INTERNATIONAL STANDARD

ISO/IEC 25185-1

First edition
2016-01-15

Identification cards — Integrated circuit card authentication protocols —

Part 1: Protocol for Lightweight Authentication of Identity

Cartes d'identification — Integrated circuit protocoles d'authentification par carte —

Partie 1: Protocole pour l'authentification de l'identité léger

Reference number
ISO/IEC 25185-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*.

ISO/IEC 25185-1 was prepared by Standards Australia under the JTC1 Fast Track process from the existing AS-5185 Australian standard as a submission to ISO/IEC JTC 1, *Information technology*.

ISO/IEC 25185 consists of the following parts, under the general title *Identification cards — Integrated circuit card authentication protocols*:

— *Part 1: Protocol for Lightweight Authentication of Identity*

Introduction

PLAID (Protocol for Lightweight Authentication of IDentity) is an ICC (smartcard) authentication protocol, which is designed to expressly support contactless applications. The protocol is designed to fill the gap in standardized protocols between tag and RFID based technologies which do not utilize cryptography but are fast, and PKI based authentication, which can be very strong cryptographically, but slower, and unsuitable for many contactless use-cases.

It is based on a cryptographic method, which uses both symmetric and asymmetric cryptography in a hybrid protocol to protect the communications between ICCs and terminal devices. This is done in such a way that strong authentication of the ICC and credentials is possible in a fast, highly secure and private fashion without the exposure of card or cardholder identifying information or any other information which is useful to an attacker.

PLAID uses standards-based cryptography commonly available on ICCs, computer systems and embedded devices and is consequently highly portable to a wide range of ICC cards and IFD devices.

ISO/IEC draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of intellectual property concerning PLAID.

ISO/IEC takes no position concerning the evidence, validity and scope of such an intellectual property right.

The holder of the right has assured ISO/IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect the licence provided is perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge. The statement of the holder of this intellectual property right is registered with ISO/IEC. Information may be obtained from:

The Commonwealth of Australia, acting through the Commonwealth Services Delivery Agency, also known as "Human Services" or such other agency as may, from time to time, administer the PLAID Licence on behalf of the Commonwealth of Australia.

Address: Attn: PLAID; Human Services; PO Box 7788, Canberra M.C. ACT 2910, Australia

Email: PLAID@humanservices.gov.au

Licence: https://www.plaid.gov.au

ISO/IEC wishes to thank the Australian Commonwealth for their support of the development of PLAID and the provision of the associated intellectual property in a royalty free and no-charge licence.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

This is the first ISO/IEC edition, the previous Australian Standard, AS 5185:2010 is technically identical other than for references where ISO/IEC standards are required to differ due to ISO convention including compliance to nominated normative standards and where cipher strengths have been updated.

Identification cards — Integrated circuit card authentication protocols —

Part 1: **Protocol for Lightweight Authentication of Identity**

1 Scope

This International Standard provides an authentication protocol suitable for use in physical and logical access control systems based on ICCs and related systems which support standards based AES-128 and RSA-2048 ciphers and the SHA-256 hashing algorithm.

The standard specifies PLAID and its implementation in sufficient detail to allow any two or more implementations to be interoperable.

This International Standard does not address how implementations share cryptographic keys, access control system credential records (including revocation) or manage payload entities such as PIN, PINHash, or biometric templates or other payload objects.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies**.**

ISO/IEC 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-5, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation*

ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

IETF RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*