National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Smart Card Security User Group (SCSUG)
Smart Card Protection Profile (SCPP), Version 3.0

Report Number:	**CCEVS-VR-01-0007**
Dated:	**October 22, 2001**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

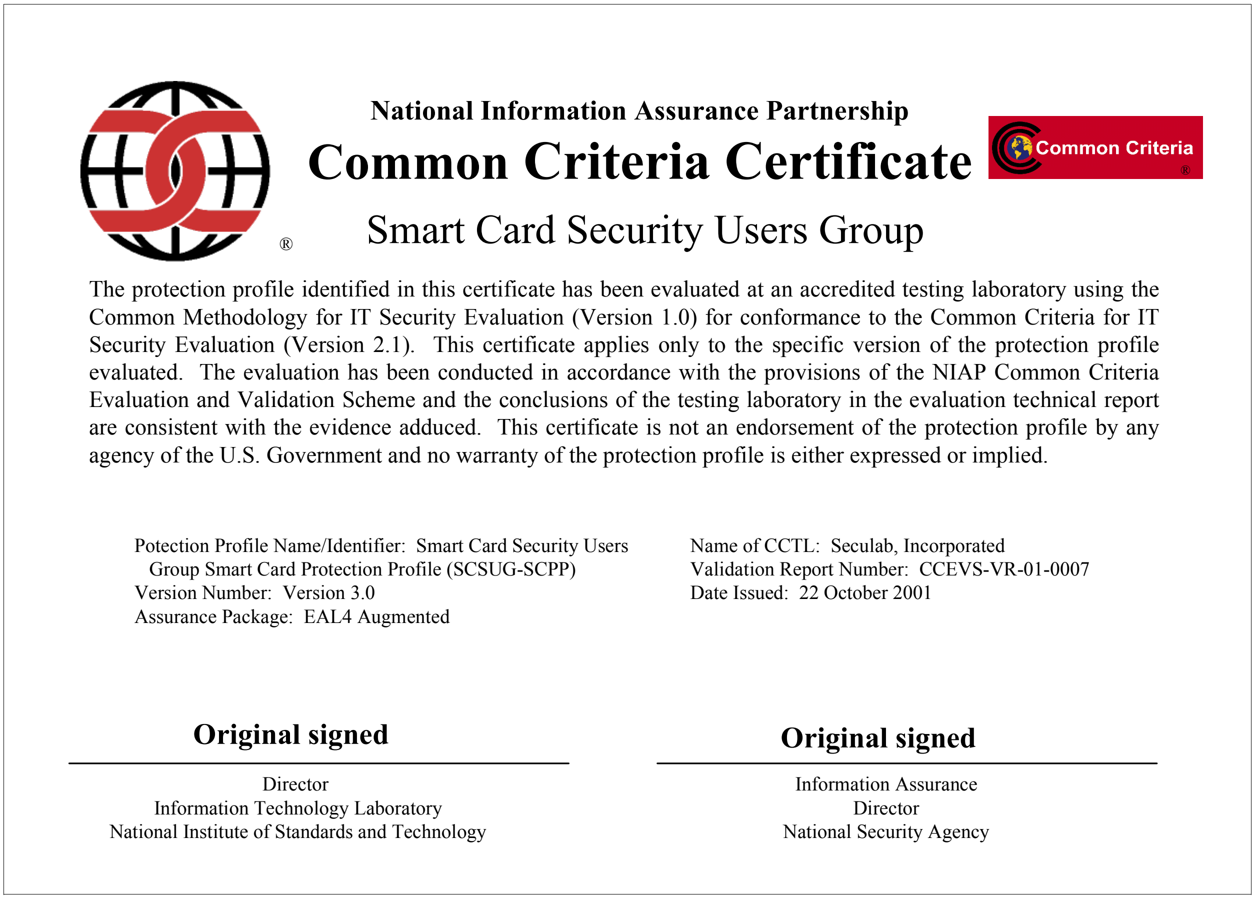
ACKNOWLEDGEMENTS

Validation Team

Daniel P. Faigin
The Aerospace Corporation, El Segundo, California

Common Criteria Testing Laboratory

Seculab, Inc.
Austin, Texas



National Information Assurance Partnership

Common Criteria Certificate

Smart Card Security Users Group

The protection profile identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version of the protection profile evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.

