INTERNATIONAL STANDARD

ISO/IEC 20009-1

First edition
2013-08-01

Information technology — Security techniques — Anonymous entity authentication —

Part 1: General

Technologies de l'information — Techniques de sécurité — Authentification d'entité anonyme —

Partie 1: Généralités

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

Reference number
ISO/IEC 20009-1:2013(E)

© ISO/IEC 2013

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

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
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

 © ISO/IEC 2013 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – 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.

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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 20009-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 20009 consists of the following parts, under the general title *Information technology — Security techniques — Anonymous entity authentication*:

— *Part 1: General*

— *Part 2: Mechanisms based on signatures using a group public key*

The following parts are under preparation:

— *Part 3: Mechanisms based on blind signatures*

— *Part 4: Mechanisms based on weak secrets*

Further parts may follow.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

 © ISO/IEC 2013 – All rights reserved

Introduction

Authenticating communicating partners is one of the most important cryptographic services. There are a wide variety of cryptographic mechanisms supporting this service, e.g. the entity authentication mechanisms specified in ISO/IEC 9798[2] and the digital signature mechanisms specified in ISO/IEC 9796[1] and ISO/IEC 14888.[4]

Anonymous authenticated communication involves hiding the identifier of an authenticated entity to its communicating partner and/or to a third party, while retaining the property that a verifier can reliably determine that its communication partner is authentic. Anonymous entity authentication mechanisms are designed to support such anonymous communications. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party.

In an anonymous entity authentication mechanism, the entity to be authenticated (the *claimant*) provides evidence to a *verifier* that it has knowledge of a secret without revealing its identifier to any unauthorized entity. That is, given complete knowledge of the messages exchanged between the parties, an unauthorized entity cannot discover the identifier of the entity being authenticated (i.e. the claimant). At the same time, an authorized verifier can obtain assurance that the claimant is authentic, i.e. that it possesses certain attributes, e.g. membership of a predefined group of entities. However, even an authorized verifier may not be authorized to learn the identifier of the entity being authenticated. Anonymous entity authentication mechanisms may permit an authorized party to perform *opening*, a process which enables the authorized party to learn the identity of the entity that engaged in a particular instance of the mechanism. Mechanisms which permit opening are referred to as partially anonymous entity authentication mechanisms.

Anonymous entity authentication can be applied in a range of scenarios including electronic business, electronic voting, electronic identities (such as e-driving licences, e-health IDs and e-passports), social networks, mobile payments and trusted computing. In many such services, a client's personally identifiable information (PII) is revealed to a service provider as part of the authentication process. As a result the service provider may be in a position to use the PII for a range of purposes, not necessarily in the interests of the PII subject. One way of restricting access by service providers to PII is through the use of anonymous authentication mechanisms. Some use cases of anonymous entity authentication are described in Annex A of ISO/IEC 29191:2012.[6]

ISO/IEC 20009 specifies a general model and a number of mechanisms for anonymous entity authentication. The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC 20009, but in the following parts of ISO/IEC 20009.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

Information technology — Security techniques — Anonymous entity authentication —

Part 1: General

1 Scope

This part of ISO/IEC 20009 specifies a model, requirements and constraints for anonymous entity authentication mechanisms that allow the legitimacy of an entity to be corroborated.

2 Terms and definitions

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

2.1
anonymity strength
number derived from the probability that an unauthorized entity can correctly determine the true signer from a given signature

Note 1 to entry: An anonymity strength of *n* means that the probability that an unauthorized entity can correctly guess the true signer from a signature is 1/*n*.

[SOURCE: ISO/IEC 20008-1:—]

2.2
anonymous entity authentication
corroboration that an entity possesses certain attributes, without distinguishing this entity from other entities with the same attributes

2.3
anonymous digital signature
signature which can be verified using a group public key or multiple public keys, and which cannot be traced to the distinguishing identifier of its signer by any unauthorized entity including the signature verifier

[SOURCE: ISO/IEC 20008-1:—]

2.4
challenge
data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier

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

2.5
claimant
entity which is or represents a principal for the purposes of authentication

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – All rights reserved

2.6
key
sequence of symbols that controls the operation of a cryptographic transformation

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

2.7
linker
entity which performs linking, i.e. which links two or more instances of anonymous entity authentication

2.8
linking
process by which two or more instances of anonymous entity authentication are shown to have been performed by the same entity

2.9
opener
authorized entity which performs opening, i.e. which learns the identity of the party that engaged in a particular instance of an anonymous entity authentication mechanism

Note 1 to entry: An opener is referred to as a designated opener in ISO/IEC 29191.

2.10
opening
process by which an authorized entity learns the identity of the party that engaged in a particular instance of an anonymous entity authentication mechanism

Note 1 to entry: Opening is referred to as re-identification in ISO/IEC 29191.

2.11
mutual anonymous authentication
anonymous entity authentication that provides both entities with assurance of the legitimacy of the other entity

2.12
partially anonymous authentication
anonymous entity authentication permitting opening by authorized entities

2.13
principal
entity whose legitimacy can be authenticated

2.14
random number
time variant parameter whose value is unpredictable

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

2.15
sequence number
time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

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

2.16
time stamp
time variant parameter which denotes a point in time with respect to a common reference

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – All rights reserved

2.17
time variant parameter
data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp

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

2.18
token
message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique

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

2.19
trusted third party
security authority or its agent, trusted by other entities with respect to security related activities

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

2.20
unilateral anonymous authentication
anonymous entity authentication that provides one entity with assurance of the legitimacy of the other entity, but not vice versa

2.21
unilateral-anonymous mutual authentication
result of a process between two parties which simultaneously provides anonymous entity authentication in one direction and entity authentication in the other direction

2.22
verifier
entity which requires assurance of the legitimacy of another entity (the claimant)

3 Symbols and abbreviated terms

3.1 Symbols

A entity participating in an anonymous entity authentication mechanism

B entity participating in an anonymous entity authentication mechanism

3.2 Abbreviations

TTP Trusted Third Party

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – All rights reserved

4 Anonymous entity authentication model

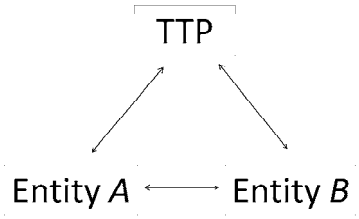

Figure 1 — Anonymous entity authentication model

The general model for anonymous entity authentication mechanisms is shown in Figure 1. It is not essential that all the entities and exchanges are present in every authentication mechanism.

