

---

---

**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*





**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
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Abbreviated terms and notations .....</b>	<b>5</b>
<b>5 General privacy principles .....</b>	<b>6</b>
5.1 General .....	6
5.2 Data minimization .....	7
5.3 User control .....	7
5.4 Data quality .....	7
<b>6 Privacy architecture .....</b>	<b>8</b>
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
<b>7 Privacy-enhancing protocols .....</b>	<b>14</b>
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

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
<b>Annex A (informative) Use cases.....</b>		<b>59</b>
<b>Annex B (informative) Privacy Impact Assessment (PIA) guidance for electronic identification, authentication and trust services.....</b>		<b>64</b>
<b>Bibliography.....</b>		<b>75</b>

## 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](http://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](http://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](http://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*.

## 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.

# 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*