
**Information technology — Security
techniques — Requirements for partially
anonymous, partially unlinkable
authentication**

*Technologies de l'information — Techniques de sécurité — Exigences
pour l'authentification partiellement anonyme, partiellement non fiable*

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Terms and definitions	1
3 General	2
4 Framework	2
5 Requirements	4
Annex A (informative) Use cases	5
Annex B (informative) Application of the mechanism for the purpose of data authentication and data protection	7
Bibliography	9

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC should not be held responsible for identifying any or all such patent rights.

ISO/IEC 29191 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 27, *IT Security techniques*.

Introduction

The current state of the art for entity authentication requires the revelation of the identifiable information of an entity being authenticated. In many types of transactions, the entity would prefer to remain anonymous and unlinkable, which means that when two transactions are performed, it is difficult to distinguish whether the transactions are performed by the same user or two different users. However, in some circumstances there are legitimate reasons to enable subsequent reidentification (e.g., the interest of accountability). The term 'partially anonymous, partially unlinkable' means that an a priori designated opener, and that designated opener only, can identify the authenticated entity. For example, a library may need to identify an entity that has not returned a borrowed book in order to send a late notice to the entity. Current cryptographic technologies are available to provide partially anonymous, partially unlinkable authentication. This International Standard defines a framework and requirements for partially anonymous, partially unlinkable authentication.

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

1 Scope

This International Standard provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.

2 Terms and definitions

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

2.1

authentication

provision of assurance in the claimed identity of an entity

[SOURCE: ISO/IEC 18014-2]

2.2

claimant

entity which is or represents a principal for the purposes of authentication

[SOURCE: ISO/IEC 9798-1:2010]

2.3

credential

representation of an identity

[SOURCE: ISO/IEC 24760-1]

2.4

designated opener

entity who can re-identify the claimant from the transcript of authentication

NOTE The selection of the designated opener should be made in advance of transactions. The entity or entities that make that selection may vary with the implementation. As the designated opener has the capability of identifying the claimant, the selection of the designated opener and the selection of the transcript of authentication to be provided to the designated opener need to be carefully performed.

2.5

identity

set of attributes related to an entity

[SOURCE: ISO/IEC 24760-1]

2.6

re-identification

identification of a claimant following a partially anonymous, partially unlinkable authentication

NOTE Re-identification is also called opening.