BS ISO/IEC 19286:2018

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19286:2018

National foreword

This British Standard is the UK implementation of ISO/IEC 19286:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 89245 5

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19286:2018

INTERNATIONAL STANDARD

ISO/IEC 19286

First edition
2018-01-15

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)

Documents
Document Sharing Hub
© ISO/IEC 2018

Full document details: BS ISO/IEC 19286:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19286:2018

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

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

INTERNATIONAL STANDARD **ISO/IEC 19286:2018(E)**

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

ERA	Enhance Role Authentication
GUI	Graphical User Interface
ICC	Integrated Circuit Card
IFD	Interface Device
MRZ	Machine Readable Zone
OID	Object Identifier
PACE	Password Authenticated Connection Establishment
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PSC	Pseudonymous Signature for Credentials
SM	Secure Messaging
SP	Service Provider
SW1-SW2	Status Word one and Status Word two

5 General privacy principles

5.1 General

A number of basic principles have evolved [e.g. in ISO/IEC 29100 or Fair Information Practice Principles (FIPPs)[24]] of which this document considers the following general principles as being the most relevant from the ICC technical perspective:

— data minimization;

— user control over user attribute release;

— quality of user attributes.

Those principles have been expressed, among others, in data protection recommendations or legislation for the protection of personal data as well as implicitly linked parameters revealing the identity of the token holder (e.g. the OECD principles[1)] for transborder flows of personal data of 2013, the Data Protection Convention and Directive of the Council of Europe[2),3)] (also known as Convention 108) or the PIA Frameworks of ISO[17], the US[4)], Canada[5)] and Australia[6)].

1) The Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (July 2013).

2) Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981.

3) Regulation 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

4) US Department Of Commerce PIA requirement based on Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors (August 27th, 2004).

5) Directive on Privacy Impact Assessment, The Treasury Board of Canada Secretariat's (TBS), April 1 2010.

6) Office of the Australian Information Commissioner, "Guide to undertaking privacy impact assessments", http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

This document focuses on security safeguards in the context of ICCs to protect PII against risks such as unauthorized access, use or modification or unintended or inappropriate disclosure.

NOTE ISO/IEC 29100 and FIPPS each list at all 11 and 8 privacy principles, respectively. The application of all these principles in a certain business case requires additional technical, organizational and procedural measures (e.g. at issuer, service provider and identity provider side) that are not addressed by this document.

5.2 Data minimization

Data minimization refers to the property of reducing the amount of PII being transmitted in a given transaction to exactly what is required from the point of view of the underlying business process the data is required for. The data minimization principle can be derived from the purpose specification and the proportionality principles.

The excessive release of user attributes as well as the establishment of non-required linkabilities between transactions is a main problem countering the data minimization principle. For instance, conventional signature schemes, such as RSA, DSA or elliptic curve use certificates, which may allow traceability of transactions if not deployed appropriately.

Realizing data minimization in practice does not only require the use of appropriate technology, but it also requires design of business processes to be data minimizing. Current business processes are defined with only the traditional technologies in mind and thus, have substantial shortcomings in terms of data minimization. Thus, implementing the data minimization principle requires the whole identity system to evolve. This document describes the technology that enables system designers to develop data minimizing solutions.

5.3 User control

User control of the release of user attributes refers to a user's authority over which user attribute is released to which entities. This control over disclosure of attribute information is at the core of European data protection legislation and also of various large R&D projects in the security and privacy domain in Europe[7)]. User control is also a key principle in the US-based NSTIC program[8)]. Different strengths of user control related to the release of data can be achieved depending on the trust in the reader devices and online versus offline interaction.

The way a solution is realized from a technical perspective determines the degree of user control. A first class of use cases is characterized by the ICC being handed over and used in the device of the attribute recipient, while a second class is characterized by the user using their own device (e.g. computer or phone). As the user should be able to select the user attributes to be released in the transaction, a user's own device may be considered more trusted.

Cryptographic technologies defined in this document can be used to enforce user control for the initial release of user attributes to a service provider. Though, in today's complex value chains of online services, data need to be provided by service providers to third party service providers. Interactions between the service providers and third-party providers are out of scope of this document.

