INTERNATIONAL STANDARD

ISO/IEC 19286

First edition
2018-01

Identification cards — Integrated circuit cards — Privacy-enhancing protocols and services

Cartes d'identification — Cartes à circuit intégré — Protocoles et services renforçant la protection des données personnelles

Reference number
ISO/IEC 19286:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms and notations ... **5**
5 General privacy principles ... **6**
5.1 General ... 6
5.2 Data minimization ... 7
5.3 User control ... 7
5.4 Data quality ... 7
6 Privacy architecture ... **8**
6.1 General ... 8
6.2 Categorization of data ... 9
6.2.1 User data and credentials ... 9
6.2.2 User input data ... 10
6.2.3 ICC data ... 10
6.2.4 Service provider data (SP data) ... 10
6.2.5 Issuer data ... 10
6.3 Participating entities ... 11
6.4 Privacy properties ... 11
6.4.1 Data minimizing properties ... 11
6.4.2 User control properties ... 12
6.4.3 Data quality properties ... 13
7 Privacy-enhancing protocols ... **14**
7.1 General ... 14
7.2 User verification ... 15
7.2.1 Purpose of user verification ... 15
7.2.2 Password verification with VERIFY command ... 15
7.2.3 Password verification with PACE ... 17
7.2.4 Biometric user verification ... 20
7.3 Device authentication protocols with optional user attribute access ... 22
7.3.1 Purpose of device authentication protocols ... 22
7.3.2 Authentication protocol PACE ... 22
7.3.3 Authentication protocol EACv2 with on-card user attributes ... 24
7.3.4 ABC protocol with on-card user attributes ... 30
7.3.5 Enhanced Role Authentication protocol (ERA) ... 34
7.3.6 Device authentication protocol OPACITY Full Secrecy ... 41
7.3.7 Device authentication protocol OPACITY BLINDED ... 43
7.4 Attribute verification mechanisms with COMPARE command ... 45
7.4.1 Purpose of attribute verification mechanism ... 45
7.4.2 General ... 45
7.4.3 Data comparison with external authentication function ... 46
7.4.4 Auxiliary data comparison with EACv2 protocol ... 47
7.5 Domain-specific identifier mechanisms ... 49
7.5.1 Purpose of domain-specific identifier mechanisms ... 49
7.5.2 Domain-specific identifier based on Restricted Identification ... 49
7.5.3 Domain-specific identifier based on pseudonymous signature for authentication ... 51
7.5.4 Domain-specific identifier based on ABC-based signatures ... 52
7.6 Pseudonymous signature mechanisms ... 52
7.6.1 Purpose of pseudonymous signatures ... 52

© ISO/IEC 2018 – All rights reserved

7.6.2 Chip Authentication based on Pseudonymous Signature for Authentication (CA-PSA) 52
7.6.3 Pseudonymous Signature of Credentials (PSC) 55
7.6.4 ABC-based signatures (ABC-Sig) 56

Annex A (informative) **Use cases** **59**

Annex B (informative) **Privacy Impact Assessment (PIA) guidance for electronic identification, authentication and trust services** **64**

Bibliography **75**

 © ISO/IEC 2018 – All rights reserved

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and security devices for personal identification.*

© ISO/IEC 2018 – All rights reserved

Introduction

National and pan-national (e.g. European) privacy regulations require the protection of personal data as well as implicitly linked parameters revealing the identity of the cardholder [see relevant documents in different countries (e.g. EU GDPR, US PIA, Canada PIA or Australian PIA)(see 5.1)].

Privacy-enhancing implementations allow a cardholder to be confident that their sensitive personally identifiable information (PII) is not exposed to an unauthorized environment. Thereby a cardholder may be exposed to an environment that might read sensitive PII from the Integrated Circuit Card (ICC) ahead of any external authentication. Such sensitive PII can be unique parameters of a card (e.g. the Card ID) or personalized parameters of the cardholder and could be linked to the cardholder.

For instance, if the nationality of a cardholder can be identified by the nature of the ICC description parameters (e.g. algorithm ID, if unique for particular country) then a cardholder of a certain nationality could be exposed to observation. An employee identification card, a health insurance card, a passport are typical examples which may require privacy protection.

ICC services ensuring privacy could, for instance, find further applications in the context of user privacy issues in eVoting systems with ICCs and in systems using the environment of Internet of Things as well as access services by means of an ICC.