Potection Profile Name/Identifier: Smart Card Security Users Group Smart Card Protection Profile (SCSUG-SCPP)
Version Number: Version 3.0
Assurance Package: EAL4 Augmented

Name of CCTL: Seculab, Incorporated
Validation Report Number: CCEVS-VR-01-0007
Date Issued: 22 October 2001

Original signed

Director
Information Technology Laboratory
National Institute of Standards and Technology

Original signed

Information Assurance
Director
National Security Agency

Table of Contents

This page intentionally left devoid of useful information.

Executive Summary

An evaluation of the Smart Card User's Group Smart Card Protection Profile (SCSUG-SCPP), v3.0, was begun in February 2001 and concluded in October 2001. The evaluation was performed by the Seculab Inc. Common Criteria Testing Laboratory (CCTL) in the United States, in accordance with the requirements drawn from the *Common Criteria for Information Technology Security Evaluation* (CC) [CC], Version 2.1, Part 3, Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the SCPP contains requirements that are:

- Justifiably included to counter stated threats and meet realistic security objectives
- Internally consistent and coherent
- Technically sound

Seculab, Inc. is certified by the NIAP Validation Body for laboratory accreditation. The CCTL has presented work units and rationale that are consistent with the CC, the *Common Methodology for Information Technology Security Evaluation* (CEM) [CEM], and CCEVS Publication Number 4, *Guidance to CCEVS Approved Common Criteria Testing Laboratories* [CCEVS4]. The CCTL team concluded that the requirements of the APE class have been met, and have issued a **pass** verdict for the Protection Profile.

The validation team followed the procedures outlined in the CCEVS Publication Number 3, *Guidance to Validators of IT Security Evaluations* [CCEVS3]. The validation team has observed that the evaluation and all of its activities were in accordance with the CC, the CEM, and the CCEVS. The validation team therefore concludes that the evaluation and its results of **pass** should be approved and accepted by the CCEVS.

Note: The purpose of this report is to document the results of the SCSUG-SCPP evaluation. This report is not an endorsement of the IT product (or PP) by any agency of the U.S. Government and no warranty of the IT product (or PP) is either expressed or implied.

This page intentionally left devoid of useful information.

1 Introduction

1.1 Report Purpose

The Common Criteria Evaluation and Validation Scheme is charged with ensuring the proper evaluation of products (i.e., Protection Profiles and Security Targets/Targets of Evaluation) by the U.S. National Information Assurance Partnership. This process has a number of distinct roles:

- A *sponsor* of an evaluation (e.g., a vendor of a product or a protection profile developer) interested in obtaining a Common Criteria evaluation makes arrangements to have their product evaluated by a Common Criteria Testing Laboratory (CCTL).
- A *Common Criteria Testing Laboratory* conducts the evaluation, following the methodology established in the CEM [CEM] and the requirements established by the scheme. The basis for the evaluation is the Protection Profile (PP) or Security Target (ST), the Target of Evaluation (if applicable), and any evidence provided by the sponsor.
- A *Validation Team*, selected by CCEVS, provides process oversight for the evaluation, ensuring that the evaluation is performed in accordance with the CEM and CCEVS requirements, and providing a liaison for resolution of evaluation issues.

This report documents the findings of the validation team. It should be read in conjuction with the Evaluation Technical Report (ETR) prepared by the CCTL [ETR] and the evaluated Protection Profile [SCPP].

Note: The purpose of this report is to document the results of the SCSUG-SCPP evaluation. This report is not an endorsement of the IT product (or PP) by any agency of the U.S. Government and no warranty of the IT product (or PP) is either expressed or implied.