5.4 Data quality

Data quality relates to user attributes being accurate and kept up to date and inaccurate or incomplete attributes are rectified or deleted. The correctness aspect of attributes has relevance in the reduction of cost, increasing efficiencies, and avoiding problems for both processing parties and citizens. Hence, data quality is the combination of organizational and technical measures. The approach adopted is to consider technical mechanisms for updating and improving the quality of data retained. Organizational elements are out of scope of this document.

---

7) ABC4Trust Consortium, ABC4Trust Web site, available at: https://abc4trust.eu/ PRIME Consortium, PRIME project web site, 2008, www.prime-project.eu PrimeLife Consortium, Primelife project web site, 2010, www.primelife.eu

8) NSTIC: National Strategy for Trusted Identities in Cyberspace, available at http://www.nist.gov/nstic/.

© ISO/IEC 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

Any technology that can convey attributes in integrity-protected form can help improve data correctness and thus data quality. Thus, the widespread use of such technology can reduce data management costs of both public and private sector service providers.

6 Privacy architecture

6.1 General

This clause provides an introductory material for the ICC privacy-enhancing protocols and services. Command and data flow between the ICC and "the external world" is defined for each protocol in the following clauses along with its privacy assessment. The "external world" could be one or more of these entities:

a) an IFD;

b) a GUI controlled by either:

   1) the ICC;

   2) the IFD;

   3) the eID-Server;

c) Service providers;

d) eID-Servers;

e) Attribute providers.

The description of multi-party protocols involving an ICC includes information about what participating entity has rights to access particular ICC data and how the user can control this access. Clause 6 lists the participating entities, categorizes the various data and links data with the respective entities. Moreover, several generic privacy requirements are listed in this clause in order to determine to what extent a particular protocol or sequence of protocols contributes to privacy. Figure 1 gives an overview of the document structure focusing on the protocols, mechanisms, data types and participating entities used.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