This document reflects these requirements by harmonized operations and/or services in regard to a corresponding level of privacy. It envisions

— to strengthen common technical measures about privacy-enabling interchange at card edge and to facilitate its adoption,

— to harmonize privacy properties or privacy framework definitions when existing, and

— to address generic technical features related to privacy implementation at card edge (interchange) regardless of the cryptographic mechanisms by considering transactional aspects as asynchronous protocols involving several entities in privacy context.

© ISO/IEC 2018 – All rights reserved

Identification cards — Integrated circuit cards — Privacy-enhancing protocols and services

1 Scope

This document aims to normalize privacy-enhancing protocols and services by

— using the mechanisms from parts of ISO/IEC 7816 and parts of ISO/IEC 18328 that contribute to security and privacy,

— providing discoverability means of privacy-enabling attributes,

— defining requirements for attribute-based credential handling, and

— identifying data objects and commands for ICCs.

Existing privacy-enhancing protocols available in a generic context are adopted for distributed systems including ICCs. Additionally, existing authentication protocols between an ICC and an external device used for establishing a secure channel are enhanced with privacy protection. Secure communication between an ICC and an on-card device is also considered.

All the protocols and services described in this document contribute to privacy. Annex B describes an example of privacy impact assessments of respective systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-8, *Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations*

ISO/IEC 7816-9, *Identification cards — Integrated circuit cards with contacts — Part 9: Interindustry commands for card and file management*

ISO/IEC 7816-11, *Identification cards — Integrated circuit cards with contacts — Part 11: Personal verification through biometric methods*

ISO/IEC 18328-3, *Identification cards — ICC-managed devices — Part 3: Organization, security and commands for interchange*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

© ISO/IEC 2018 – All rights reserved

3.1
access phrase
alpha-numeric string to be captured by interface device to gain access to ICC

EXAMPLE MRZ printed on electronic passports and optically captured by inspection system.

3.2
anonymity
characteristic of information that does not permit a *personally identifiable information principal* (3.22) to be identified directly or indirectly

[SOURCE: ISO/IEC 29100:2011, 2.1]

3.3
attribute
user attribute
quality or characteristic ascribed to someone or something

[SOURCE: NIST SP 800-63-3]

EXAMPLE User name, address, date of birth or assertion about date of birth are user attributes.

Note 1 to entry: Examples of user attributes that can be used to identify natural persons are given in Reference [14].

3.4
attribute integrity
capability of an *attribute* (3.3) to resist to unintended or unauthorized modification

3.5
attribute provider
entity (3.13) that makes *user attributes* (3.3) available

Note 1 to entry: An attribute provider may be an *identity provider* (3.18) or an entity mandated by an identity provider.

3.6
attribute statement
statement or assertion about user attributes comprising predicates over *attributes* (3.3)

EXAMPLE The business case age verification usually does not require information about the user attribute "date of birth" but only the verification if the age is above a specific threshold, i.e. the attribute statement over the "date of birth" saying "is over 21".

3.7
authentication
provision of assurance in the *identity* (3.17) of an *entity* (3.13)

[SOURCE: ISO/IEC 29115:2013, 3.2]

3.8
authentication protocol
defined sequence of messages between an *entity* (3.13) and a verifier that enables the verifier to perform *authentication* (3.7) of an entity

[SOURCE: ISO/IEC 29115:2013, 3.4]

3.9
credential
set of data presented as evidence of a claimed or asserted *identity* (3.17) and/or entitlements

[SOURCE: ISO/IEC 29115:2013, 3.8]

© ISO/IEC 2018 – All rights reserved

3.10
domain-specific identifier
attribute (3.3) or *attribute statement* (3.6) over an *identifier* (3.16) of an entity, which carries semantics only in specific domains or contexts

Note 1 to entry: In the literature, such domain-specific identifiers may be also referred to as pseudonyms, domain pseudonyms, context-specific identifiers or sector-identifiers and in pseudonymization (see ISO/IEC 29100 for definition of pseudonymization).

Note 2 to entry: In contrast to *anonymity* (3.2), the *user* (3.32) creates and uses an ambiguous parameter, the pseudonym (e.g. a phantasy name), which is not sufficient for user *identification* (3.15) but is useful to partially recognize and address the user for dedicated communication purpose (e.g. chat room, forum).