1.2 Protection Profile Identification

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

1.3 Evaluation Specific Details

Dates of Evaluation:	February 2001 – October 2001
Evaluated Product:	Smart Card Security Users Group Smart Card Protection Profile (SCSUG-SCPP), Version 3.0, 9 September 2001.
Developer:	Smart Card Security Users Group
CCTL:	Seculab, Inc.
Evaluation Class:	EAL4 Augmented
Validation Team:	Daniel P. Faigin, The Aerospace Corporation

2 Protection Profile Summary

2.1 Overview

[Note: This summary is adapted from text in the SCSUG-SCPP.]

The SCSUG-SCPP presents functional and assurance security requirements for a smart card to be used in connection with sensitive applications, such as banking industry financial payment systems. The term "smart card" refers to an integrated circuit containing a microprocessor, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier, typically the size of a common credit card. The integrated circuit is a single chip incorporating CPU and memory, which may include RAM, ROM, and/or programmable non-volatile memory. The carrier is typically made of plastic and usually conforms to ISO 7810 and 7813 - Identification Cards, but could be smaller. The chip is embedded in a module that provides the capability for standardized connection to systems separate from the chip (typically through contacts in accordance with ISO 7816-3 [ISO7816], or contactless in accordance with ISO 14443-4 [ISO14443]).

The SCSUG-SCPP addresses the smart card's integrated circuit and operating software, but does not include specific applications. The intent is that Application-specific PPs or security targets may use the SCSUG-SCPP as a foundation for further work.

The SCSUG-SCPP is applicable to both contact and contactless smart cards, without special regard for form factor or physical card security features. This PP does not cover card features such as printing, the magnetic stripe (if present), security features such as holograms, or any other part of the card. It also does not cover security requirements for card acceptor devices (CADs) or networks interfacing with them.

Targets of Evaluation (TOEs) that are compliant with the SCSUG-SCPP would be the smart card platform, consisting of the integrated circuit and operating software, including the mechanisms that allow communication with the outside world. There must be sufficient hardware and software elements to be capable of establishing a trusted channel to a trusted source for application loading or for other potentially privileged commands. The smart card must have the following features in order to support the intended functionality:

- *Cryptographic functions*, to support the establishment and control of a trusted channel.
- *Access control and information flow control capabilities*, to support approval and processing of requests to load or manipulate user and security function information.
- *Information processing and storage capability*, to allow execution of loaded commands.
- *Security related functions*, to maintain the confidentiality and integrity of specified user and security function data.
- *Identification and audit-like capability*, to support post processing security review.

2.2 Environment of Use

2.2.1 Assumptions About the Operating Environment

The Protection Profile makes the following assumptions about the operating environment:

A.CAD_SEC-COM A CAD to which the TOE establishes a secure link is assumed to be secure.

A.DATA_STORE Management of TOE data off of the TOE is assumed to be performed in a secure manner.

A.KEY_SUPP All imported cryptographic keys are assumed to be supported off-card in a secure manner.

A.PWR_CLOCK Power and clock come from the CAD.

A.ROLE_MAN Management of roles for the TOE is performed in a secure manner off-card.

2.2.2 Threats Addressed by the Operating Environment

The Protection Profile assumes that the environment addresses the following threats:

T.CARRIER_TAMPER An attacker may use a modified TOE in an original carrier to masquerade as an original TOE so that user data can be fraudulently accessed.

T.PRIV A careless, willfully negligent, or hostile administrator or other privileged user may create a compromise of user data or TSF data through execution of actions which expose the security functions or the protected data.

2.3 Threats Addressed by the Protection Profile

Products compliant with the SCSUG-SCPP are designed to address the following threats:

2.3.1 Threats Associated with Physical Attack on the TOE

T.P_PROBE An attacker may perform physical probing of the TOE to reveal design information and operational contents.

T.P_ALTER An attacker may perform physical alteration of the TOE in order to reveal operational contents or design information, or to change TOE Security Function (TSF) data or the TOE security functions so that the TOE can be used fraudulently.

2.3.2 Threats Associated with Logical Attack on the TOE

T.FLT_INS An attacker may determine user and TSF information through observation of the results of repetitive insertion of selected data.

T.FORCD_RST An attacker may corrupt TSF data through inappropriate termination of selected operations.

T.INV_INP An attacker may compromise the TSF data through introduction of invalid inputs.