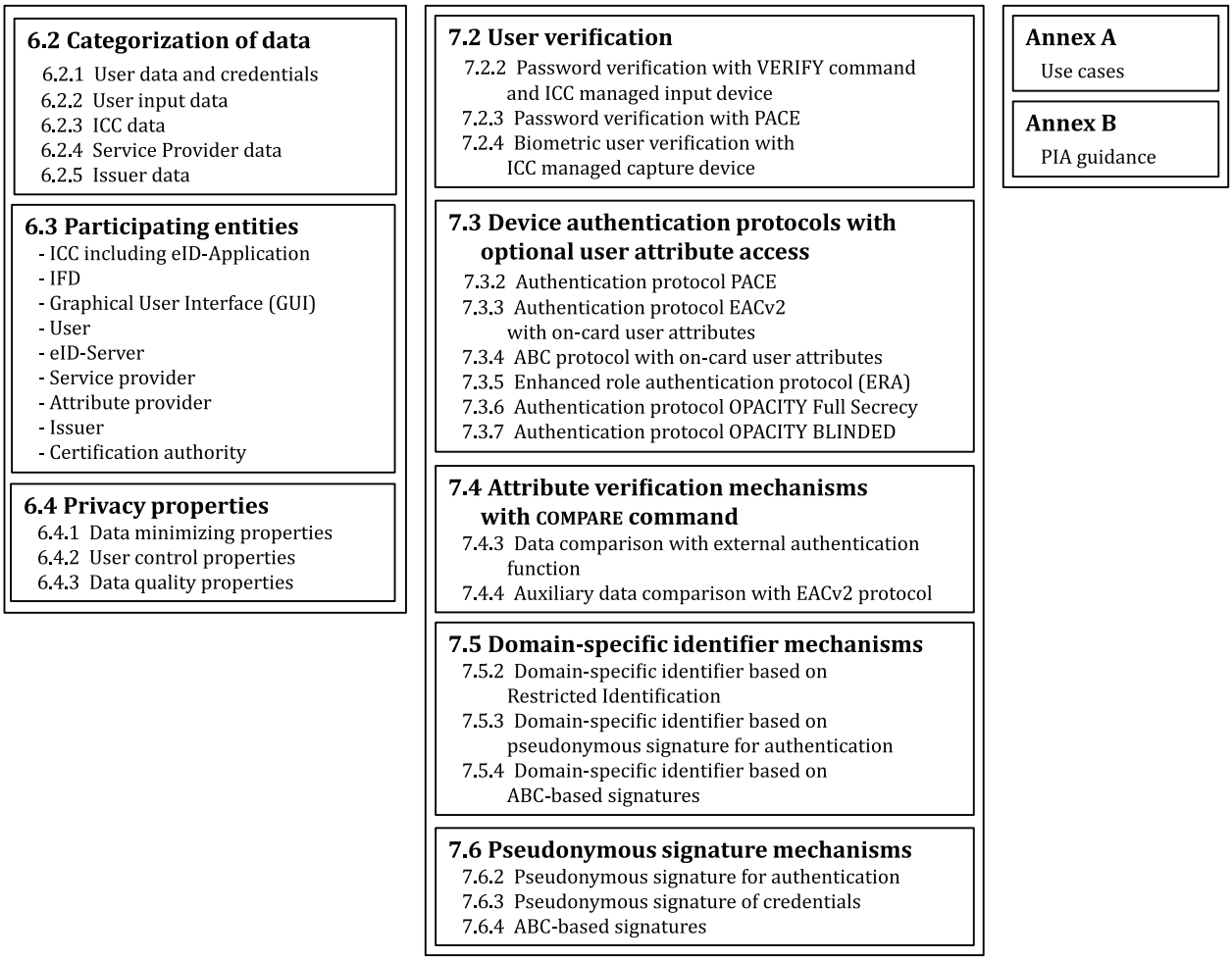

Figure 1 — Overview on the structure of this document without introductory and general clauses

6.2 Categorization of data

6.2.1 User data and credentials

User data (e.g. user attributes or attribute statements or credentials) are PII and refer to any item of personal information identifying the user and delivered under control of an issuing authority. Such data may be stored within an ICC and protected by access rules depending on the issuer's policy. These data may be requested either by an authority eligible to identify the user or by a system granting access to some electronic service (e.g. service provider, identity provider or certification authority).

User attributes

— may be in all or parts of information disclosed to a system upon user consent and upon access condition defined by issuer's policy,

— may be stored in any structure defined in ISO/IEC 7816-4 or in any proprietary structure depending on the application,

— may be replicated on-card of an ICC and stored in a database from where they may be updated onto the ICC,

— may encompass as well the biometric reference data of the user,

— may be permanent or updated over time,

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

— may be valid for a single access,

— may be valid for a specific time period (e.g. the time period is indicated by the authority that has issued the identity attribute), and

— may be valid until revoked.

Attribute statements can be divided into three main sub-types.

— Domain-specific identifiers (pseudonyms)[9]**:** This sub-type is unique to a domain. A domain-specific identifier may be generated by the user or resulting from a computing process that can take place either within an ICC under user control or on server side.

— Dynamic attribute statements: This may be a certified statement signed by an authority, a statement delivered by a trusted third party under secure conditions or a statement computed by the ICC. These are generated upon request for a service and may be bound to a given service provider.

— Static attribute statements: This represents statements pre-computed by an authority, i.e. not generated in the running course of a transaction. They are not associated to a given service provider and so, they have a generic aspect.

6.2.2 User input data

User input data represent any data deliberately revealed by the user when prompted by a system (e.g. through a human computer interface). This category includes PIN, password or biometric data (e.g. fingerprint data captured on an external or an on-card biometric capture device).

The presentation of user input data (e.g. a password) together with authorization to disclose a list of attributes serves to obtain user consent.

NOTE The very nature of these data can jeopardize the entire privacy measures if not handled with caution by the user (e.g. choosing weak passwords), but they lie outside the boundaries of controlled digital security and can only be mitigated by guidelines and recommendations and by improving users' awareness.

6.2.3 ICC data

This is a category of data stored and retrieved from the ICC and is subject to traceability (e.g. ICC serial number or cryptographic unique identifier). This data is associated with the ICC and may result from its personalization and be set before ICC issuance. This data relates to the identification of a physical support and may be specific to the manufacturer or to the issuer and hence, may allow for indirect user identification. This data may be protected by security attributes specified in ISO/IEC 7816-4 to prevent their disclosure to unauthorized entities.

6.2.4 Service provider data (SP data)

Service provider data is information about the service provider [e.g. the Unique Resource Locator (URL), company name or financial figures]. Parts of this information may be presented to the user by the service provider. The communication protocol used to request a service by the user from the service provider (e.g. the user's computer system or web browser) is out of scope of this document.

