRT Key Generation	0	Key Generation	SF.CRYPTO	-	-
ECDSA	256	Signature generation and verification	SF.CRYPTO	ANSI_X.9.62	-

Algorithm	Bit Length	Purpose	Security Function	Standard of Implementation	Standard of Application
ECDSA Key Generation	256	Key Generation	SF.CRYPTO	ISO_15946-1	-
ECDH Key Agreement Algorithm over GF(p)	256	Key generation/Key derivation	SF.CRYPTO	ISO 11770-3	-
SHA-1	-	Key derivation	SF.CRYPTO	FIPS_180-1	ICAO Technical Report: Machine Readable Travel Documents – Supplementa l Access Control for Machine Readable Travel Documents; Version 1.01; November 11, 2010

Table 3: Cryptographic Algorithms used by the TOE

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionalites it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The Cryptographic Functionality 2-key Triple DES (2TDES) and SHA-1 provided by the TOE achieves a security level of maximum 80 Bits (in general context).

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 limited validity for the usage of cryptograhic algortithms has to be considered by the user and his system risk management process.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

3DES	Symmetric block cipher algorithm based on the DES
AIS	Application Notes and Interpretations of the Scheme
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CRT	Chinese Remainder Theorem
EAL	Evaluation Assurance Level
EBC	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithmus
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organisation
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PACE	Password Authenticated Connection Establishment
PKCS	Public-key cryptography standards
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithmus
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSCD	Secure Signature Creation Device
ST	Security Target
TOE	Target of Evaluation

TSF	TOE Security Functionalities
TSFI	TSF Interface

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0694-2012, Version 2.2.18.0, Date 19.12.2011, Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)

[7] Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009

[8] Evaluation Technical Report, Version 3, Date 18.01.2012, SmartApp SIGN 2.2 of Polska Wytwórnia Papierów Wartościowych S.A.., TÜV Informationstechnik GmbH, (confidential document)

[9] SmartApp SIGN 2.2, Preparative Procedures, Version 2.2.13.0, Date 19.12.2011, Polska Wytwórnia Papierów Wartościowych S.A..

[10] SmartApp SIGN 2.2, Operational user guidance, Version 2.2.16.0 Date: 07.09.2011, Polska Wytwórnia Papierów Wartościowych S.A..

[8] specifically

- AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Reuse of evaluation results

This page is intentionally left blank

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	**Assurance Components**
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	**Assurance Components**
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development
and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0694-2012

Evaluation results regarding development and production environment

The IT product SmartApp SIGN 2.2 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 22.12.2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Polska Wytwórnia Papierów Wartościowych S.A., ul. R. Sanguszki 1, 00-222 Warszawa, Poland (development, manufacturing, initialisation)

For development and production sites regarding the platforms please refer to the certification reports BSI-DSZ-CC-0410-2007-MA-07, BSI-DSZ-CC-0709-2010 and BSI-DSZ-CC-0674-2010.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.