T.REUSE An attacker may corrupt the TSF data through replaying authentication data that was once valid but is not presently valid.

T.BRUTE-FORCE An attacker may search the entire user-accessible data space to identify TSF data such as PINs.

T.UA_LOAD An attacker may utilize unauthorized programs to modify TSF data or the TOE Security Function code so that the TOE can be compromised.

2.3.3 Threats Associated with Control of Access

T.ACCESS A user or an attacker of the TOE may gain access to user or TSF data without having permission from the person who owns or is responsible for the information or resources.

T.FIRST_USE An attacker may gain access to user or TSF data by unauthorized use of a new, previously unissued TOE.

2.3.4 Threats Associated with Unanticipated Interactions

T.APP_FTN An attacker may exploit interactions between applications to expose sensitive TOE or user data.

T.LC_FTN An attacker may exploit commands, particularly test and debug commands, which were necessary for another part of the TOE life cycle but are not presently allowed, to expose TSF data or sensitive user data.

2.3.5 Threats Regarding Cryptographic Functions

T.CRYPT_ATK An attacker may defeat TOE Security Functions through a cryptographic attack against the algorithm or through a brute-force attack on the function inputs.

2.3.6 Threats That Monitor Information

T.I_LEAK An attacker may exploit TSF data which is leaked from the TOE during normal usage.

T.LINK An attacker may observe multiple uses of resources or services and, by linking these observations, deduce information that may reveal TSF data.

2.3.7 Miscellaneous Threats

T.ENV_STRS An attacker may induce errors in the TSF data through exposure of the TOE to environmental stress.

T.LNK_ATT An attacker may perform simultaneous attacks with the result that the TOE Security Functions become unstable or some part of the TSF data is degraded resulting in exposure of TSF data or sensitive user data.

T.CLON An attacker may utilize design information gained from inspection of the TOE to fabricate a clone to develop further attacks.

2.4 Organizational Security Policies addressed by the Protection Profile

The Protection Profile addresses the following organizational security policies. In the profile, these are expressed as abstractions of the actual policy, which is drawn from documents such as EMV '96 [EMV96].

P.AUDIT The TOE shall preserve information about selected security-relevant events.

P.CRYPT_STD Cryptographic entities, data authentication, and approval functions must be in accordance with ISO, associated industry, or organizational standards or requirements.

P.DATA_ACC Except for a well-defined set of allowed operations, the right to access specific data and data objects is determined on the basis of:

a) The attributes of the object

b) The attributes of the subject attempting the access

c) The implicit and explicit access rights to the object granted to the subject by the object attributes

This will be represented in a well-defined set of roles, including at least a "user" and "administrator". Other roles may be defined depending on the implementation of the TOE.

P.FILE_STR The right to establish files and the access control structure is determined on the basis of:

a) The attributes of the files

b) The attributes of the subject attempting to perform setup

c) The implicit and explicit access rights to the files granted to the subject by the file attributes

This will be represented in a well-defined set of roles, including at least a "user" and "administrator". Other roles may be defined depending on the implementation of the TOE.

P.IDENT The TOE must be capable of being uniquely identified.

P.SEC_COM Secure communication protocols and procedures shall be supported between the TOE and a trusted CAD.

2.5 Security Requirements of the Protection Profile

To address the identified threats and organizational policies, the Protection Profile provides both functional and assurance requirements.

Functional requirements are provided in the areas of:

- *Audit*. The SCSUG-SCPP does not include a requirement for a traditional audit trail, as smart cards are dependent on the CAD for timing and clock information. However, the SCSUG-SCPP does include a requirement for an audit list, which records, at minimum, the circuit manufacture date and serial number, together with the operating software version and release date. Audit requirements also address the need to monitor for potential security violations and to take appropriate actions when potential violations are detected. There are also requirements to protect the audit list, to provide actions when the audit list size maximum is reached, and to selectively record events in the audit list.

- *Cryptographic Mechanisms*. The SCSUG-SCPP has generic requirements in the areas of cryptographic key generation, access, and cryptographic operations. It does not mandate the use of particular cryptographic standards, as the appropriate standards vary depending on the organization utilizing compliant products.

