INTERNATIONAL STANDARD

ISO/IEC 29191

First edition
2012-12-15

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 reliable

Reference number
ISO/IEC 29191:2012(E)

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

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.

2.6
transcript of authentication
record of sequences of exchanged data from a process of authentication

3 General

Many cryptographic mechanisms are available and in use today to improve the security of the authentication process. This leads to greater trust when, following a successful authentication, an entity is given appropriate access to protected resources using some authorization process. Note that the details of authorization are out of scope for this standard and thus marked in parentheses. A typical authentication and authorization model includes the following steps (with each step usually including a number of sub-steps, many of which are covered in ISO/IEC 29115):

a) Enrollment

b) Authentication

c) (Authorization)

Most cryptographic mechanisms in use today require the revelation of the identifiable information and enable tracking of an entity across transactions. For example, the use of public keys could hide an entity's real name. However, if the same public key or pseudonym is used for multiple authentications, it can be used to link information about the entity across transactions and so build a profile.

But complete anonymity and unlinkability may not always be desirable. For example, an entity could use anonymity to escape punishment for exploiting a system. So, while anonymity and unlinkability may be appropriate in some situations, there are cases where it may be necessary to give certain parties the ability to re-identify an entity.

To achieve the goal of partially anonymous, partially unlinkable authentication, the process steps now look like:

a) Registration/enrollment, including setup to achieve anonymity

b) Authentication

c) (Authorization)

d) Re-identification (when appropriate)

4 Framework

For the sake of understanding an overview of the framework, a typical scenario is exemplified, where a claimant begins by enrolling with a service. The service includes an issuer that generates credentials and issues them to the claimants. The claimants then use the credentials for authentication. If the authentication is successful, a transcript of authentication is created. Although it may contain other things, this transcript shall include information necessary to enable re-identification by the designated opener. If re-identification is required, the transcript of authentication is given to the designated opener who, a priori to any transactions, must be established and provided with the necessary cryptographic components required for re-identification. Each system will have its own set of practices and principles for determining when re-identification is appropriate or necessary. Those details are not within the scope of this standard. Principles such as openness, transparency and notice are explained in ISO/IEC 29100.

Every application will have its own requirements so any particular implementation may have variations from the flow described above. For example, the cryptographic-based credentials could be generated by the claimant, rather than the issuer; or credentials may be issued electronically or in person. But such variations do not change the fundamental aspects of the framework.

This framework defines a set of roles and operations, which are shown in Figure 1.

The four roles are:

a) Issuer – the entity who issues credentials to claimants

b) Claimant – the entity who will be authenticated by a verifier

c) Verifier – an entity that checks whether the claimant possesses credentials that are valid

d) Designated opener – the entity that can re-identify the claimant

Among the above four roles, there are four basic operations in this framework.

1) A process between an issuer and a claimant to perform a credential issuing process. After this process a claimant has a credential.

2) A process for the designated opener to setup the cryptographic information necessary for re-identification.

3) A process between a claimant and a verifier to perform authentication, which produces a transcript of authentication. Authentication is successful if the verifier can determine that the claimant possesses a valid credential.

4) A process by a designated opener to identify the claimant from the transcript of authentication, called re-identification. In this process, a designated opener uses the transcript of authentication and may use other information, where appropriate, to enable re-identification

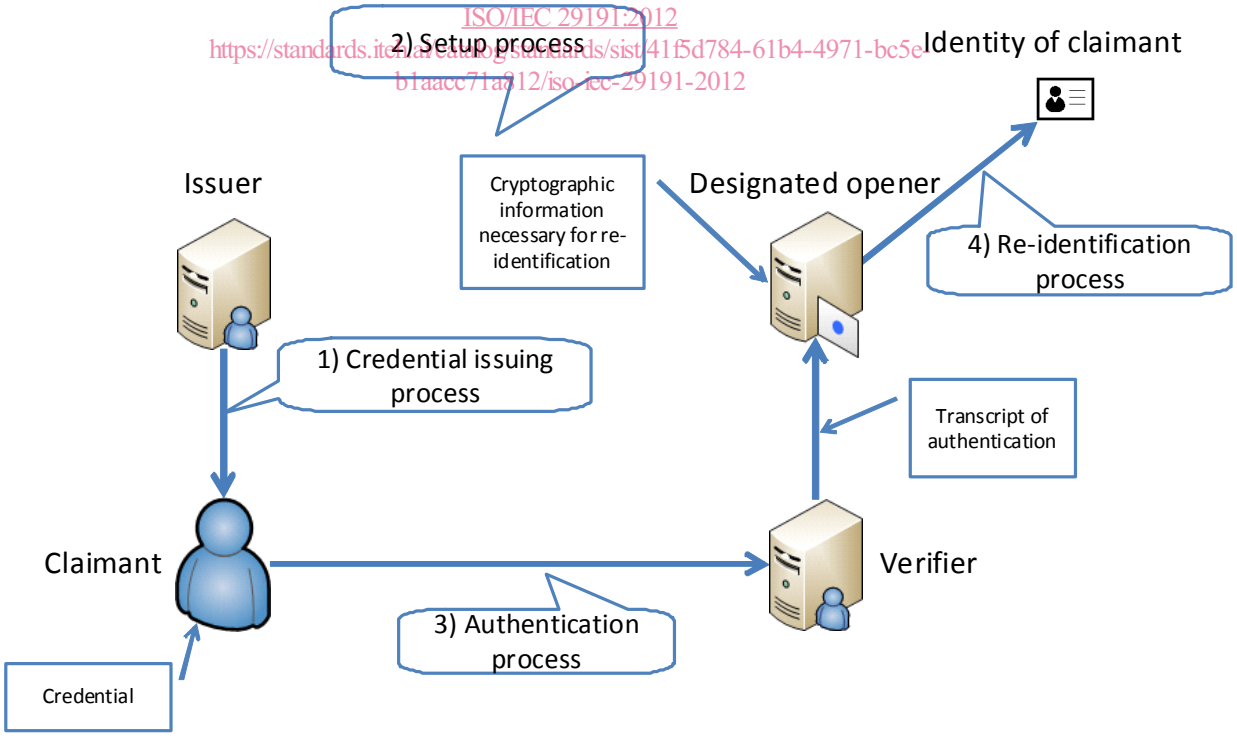

Figure 1 — Framework of partially anonymous, partially unlinkable authentication