Certification Report

Evaluation of the Smart Card Security User Group Smart Card Protection Profile

Version 3.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-6-2
Version: 1.0
Date: 1 October 2001
Pagination: i to iv, 1 to 6

DISCLAIMER

The protection profile identified in this certificate has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO 15408). This certificate applies only to the specific version of the protection profile listed in this certificate and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme 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 protection profile by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the profile by CSE or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS) provides a third-party evaluation service for determining the trustworthiness of information technology (IT) security products. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Canadian CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the ISO Guide 17025, *General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN) administered by the Standards Council of Canada.

By awarding a certificate, a certifying body asserts that a protection profile complies with the requirements for protection profile (PP) evaluation specified in the Common Criteria for Information Security Evaluation. A protection profile is an implementation-independent set of security requirements for a category of IT that meets specific consumer needs. The objective of a protection profile evaluation is to ensure that the protection profile is complete, consistent, technically sound and, therefore, suitable for use as the basis of security requirements for the relevant category of IT.

The protection profile associated with this certification report is identified by the following nomenclature:

Smart Card Security User Group
Smart Card Protection Profile
Version 3.0
9 September 2001

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP), version 3.0, developed by the Smart Card Security User Group (SCSUG) describes the information technology (IT) security requirements for a smart card to be used in connection with sensitive applications, such as banking industry financial payment systems. The SCSUG-SCPP was evaluated against the APE class of assurance requirements specified in the Common Criteria (CC).

The evaluation has determined that the SCSUG-SCPP is a well-written, mature document, which clearly defines the intended target of evaluation (TOE), and its intended operating environment. It meets all of the CC requirements specified for protection profile evaluation. The SCSUG-SCPP is CC Part 2 extended (containing a security functional requirement not included in CC Part 2). The SCSUG-SCPP is CC Part 3 conformant, with assurance requirements comprising Evaluation Assurance Level 4 (EAL4), augmented by additional requirements for:

- resistance to attackers possessing a moderate attack potential, and
- modularity in the design of the TOE.

The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS). The Canadian CCS has established a Certification Body (CB) that is managed by the Communications Security Establishment (CSE). The evaluation was performed using the Common Criteria for Information Technology Security Evaluation (CC) [1], and the Common Methodology for Information Technology Security Evaluation (CEM) [2][3].

The Common Criteria Evaluation Facility (CCEF) that conducted the evaluation of the SCSUG-SCPP is CGI Information Systems and Management Consultants Inc., located in Ottawa, Canada. The evaluation process began in September 2000, with version 2.0, and culminated with the successful evaluation of version 3.0. For versions 2.0 and 2.1d, all evaluation activities were performed by the CCEF, in accordance with the CEM. Subsequent versions, including version 3.0, were evaluated by the Canadian CCS CB in collaboration with an international working group, charged with ratifying common concerns with version 2.1d of the SCSUG-SCPP.

Recommendations are provided in this report for those wishing to use or claim conformance to SCSUG-SCPP.

1 Identification

1.1 Protection profile

The evaluated protection profile, the subject of this certification report, is identified by the following nomenclature:

Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP)
Version 3.0
9 September 2001

1.2 Protection profile developer

The Smart Card Security User Group (SCSUG) developed the protection profile. The members of the SCSUG at the time of the drafting of the protection profile included:

American Express;
Europay International;
JCB Co Ltd;
MasterCard International;
Mondex International;
Visa International;
National Institute of Standards and Technology (United States of America);
National Security Agency (United States of America).

1.3 Evaluation sponsor

The sponsor of the evaluation was:

American Express
210 North 2100 West
Salt Lake City, UT 84116
United States of America

1.4 Evaluator

The Common Criteria Evaluation Facility (CCEF) that conducted the evaluation is CGI Information Systems and Management Consultants Inc., located in Ottawa, Canada.

2 Results of the evaluation

The SCSUG-SCPP was successfully evaluated against the requirements of the Protection Profile Evaluation (APE) class of Common Criteria assurance requirements. This means that the PP is technically sound and suitable for use as a statement of security requirements for smart card evaluation.

The protection profile was found to be a well-written, mature document that clearly defines the intended target of evaluation (TOE). It is comprehensive in its description of the environment in which the intended TOE would operate and the anticipated threats it would face.

3 Evaluation activities

The evaluation involved an analysis of the SCSUG-SCPP against the requirements of the APE class of Common Criteria assurance requirements. The objective of protection profile evaluation is to determine, by analysis, that the specified security requirements are effective at solving the security problem defined for the environment in terms of threats, policies and assumptions. The approach to analysis is pair-wise, whereby the stated security objectives are verified to be effective against the security problem, and the security requirements verified to satisfy the security objectives. Finally, the security requirements are analyzed to determine that they are mutually supportive and cohesive.

The evaluation of the SCSUG-SCPP was an iterative process, whereby observations discovered during evaluation resulted in a revision of the SCSUG-SCPP and its subsequent re-evaluation. The evaluation process began in September 2000, with version 2.0 and culminated with the successful evaluation of version 3.0. For versions 2.0 and 2.1d, all evaluation activities were performed by the CCEF, in accordance with the Common Methodology for Information Technology Security Evaluation [2][3]. The subsequent versions, including version 3.0, were evaluated by the Canadian CCS CB in collaboration with an international working group, charged with ratifying common concerns with version 2.1d of the SCSUG-SCPP. The process involved assessing the impact of changes between versions with the aim of reusing previous evaluation results where feasible.