6.2.5 Issuer data

Issuer data is any information that identifies the issuer (e.g. electronic signatures, cv-certificates according to ISO/IEC 7816-8 or X.509 certificates according to ITU-T[19] or organization name). This data is typically associated with the ICC and may result from its personalization and be set before

9) In the literature, such domain-specific identifiers may be also referred to as pseudonyms, domain pseudonyms, context-specific identifiers or sector-identifiers. Moreover, there are also other types of pseudonyms in literature, e.g. transaction pseudonyms.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

ICC issuance. Issuer data may allow for indirect user identification and may be protected by security attributes specified in ISO/IEC 7816-4 to prevent their disclosure to unauthorized entities.

6.3 Participating entities

The following participating entities are considered in this document.

a) ICC including eID-Application**:** An ICC may support one or more eID-Applications that manage user attributes and control the access to the user attributes. The user attributes may be written to the ICC, including eID-Application, during personalization or after issuing the ICC to the user. Typically, the eID-Application releases user attributes to a service provider after user authentication.

b) IFD: The IFD generally includes all locally operated components communicating with the ICC. The IFD may:

   1) communicate with the ICC (e.g. according to ISO/IEC 7816-3 or ISO/IEC 14443);

   2) provide means for password entry, biometric user authentication or for displaying information to the user (e.g. a GUI);

   3) be embedded in a hardware device or run as software on a local device (e.g. computer or mobile device) also often referred to as middleware;

   4) manage the communication to one or more remote eID-Servers.

c) Graphical User Interface (GUI): A GUI may display information to the user and may request interaction with the user. A GUI may be controlled by the IFD, by the ICC itself according to ISO/IEC 18328 or by a remote eID-Server.

d) User (see 3.32).

e) eID-Server (see 3.12).

f) Service provider (see 3.27).

g) Attribute provider (see 3.5).

h) Issuer (see 3.19).

i) Certification authority: A certification authority is the entity that certifies a digital identity, typically by issuing digital certificates binding a public key to an identity. An issuer may run a certification authority.

6.4 Privacy properties

6.4.1 Data minimizing properties

6.4.1.1 Partial attribute release

Partial release of user attributes and attribute statements contributes to realizing data minimization. This requires the use of technology, which does not inherently lead to the release of all or large parts of the PII in each transaction.

NOTE Data minimization is closely linked to the principle of “collection limitation” but goes further than that. Whereas “collection limitation” refers to limited data being collected in relation to the specified purpose, “data minimization” strictly minimizes the processing of PII (see ISO/IEC 29100:2011, 5.5).

6.4.1.2 Unlinkability

Unlinkability of transactions at the cryptographic or protocol level may contribute to data minimization. Any identifiers should be made available consciously to establish linkabilities with other transactions.

© ISO/IEC 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

as required. Establishing linkability of a transaction with other transactions by default through an improperly designed cryptographic protocol layer counters the ideas of data minimization.

NOTE Today's schemes based on conventional signature schemes lead to linkability. This poses an increasing problem through the use of an eID in a large number of a user's interactions on the Internet.

6.4.1.3 Domain-specific identifier (Pseudonym)

Domain-specific identifiers, or pseudonyms, are another concept towards data minimization. They are a form of identifiers which avoid the use of the same unique identifier for a user in all its interactions. Particularly, when an ICC is used for both governmental applications and private sector applications, some countries mandate different identifiers to be used for public and private sectors. This is to prevent the exposure of substantial personal information from one entity's data to other entities.

6.4.1.4 Pseudonymous signatures

Computing a digital signature based on a domain-specific identifier (pseudonym) and associated attribute statements is a feature relevant for privacy-enhanced interactions where non-repudiation is required. Those signatures can either be an inherent part of the authentication protocol or exposed as a feature for legally-acknowledged digital signatures.

6.4.2 User control properties

6.4.2.1 User-centric system

In a user-centric system, the users have control over the use of their attributes, whether the user attributes are stored within the ICC or managed by an identity provider.

6.4.2.2 Offline/online operation

An online or an offline setting determines whether there is a remote entity (e.g. a service provider) to the transaction or whether the transaction is carried out autonomously without referral to a remote entity. In the offline setting, the user is present at the point where the transaction is executed. In this setting, the ICC may be physically inspected in addition to the use of the digital user attributes. The offline setting typically does not consider the service provider to communicate over a network.

In the online setting, the user performs the transaction remotely over a communication network. Stronger data minimizing and accountability properties are desired in online transactions.