- *User Data Protection*. The SCSUG-SCPP includes requirements for both access control and information flow, both of which are stated generically, allowing products to select appropriate policies based on the specific needs of the applications in the smart cards (see the comment in section 3.4.1, page 13). It also includes requirements related to export of data, internal transfer protection, residual information protection, and data exchange integrity.

- *Identification and Authentication*. The SCSUG-SCPP includes requirements for identification and authentication, including the handling of authentication failures. It does not mandate a particular authentication approach. Smart cards, in general, use a variety of authentication approaches, from Personal Identification Numbers to biometrics.

- *Management of the TSF*.The SCSUG-SCPP includes a large list of restricted management activities, as well as requirements for management of security attributes, TSF data, and rules related to the values assigned to attributes.

- *Protection of the TSF*. The SCSUG-SCPP does require the presence of a reference monitor and domain separation. It requires trusted recovery, resistance against physical attacks that include environmental stress and information monitoring, internal transfer protection, detection of modification of TSF data, replay protection, and the ability to perform self tests.

- *Trusted Path*. The SCSUG-SCPP requires the TSF to provide the ability to create a trusted channel between the smart card and a remote trusted information technology product.

Assurance is at EAL4, augmented with AVA_VLA.3 (Vulnerability Assessment) and ADV_INT.1 (Modularity). This is based on the likelihood that smart cards compliant with the profile will be used in financial systems, and thus may contain, represent, or provide monetary value. The smart cards will also be in the hands of untrusted users. EAL4, as augmented, provides what is claimed to be the highest level of commercially viable assurance.

3 Validation Results

3.1 Validation Process

The validation was conducted through interaction with the evaluation team, review of evaluation evidence produced by the evaluation team, selected validation of evaluation results, and a site visit to ensure that the evaluation facility was in compliance with its documented quality processes.

3.2 Evaluation Results

The CCTL conducted the evaluation in accordance with the CC and the CEM, and concluded that the requirements of the APE class were satisfied. They have issued a **pass** verdict.

3.3 Validation Results

The Validator has reviewed the results of the evaluation provided by the CCTL. Although there are some minor problems identified with the profile, the Validator does not believe these problems are significant. The evidence indicates that the CCTL conducted the evaluation and its activities in accordance with the CC, the CEM, and the requirements of the CCEVS. It also indicates that the CCTL has presented appropriate CEM work units and rationale. The Validator therefore concludes that the evaluation, and its results of **pass**, are complete, correct, and should be approved by CCEVS.

3.4 Validator Observations

The Validator remains concerned about a number of aspects of presentation of the Protection Profile. None of these concerns are significant enough to effect the validation results, or to indicate that a different conclusion with respect to either the evaluation or validation should be drawn. They are presented here to provide clarification to users of the profile, and to hopefully encourage the developers of the profile to improve the profile in subsequent versions.

Many of these concerns have been raised to the sponsoring organization. However, as this validation/evaluation is a coordinated effort amongst multiple schemes, time did not permit them to be addressed in this version of the SCSUG-SCPP.

3.4.1 Data Protection Policy Examples

The SCSUG-SCPP calls out use of access control and information flow policies in order to address the policy requirements related to protection of data. However, it provides no explicit guidance or examples on how these policies will be used. This is not a concern for the access control policy, which is typically understood to be a form of discretionary access control. It is more of a concern for the information flow policy, which is typically used for mandatory access controls.

At the lower levels of the functional component hierarchy, the access control and information flow requirements are very similar. In fact, the primary difference is that access control refers to control of access to *objects*, whereas information flow refers to control of access to *information*. Both base access control decisions on the attributes of the accessing subject. It is important to note that the lower levels of information flow do not mandate Mandatory Access Control, in the “label” sense. Indeed, a more typical usage in a smart card environment would relate to the use of Public-Key Certificates, where information in the certificate, such as expiration date would be used to control access to the contents of the certificate.

The protection profile would be improved if examples of the use of the data protection policies were provided as informative material. This would serve to provide guidance to Security Target authors as to how to complete the functional requirements. However, the lack of this material does not result in a failure, as it does not appear that the selected functional components could be completed in a way to prevent achievement of the PP's objectives. Note that the PP does make it clear that both access control and information flow policies are required.