For the anonymous entity authentication mechanisms specified in the other parts of ISO/IEC 20009, for unilateral anonymous authentication, entity *A* is considered the claimant, and entity *B* is considered the verifier. For mutual anonymous authentication, *A* and *B* each take the roles of both claimant and verifier. For unilateral-anonymous mutual authentication, *A* and *B* each take the role of both claimant and verifier; in addition, one direction of the authentication is anonymous and the other is not (for example, *A* verifies *B*'s identity and *B* verifies that *A* is a member of a pre-defined group of entities).

The precise role of the TTP depends on the mechanism in use. Some mechanisms may not use any trusted third parties. Alternatively, a TTP may only be involved in an offline way, e.g. by providing one or both of *A* and *B* with information supporting use of the mechanism prior to its use. As a third alternative, a TTP may be actively involved in the mechanism by exchanging messages with one or both parties during use of the mechanism. A TTP may also be involved in the opening or linking processes. If a TTP is involved, either offline or online, then it must be trusted by the involved parties for the purpose of anonymous entity authentication.

For anonymous entity authentication purposes, the entities generate and exchange standardised messages, called tokens. It takes the exchange of at least one token for unilateral anonymous authentication and the exchange of at least two tokens for mutual anonymous authentication. An additional pass may be needed if a challenge has to be sent to initiate the anonymous entity authentication exchange. Additional passes may be needed if a trusted third party is involved.

In Figure 1 the arrows indicate potential information flow. Entities *A* and *B* may directly interact with each other, directly interact with the trusted third party through *B* or *A* respectively, or use information issued by the trusted third party.

The message exchanges making up an anonymous entity authentication mechanism provide evidence to the verifier that the claimant is authentic, i.e. that it possesses certain attributes, e.g. membership of a predefined group of entities. This evidence takes the form of demonstrating knowledge via cryptographic techniques of certain secret information, which only an authentic entity is entitled to possess. In addition, certain mechanisms also allow the claimant to demonstrate to the verifier that it possesses other attributes in addition to being an authentic entity.

Details of the anonymous entity authentication mechanisms of ISO/IEC 20009 are specified in subsequent parts of this multipart standard.

5 General requirements and constraints

In order that one entity (i.e. the verifier) can anonymously authenticate another entity (i.e. the claimant), both claimant and verifier shall use a common set of cryptographic techniques and parameters.

During the operational life of a cryptographic key, the values of all time-variant parameters on which the key operates (i.e. time stamps, sequence numbers and random numbers) shall be non-repeating, at least with overwhelming probability.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

 © ISO/IEC 2013 – All rights reserved

It is assumed that, during use of an anonymous entity authentication mechanism, the entities *A* and *B* are aware of each other's claimed status, i.e. which group the claimant is claiming membership of, and what, if any, additional characteristics it is asserting to be true. This may be achieved by the inclusion of data (including cryptographically generated data strings) in information exchanges between the two entities, or it may be apparent from the context of the use of the mechanism.

The authenticity of the claimant can be ascertained only for the instant of the anonymous entity authentication exchange. To guarantee the authenticity of data subsequently communicated between claimant and verifier, the anonymous entity authentication exchange shall be used in conjunction with a secure means of communication (e.g. a communications session whose content is integrity-protected using a data integrity mechanism such as a digital signature or message authentication code, where the necessary secret key or public/private key pair is established during the anonymous entity authentication exchange).

If partially anonymous authentication is required, the claimant must provide sufficient data during the authentication exchange to enable subsequent opening by authorized entities.

6 Managing anonymity

The degree of anonymity offered to an individual will vary depending both on the properties of the anonymous entity authentication mechanism employed, and the environment in which it is used. For example, if an entity demonstrates possession of an attribute known from the context of use to be possessed by only two individuals, then the degree to which the entity remains anonymous is clearly limited. This motivates the notion of anonymity strength as the size of the set of entities within which an entity is known to belong; in the above example, the entity with the almost unique attribute would have an anonymity strength of 2.

In some cases it may be necessary for the anonymity of a participant in an authentication session to be revoked after use of a mechanism, where this loss of anonymity may be complete or limited. We identify two specific cases of such a reduction in anonymity, namely linking and opening. Linking is a process, performed by an entity known as a linker, by which two or more instances of anonymous entity authentication are shown to have been performed by the same entity, and represents some loss of anonymity. Opening is a process by which an authorized entity, known as an opener, learns the identity of the party that engaged in a particular instance of an anonymous entity authentication mechanism, and represents complete loss of anonymity, at least with respect to the opener. It is important to note that not all mechanisms necessarily support linking or opening. An anonymous entity authentication mechanism which permits opening by authorized entities is known as a partially anonymous authentication mechanism. An anonymous entity authentication mechanism which permits opening by authorized entities and which does not have a linking capability is known as a partially anonymous, partially unlinkable authentication mechanism.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20009-1:2013

© ISO/IEC 2013 – All rights reserved