6.4.2.3 Sharing protection

Sharing refers to the voluntary act of the user of giving another person access to the ICC. Thereby, privileges associated with the ICC may be shared with parties who may then be able to illegitimately claim those privileges without holding them. To avoid this, sharing protection can be seen as a basic security requirement. It is crucial that sharing be protected against in order to avoid people claiming privileges they do not hold.

6.4.2.4 User accountability

Accountability of the user is the property that a relying entity, i.e. the service provider, can hold a user accountable for their actions, even if the user is not identified or known under a civil identity at the time of the transaction. Ability to hold user accountable can allow the relying entity to take appropriate actions (e.g. legal investigation or enforcement of its rights). It is important to ensure that such capacity of a system is clearly explained to the user at enrolment and that suitable controls exist that ensure the revelation of an otherwise hidden identity can only occur under specified circumstances.

Those organizational measures are out of scope of this document. A variant of this is that a third-party obtains the identifying statement under the condition and can perform actions. Different trust and

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

execution models may apply for realizing different variants of the user accountability depending on the use case or deployment.

6.4.3 Data quality properties

6.4.3.1 Attribute authenticity

This refers to the authenticity and integrity of attributes being protected and released to the relying entities being consistent with the attributes the issuer has issued. Thus, attribute integrity and authenticity are the basic security properties assuring security of user attribute information not being tampered with. Achieving authenticity and integrity of the contained attributes is a foundational function of any government-issued security document.

6.4.3.2 Civil identity authentication

This refers to the authentication of user attributes or attribute statements corresponding to the civil identity of the user. A civil identity is considered a set of user attributes issued and maintained by a governmental institution. Thus, this is a special case of authenticating attributes with the intention of identifying the user.

NOTE The set of attributes used for identification is often a subset or extended subset of the civil identity of the user to be identified. Many business or government processes require identification, though many of those processes could suffice with less information being revealed, particularly without identifying the user.

6.4.3.3 Verifier accountability

Accountability of the verifier, i.e. the service provider, refers to the responsibility of the verifier of proving to a third-party that a proper verification of certain identity properties of users has been performed. For privacy reasons, this form of accountability should be possible without the users necessarily being identified.

EXAMPLE A merchant is able to prove to third parties intending to check compliance of the merchant, that the minimum age requirement of its customers as stipulated in legal regulations has been verified, without the customers necessarily being identified.

6.4.3.4 User binding

The ICC and, particularly, the credentials should be bound to the user, i.e. the legitimate holder to whom it is issued. This is crucial for the basic function of any government-issued document of associating attributes with people to whom they should apply.

6.4.3.5 Cloning protection

Cloning refers to the illegitimate reproduction of the ICC and user attributes. This may comprise cloning of the physical card body, the digital data stored on the token, or a combination thereof. Cloning may illegitimately give parties using cloned tokens privileges they would not hold otherwise.

6.4.3.6 Eavesdropping protection

Protocols executed between the ICC and a local or remote entity may protect against eavesdropping at the communication and logical layer. The basic security property is to ensure that such eavesdropping does not yield any personal information or any other information that may be useful to an attacker (e.g. information that would allow credential or user attribute cloning).

This is a very basic security property with privacy implications in terms of preventing the leakage of personal information to unauthorized parties. This requirement is crucial for the usage of the ICC in both offline and online settings.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

6.4.3.7 Attribute update

The update of attributes refers to the change of attribute values or addition of attributes regardless of whether the attributes are stored within an ICC or on a server. The attribute update can be performed in the field or remotely with or without the holder being required to be in-person.

6.4.3.8 Attribute revocation

Revocation of attributes refers to preventing the revoked attributes from being used in future transactions or ensuring that such use would be recognized as illegitimate by verifiers.

EXAMPLE Revocation of attributes stored in an ISO-compliant driving license can be required in case of the loss of certain driving-related permissions.

7 Privacy-enhancing protocols

7.1 General

This clause describes commands and data flow for interchange of privacy-enhancing protocols and services. These protocols are divided into the following five groups:

— user verification (see 7.2);

— device authentication (see 7.3);

— attribute verification (see 7.4);

— domain-specific identifier (see 7.5);

— pseudonymous signature (see 7.6).

An application designer can choose from the described protocols to best meet their individual requirements. Not every protocol can fulfill the needs of an application and not all protocols can be combined arbitrarily. Selecting an appropriate protocol for a given application is out of scope for this document.