4 Using the protection profile

The protection profile has been developed with the following assumptions made regarding its use:

1. The SCSUG-SCPP describes the information technology (IT) security requirements for a smart card to be used in connection with sensitive applications, such as banking industry financial payment systems, for which the required assurance is commensurate with the EAL4 augmented assurance package specified therein.

2. The SCSUG-SCPP is intended to be applied to an integrated product produced by potentially different manufacturers and developers. However, users may find the provision for requirement packages described in the protection profile to be helpful. Using requirement packages, components of the overall smart card system could individually be evaluated in a manner that would be directly supportive of the final evaluation of the integrated system. Annex D of the SCSUG-SCPP describes the potential use of packages, as well as the limitations related to protection profile compliance claims.

3. As permitted by the Common Criteria, only some functional requirement operations have been completed. The completion of all operations would have imposed unnecessary restrictions on product implementation. Annex C, section C.2.2 of the SCSUG-SCPP, provides a list of the requirements that have uncompleted assignment or selection operations, as defined in Part 1, section 2.3, of the Common Criteria [1]. These requirement operations will need to be completed when instantiating security targets that claim conformance to the SCSUG-SCPP.

5 Comments, observations and recommendations

5.1 EAL4 augmented

The Arrangement on the Recognition of Common Criteria Certificates (CCRA) provides for the recognition of certificates awarded by any participating Common Criteria scheme by all other participating schemes. The current scope of the CCRA is limited to Common Criteria assurance requirements for EAL4 and below. By specifying an EAL4 augmented assurance requirements package, the evaluation results for products certified to meet the SCSUG-SCPP may not be mutually recognized under the current CCRA. This does not suggest that the assurance requirements package specified in the SCSUG-SCPP is invalid, only that it is outside of the current scope of the CCRA.

5.2 Explicitly stated security requirements

The SCSUG-SCPP uses the explicitly stated security functional requirement FAU_LST.1 (Audit list generation) in place of FAU_GEN.1 (Audit data generation) and its dependency on FPT_STM.1 (Reliable time stamps). The reason for using an explicitly stated requirement in lieu of the ones provided by the Common Criteria is due to the nature of smart cards. Since smart cards have no internal power source, there is no way to provide reliable timestamps necessary to meet the requirement of FPT_STM.1. The time stamp is a key component of the information required by FAU_GEN.1. The extended requirement FAU_LST.1 restructures the audit event information and uses the sequence of operations for events, instead of time stamps, that is consistent with best practices for smart card audit records.

6 Claiming conformance to protection profiles

One of the benefits of claiming conformance to an evaluated protection profile is the reuse of protection profile evaluation results for a security target evaluation. The following guidelines and restrictions apply when claiming conformance to a protection profile and reusing the protection profile evaluation results.

1. A security target cannot claim conformance to a protection profile if it implements a subset of the security requirements, either functional or assurance, specified in the protection profile. A security target may, however, implement a superset of the security requirements specified in a protection profile and claim conformance to that protection profile. A security target may also claim conformance to multiple protection profiles. Security targets that implement a superset of protection profile security requirements, or that claim conformance to more than one protection profile, must by evaluated to determined that the security requirements remain mutually supportive.

2. A security target which claims conformance to a protection profile, but contains a superset of the security requirements, must clearly identify the additional requirements as well as any additional security objectives, threats, organizational security policies and assumptions.

3. A protection profile to which conformance is claimed may contain uncompleted security requirement operations. A security target claiming conformance to such a protection profile must complete all operations.

7 Abbreviations and acronyms

CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories Canada
PP	Protection Profile
SC	Smart Card
SCPP	Smart Card Protection Profile
SCSUG	Smart Card Security User Group
ST	Security Target
TOE	Target of Evaluation

8 References and bibliography

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

1. Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.
2. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, 11 January 1997.
3. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation methodology, Version 1.0, August 1999.
4. Evaluation Technical Report for Smart Card Security User Group Protection Profile (Version 2.0), CGI-ITSETF-00-ETR-01, 27 October 2000.
5. Evaluation Technical Report for Smart Card Security User Group Protection Profile (Version 2.1d), CGI-ITSETF-01-ETR-01, 22 May 2001.
6. Final Report, Executive Subcommittee Ad Hoc Working Group, 7 September 2001.
7. Letter to SCSUG Chairman, SCSUG SC Protection Profile, 25 June 2001.
8. Preliminary Certification Report for Smart Card Security User Group Protection Profile (Version 2.0), CGI-ITSETF-00-PCR-01, 31 October 2000.
9. Preliminary Report, Executive Subcommittee Ad Hoc Working Group, 29 June 2001.
10. Smart Card Security User Group, Smart Card Protection Profile, Draft, Draft Version 2.0, 1 May 2000.
11. Smart Card Security User Group, Smart Card Protection Profile, Draft, Draft Version 2.1d, 21 March 2001.
12. Smart Card Security User Group, Smart Card Protection Profile, Draft, Draft Version 2.2, 3 July 2001.
13. Smart Card Security User Group, Smart Card Protection Profile, Draft, Draft Version 2.3, 4 August 2001.
14. Smart Card Security User Group, Smart Card Protection Profile, Draft, Draft Version 2.4, 21 August 2001.
15. Smart Card Security User Group, Smart Card Protection Profile, Version 3.0, 9 September 2001.
16. Technical Oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), CCS#4, Version 0.84 - Draft.