3.4.2 Organizational Security Policies

The protection profile states its organization security policies without explicit reference to the actual EMV policies. Such an explicit reference is not required; the CCTL has confirmed that each policy can be traced to a published specification. However, the utility to the user would be enhanced if there was an explicit tracing of the stated organizational security policies backed to the published sponsor specifications.

3.4.3 Proofreading and Readability

The protection profile suffers from numerous small readability problems, primarily due to the style of writing. None of these are sufficient to make the document incomprehensible, especially for those intimately acquainted with the technology area. However, the language could probably be simplified, making the document more accessible to those less familiar with the technology.

There are also numerous minor typos and grammatical problems that could be corrected with a thorough proofreading pass. None of these are sufficiently significant as to warrant failure.

4 Acronyms

ADV_INT	(CC Class) Development→(CC Family) TSF Internals
APE	(CC Class) Protection Profile Evaluation
AVA_VLA	(CC Class) Vulnerability Assessment→(CC Family) Vulnerability Analysis
CAD	Card Accepting Device
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Methodology for Information Technology Security Evaluation
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
EMV	Europay, Mastercard, Visa
ETR	Evaluation Technical Report
ISO	International Organisation for Standardization
NIAP	National Information Assurance Partnership
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
SCPP	Smart Card Protection Profile
SCSUG	Smart Card Security User Group
SCSUG-SCPP	Smart Card Security Users Group Smart Card Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

5 References

[CEM] COMMON CRITERIA SPONSORING ORGANIZATIONS. *Common Methodology for Information Technology Security Evaluation*. Two parts:

- Part 1: Introduction and General Model. Version 0.6, January 1997 (draft)
- Part 2: Evaluation Methodology. Version 1.0, August 1999. CEM-99/045.

Available at http://csrc.nist.gov/cc/cem/cemlist.htm

[CC] COMMON CRITERIA SPONSORING ORGANIZATIONS. *Common Criteria for Information Technology Security Evaluation*, Version 2.1. August 1999. Three parts:

- Part 1: Introduction and General Model, CCIMB-99-031, ISO/IEC 15408-1
- Part 2: Security Functional Requirements, CCIMB-99-032, ISO/IEC 15408-2
- Part 3: Security Assurance Requirements, CCIMB-99-033, ISO/IEC 15408-3

Available at http://csrc.nist.gov/cc/ccv20/ccv2list.htm

[CCEVS3] COMMON CRITERIA EVALUATION AND VALIDATION SCHEME. *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Validators of IT Security Evaluations*, Draft Version 0.5, February 2001.

[CCEVS4] COMMON CRITERIA EVALUATION AND VALIDATION SCHEME. *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Common Criteria Testing Laboratories*, Draft Version 1.0, 20 March 2001. Available at http://niap.nist.gov/cc-scheme/DownloadSchemePub4.html

[EMV96] EMV (EUROPAY, MASTERCARD, VISA) CO. LLC. *Integrated Circuit Card Specifications.* Version 3.1.1. Available at http://www.emvco.com/specifications.cfm

[ETR] SECULAB, INC. *Evaluation Technical Report for a Protection Profile: Smart Card Security Users Group Smart Card Protection Profile, 9 September 2001, Version 3.0.* ETR Version 1.0, 18 October 2001. Available from Seculab, Inc., Austin, TX.

[ISO7816] INTERNATIONAL ORGANISATION FOR STANDARDIZATION. *Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 3: Electronic signals and transmission protocols*. ISO 7816-3. 2nd edition. 15 December 1997. May be ordered through http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm

[ISO14443] INTERNATIONAL ORGANISATION FOR STANDARDIZATION. *Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 4: Transmission protocol.* ISO 14443-4. 1st edition. 18 January 2001. May be ordered through http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm

[SCPP] SMART CARD SECURITY USERS GROUP. *Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP)*, Version 3.0, 9 September 2001. Available at http://csrc.nist.gov/cc/sc/Scsug.pdf