First edition
2013-12-01

Information technology — Security techniques — Anonymous entity authentication —

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

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

Partie 2: Mécanismes fondés sur des signatures numériques utilisant une clé publique de groupe

Reference number
ISO/IEC 20009-2:2013(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.

ISO/IEC 20009-2 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*

Mechanisms based on blind signatures and *Mechanisms based on weak secrets* will form the subjects of future Parts 3 and 4, respectively.

Further parts may follow.

Introduction

Anonymous entity authentication is a special type of entity authentication. In an anonymous entity authentication mechanism, given a message that was generated during the authentication protocol, an unauthorized entity cannot discover the identifier of the entity being authenticated (the claimant). At the same time, an authorized verifier can obtain assurance that the claimant is authentic. However, even an authorized verifier may not be authorized to learn the identifier of the entity being authenticated.

The anonymous entity authentication mechanisms specified in this part of ISO/IEC 20009 are based on anonymous signatures using a group public key, discussed in ISO/IEC 20008-2. An anonymous signature using a group public key is sometimes simply known as a group signature. A group signature has the following properties.

— Only group members are able to correctly sign messages.

— The verifier can verify that it is a valid group signature, but cannot discover which group member generated it.

— Optionally, the signature can be “linked” or “opened”.

The anonymous entity authentication mechanisms specified in this part of ISO/IEC 20009 involve the following basic operations.

— An entity (verifier) which wants to authenticate another entity (claimant) interacts with the claimant.

— The claimant sends a token (and optionally a group public key certificate) to the verifier.

— The verifier confirms the validity of the provided token (and optionally the group public key certificate).

One of the major differences between a (conventional) entity authentication mechanism based on (conventional) digital signatures and an anonymous entity authentication mechanism based on signatures using a group public key is the nature of the digital signature scheme used to produce tokens and to provide confirmation of messages that were generated during the authentication protocol. Another difference is that, for an anonymous authentication mechanism, the claimant belongs to a group, and authentication is conducted with respect to this group. Authentication mechanisms require associated methods to manage the relationship between an entity and a group; for example, how an entity joins the group, how its activity can be linked, and how it can be later identified must all be specified. Thus, this standard specifies methods for issuing, linking and opening.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent right have ensured the ISO and IEC that they are willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

— Electronics and Telecommunications Research Institute (ETRI)
161, Gajeong-dong, Yuseong-gu, Daejeon, 305-700, KOREA

— China IWNCOMM Co., LTD.
A201,QinFeng Ge, Xi’an Software Park, No.68 KeJi 2nd Road,
Xi’an Hi-tech Industrial Development Zone, Shaanxi, P.R.China 710075

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain online databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