EXAMPLE 1 There are application requirements that do not allow the user attributes to be stored within the ICC but at an attribute provider or vice versa or both, i.e. some user attributes are managed by the ICC whereas other user attributes are managed by one or more attribute providers.

This document focuses on the command and data flow at ICC interface but additionally takes into account the information flow of the external world which allows for addressing privacy issues. The participating entities (e.g. local terminal, remote terminal, attribute/service provider, user or user input/output device) as well as actions to be taken by the entities are named. For instance, it is of importance to describe which entity is in possession of secure messaging keys. Furthermore, how a user can control the information flow related to its user attributes is expressed.

While it is true that the protocols and mechanisms introduced in this document provide certain privacy properties, an application designer deploying one or more of the protocols and mechanisms should be aware that privacy protection requires the entire system to be considered.

EXAMPLE 2 An ICC implements a device authentication protocol with the privacy property of unlinkability and hence, cannot be tracked or traced. If this ICC additionally implements an elementary file readable without any access control and holding a unique serial number, the entire ICC does not fulfill the unlinkability property.

The protocol descriptions are structured in clauses as follows.

a) General protocol description

   This clause describes the main purpose of the protocol and application notes in text format. This clause also lists the fulfilled privacy and security properties (see 6.4).

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

b) Protocol sequence

This clause describes the overall protocol steps taking all participating entities and the information flow into account in the format of a sequence diagram with the following semantics for the information flow.

⟷	APDU Interface according to ISO/IEC 7816-4 (one or more SM C-RPs)
⟷	SM APDU Interface according to ISO/IEC 7816-4 (one or more SM C-RPs)
<----->	Interface out of scope

c) Data types and relying entities

This clause refines the information flow according to the protocol steps by specifying the type of information as given in 6.2, that is transmitted between a pair of participating entities in the format of a table.

d) C-RP description

This clause specifies the command sequence at ICC interface. Detailed information about data encoding and computations to be taken by the ICC is also specified.

NOTE Specifications are provided for all protocol steps that require actions by the ICC in the format of a C-RP sequence, i.e. the protocol steps marked as line with arrows in normal or bold font in the overall protocol sequence.

e) Protocol-dependent descriptions

This optional clause gives further information about data structures and algorithms related to the protocol.

7.2 User verification

7.2.1 Purpose of user verification

Successful user verification provides some level of assurance that the legitimate user is accessing the ICC. If the ICC fails to authenticate the user, a person may not be the legitimate user and/or the user may use an ICC he is not authorized to use. The success of user verification also provides the user's consent to grant access to credentials, user attributes and/or attribute statements managed by the ICC. User verification should be achieved at the beginning of an authentication process.

7.2.2 Password verification with VERIFY command

7.2.2.1 General protocol description

The user is authenticated by verification of the user password. The password, i.e. the verification data, shall be transmitted to the ICC either in the data field of the VERIFY command or by an ICC-managed input device which may require a sequence of ADDITIONAL DEVICE MANAGEMENT commands according to ISO/IEC 18328-3. If the verification data are transmitted in the data field of the VERIFY command, a device authentication protocol shall be performed prior to command execution (see 7.3).

The password verification is a one-to-one comparison performed by the ICC between the verification data and the reference data stored in the ICC.

If the password verification protocol involves an ICC with an ICC-managed input device, i.e. ICC-managed keypad, the protocol provides user binding and eavesdropping protection property, as well as strong unlinkability.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

7.2.2.2 Protocol sequence

This document provides two protocol sequences for password verification with VERIFY command considering an ICC-managed input device (e.g. a keypad) as it is described in ISO/IEC 18328-3. Device handling is either implicit or explicit.

a) Implicit device handling — Password verification with ICC-managed input device and implicit device handling includes the following steps (see Figure 2 without Step 2):

   1) IFD transmits VERIFY command with odd INS code and empty optional verification data DO expressing that the verification data comes from an ICC-managed input device;

   NOTE ISO/IEC 7816-4 describes that in case of empty verification data DO, the verification data come from a sensor (e.g. fingerprint sensor) on the card. This document considers ICC-managed keypad as input device and uses empty optional verification data DO.

