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

Reference number
ISO/IEC 20009-1:2013(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

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.

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.