3.11
eID-Application
on-card application that manages *user attributes* (3.3) for electronic *identification* (3.15) purposes and controls access to the user attributes

3.12
eID-Server
application running on a local or remote server that enables access to *user attributes* (3.3) managed by an *eID-Application* (3.11)

3.13
entity
something that has separate and distinct existence and that can be identified in a context

[SOURCE: ISO/IEC 29115:2013, 3.10]

3.14
generic attributes
user attributes (3.3) that are not linked to the *terminal domain-specific identifier* (3.29) of the requesting terminal stored in a file and identified by a file identifier

3.15
identification
process of distinguishing an *entity* (3.13) within a given context by the unique association of a set of descriptive parameters

EXAMPLE User attributes are descriptive parameters.

3.16
identifier
data which identifies an *entity* (3.13) in a given context towards another entity

3.17
identity
set of *attributes* (3.3) related to an *entity* (3.13)

[SOURCE: ISO/IEC 29115:2013, 3.13]

3.18
identity provider
trusted actor that issues and/or manages *credentials* (3.9)

Note 1 to entry: In literature, such identity provider is often referred to as identity information provider (see ISO/IEC 24760-1) or credential service provider (see ISO/IEC 29115).

© ISO/IEC 2018 – All rights reserved

3.19
issuer
entity that is an *identity provider* (3.18) or attribute provider

Note 1 to entry: An issuer may also issue the *token* (3.30).

3.20
mutual authentication
authentication of *identities* (3.17) of *entities* (3.13) which provides both entities with assurance of each other's identity

3.21
password
alpha-numeric string kept secret by the user and used for user verification

3.22
personally identifiable information
PII
any information that (a) can be used to identify the *PII principal* (3.23) to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.23
PII principal
natural person to whom the *personally identifiable information (PII)* (3.22) relates

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.24
privacy impact assessment
PIA
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information* (3.22), framed within an organization's broader risk management framework

Note 1 to entry: This process is also known as a privacy risk assessment.

[SOURCE: ISO/IEC 29134:2017, 3.7]

3.25
secure channel
communication link between the ICC and the external world that provides confidentiality and/or integrity

3.26
sensitive PII
category of *personally identifiable information (PII)* (3.22), either whose nature is sensitive, such as those that relate to the *PII principal's* (3.23) most intimate sphere, or that might have a significant impact on the PII principal

[SOURCE: ISO/IEC 29100:2011, 2.26]

3.27
service provider
entity (3.13) providing one or more services

3.28
specific attributes
user attributes (3.3) that are stored in data containers each linked to a *terminal domain-specific identifier* (3.29)

© ISO/IEC 2018 – All rights reserved

3.29
terminal domain-specific identifier
identifier of a terminal which carries semantics only in specific domains or contexts

Note 1 to entry: In contrast to domain-specific identifiers generated by the ICC to provide a pseudonym of the user, a terminal domain-specific identifier links a certain terminal identity to a certain domain (sector).

3.30
token
physical device or digital information, holding *credentials* (3.9), *user attributes* (3.3), *attribute statements* (3.6) and/or other information to be used in authentication procedures

3.31
unlinkability
property that *user's* (3.32) transactions are not linked with other transactions of the same user

3.32
user
natural person who receives and subsequently holds the *token* (3.30) and uses it to assert *user attribute* (3.3) information to relying entities

4 Abbreviated terms and notations

ABC	Attribute-Based Credentials
ADF	Application Dedicated File
APDU	Application Protocol Data Unit
AtP	Attribute Provider
CA-ABC	Chip Authentication based on ABC-based signatures
CA-PSA	Chip Authentication based on Pseudonymous Signature Authentication
CAR	Certificate Authority Reference
CAv2	Chip Authentication version 2 as part of EACv2
CHA	Certificate Holder Authorization
CIA	Cryptographic Information Application
CHAT	Certificate Holder Authorization Template
CHR	Certificate Holder Reference
C-RP	Command Response Pair, i.e. pair of command and response APDU
DF	Dedicated File
EACv2	Extended Access Control version 2
	NOTE Extended access control version 1 is defined for EU passports.
EF.ATR	Elementary File for Answer-To-Reset
eID	electronic Identification
eMRTD	electronic Machine Readable Travel Document

© ISO/IEC 2018 – All rights reserved