   2) user enters password, i.e. the verification data, in the ICC-managed input device;

   3) if VERIFY command is successfully executed, security status is set.

b) Explicit device handling — Password verification with ICC-managed input device and explicit device handling includes the following steps (see Figure 2):

   1) sequence of additional device management commands (e.g. ADM OPEN DEVICE and ADM MANAGE DEVICE CONFIGURATION) to open and configure ICC-managed input device prior to the execution of VERIFY command;

   2) continue with VERIFY command as described in implicit device handling.

NOTE ISO/IEC 18328-3 specifies the command ADDITIONAL DEVICE MANAGEMENT (ADM) for a set of functions which are used to perform all activities of an ICC controlling any ICC-managed device independent of existing or future physical interfaces.

It is out of scope of the protocol descriptions how the user is informed by the IFD or a GUI to present its password, i.e. the verification data. Nevertheless, the protocol sequences can be easily extended by further ADDITIONAL DEVICE MANAGEMENT commands to present a display message to an ICC-managed output device.

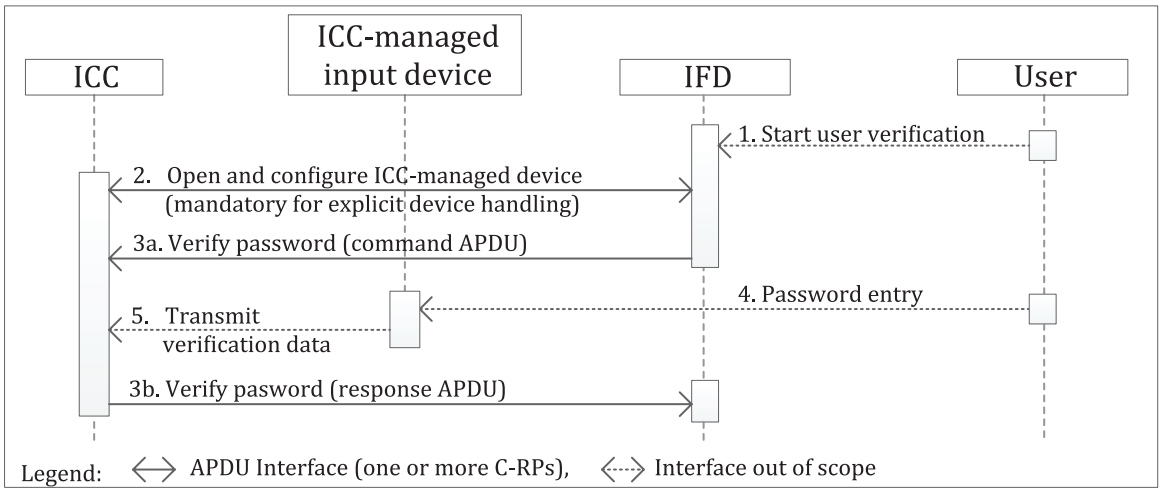

Figure 2 — Password verification with ICC-managed input device

7.2.2.3 Data types and relying entities

Table 1 shows data types and relying entities of password verification with VERIFY command and ICC-managed input device.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

Table 1 — Data flow of password verification with ICC-managed input device

Step	Sending entity	Receiving entity	Data type	Description
1	User	IFD	n/a	Start user verification
2	IFD	ICC	ICC data	In case of explicit device handling, the IFD may retrieve general feature management DO on supported services of ICC and sets input device in READY state
3a	IFD	ICC	ICC data	IFD starts password verification with command APDU of VERIFY command and implicitly sets input device in DEVICE OPERATION state
4	User	Input device	User input data	User presents its password to the input device (e.g. by typing the password)
5	Input device	ICC	User input data	Password of the user, i.e. verification data, transmitted to the ICC in a proprietary format
3b	IFD	ICC	ICC data	IFD gets response APDU and verification result from ICC

7.2.2.4 C-RP description

Table 2 shows the C-RP descriptions of password verification with VERIFY command and ADDITIONAL DEVICE MANAGEMENT command.

Table 2 — C-RP sequence of password verification with ICC-managed input device

Step	Command – INS	P1-P2	Command data field, Le field	Response data field, SW1-SW2
2_1	ADDITIONAL DEVICE MANAGEMENT – '16' Function in P1: OPEN DEVICE	'03 00'	Le='01' – {Device identifier} Device identifier may be obtained from general feature management DO in EF.ATR/INFO; step is mandatory for explicit device handling	{device handle number (DHN)} SWs according to ISO/IEC 18328-3
2_2	ADDITIONAL DEVICE MANAGEMENT – '16' Function in P1: MANAGE DEVICE CONFIGURATION	'0C xx'	'xx' – DHN from Step 2_1 {80 – L – see ISO/IEC 18328-3} Configure ICC-managed input device; step is optional for explicit device handling	Data field absent SW1-SW2 according to ISO/IEC 18328-3
3a/b	VERIFY – '21'	'00 yy'	'yy' – identifier of reference data {'5F 62' – '00' – optional verification data DO (empty)} {'4D' – L – extended header list referencing verification data DO (optional)} Verify password according to ISO/IEC 7816-4; identifier 'xx' may be obtained from CIA according to ISO/IEC 7816-15; an empty optional verification data DO expresses that the verification data come from an ICC-managed input device	Data field absent
Password verified, security status set				

7.2.3 Password verification with PACE

7.2.3.1 General protocol description

The PACE protocol[2][25] provides user authentication by deriving cryptographically strong session keys from a password with low entropy entered by the user at IFD side. With the successful establishment of

© ISO/IEC 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018

the secure channel between ICC and IFD, the user password has been verified. In contrast, a password verification (e.g. with VERIFY command) requires the transmission of the password to the ICC for one-to-one comparison within the ICC. The PACE protocol does not require the transmission of the password, which makes the protocol especially applicable for ICCs with contactless interface.

Password verification with PACE protocol includes the ICC, the IFD managing an input device and the user. The protocol provides strong eavesdropping protection and unlinkability properties, according to 6.4. Property user binding depends on the security of the input device (e.g. key pad securely managed by the IFD). However, a password can always be shared by the user on purpose.

NOTE A security analysis of the PACE protocol can be found in Reference [20].

If PACE is used in combination with EACv2, the protocol additionally provides confined authorizations of access rights of the local or remote entity. The user may restrict access rights of that entity by means of confined authorizations (see 7.2.3.4.2).

7.2.3.2 Protocol sequence

Figure 3 shows the protocol sequence of password verification with PACE.

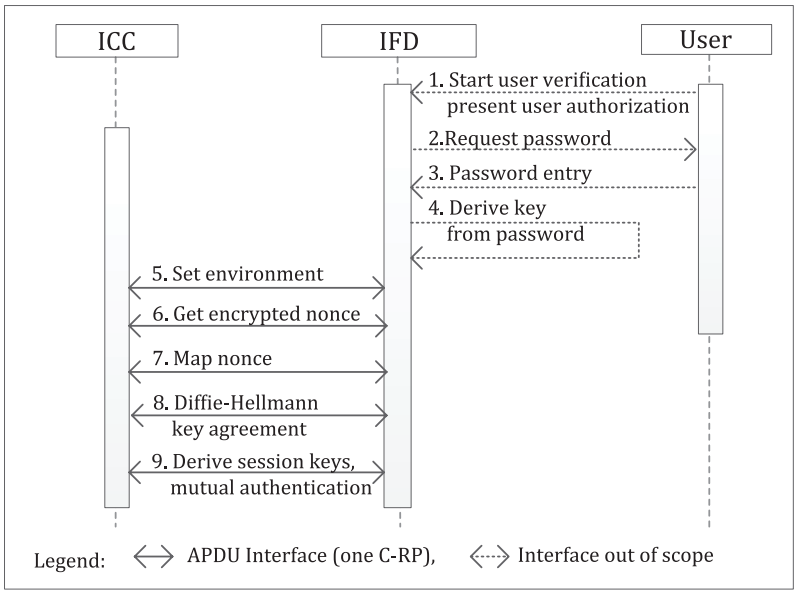

Figure 3 — Password verification with PACE

7.2.3.3 Data types and relying entities

Table 3 shows data types and relying entities of password verification with PACE.

Table 3 — Data flow of password verification with PACE

Step	Sending entity	Receiving entity	Data type	Description
1	User	IFD	User data	Start user verification, conditionally send user CHAT object encoding the restricted access rights by the local or remote terminal (e.g. eID-Server) to be verified in EACv2
2	IFD	User	n/a	Request user password
3	User	IFD	User input data	Present user password by typing password in IFD-managed input device
4	IFD	IFD	User input data	Derive PACE-key from user password

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19286:2018