INTERNATIONAL STANDARD

ISO/IEC 9798-5

Third edition
2009-12-15

Information technology — Security techniques — Entity authentication —

Part 5: Mechanisms using zero-knowledge techniques

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

Partie 5: Mécanismes utilisant des techniques à divulgation nulle

Reference number
ISO/IEC 9798-5:2009(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.

ISO/IEC 9798-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 9798-5:2004), which has been technically revised. This edition adds a new mechanism based on elliptic curve discrete logarithm.

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

— *Part 1: General*

— *Part 2: Mechanisms using symmetric encipherment algorithms*

— *Part 3: Mechanisms using digital signature techniques*

— *Part 4: Mechanisms using a cryptographic check function*

— *Part 5: Mechanisms using zero-knowledge techniques*

— *Part 6: Mechanisms using manual data transfer*

Introduction

This part of ISO/IEC 9798 specifies authentication mechanisms that involve exchanges of information between a claimant and a verifier.

In accordance with the types of calculations that need to be performed by the claimant and the verifier, the mechanisms can be classified into the following four main groups (see Annex C).

— The first group (see Clauses 4 and 5) is characterized by the performance of short modular exponentiations. The challenge size needs to be optimized since it has a proportional impact on workloads.

— The second group (see Clauses 6 and 7 and 8) is characterized by the possibility of a "coupon strategy" for the claimant. A verifier can authenticate a claimant with very limited computational power. The challenge size has no practical impact on workloads.

— The third group (see 9.2) is characterized by the possibility of a coupon strategy for the verifier. A verifier with very limited computational power can authenticate a claimant. The challenge size has no impact on workloads.

— The fourth group (see 9.3) has no possibility of a coupon strategy.

ISO and IEC draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 9798 may involve the use of the following patents and their counterparts in other countries.

US 4 995 082 issued 1991-02-19, Inventor: C.P. Schnorr,

US 5 140 634 issued 1992-08-18, Inventors: L.C. Guillou and J-J. Quisquater,

EP 0 311 470 issued 1992-12-16, Inventors: L.C. Guillou and J-J. Quisquater,

EP 0 666 664 issued 1995-02-02, Inventor: M. Girault,

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

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applications 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 the companies listed overleaf.

RSA Security Inc. Attention General Counsel 174 Middlesex Turnpike Bedford, MA 01730, USA	US 4 995 082
France Telecom R&D Service PIV 38-40 Rue du Général Leclerc F 92794 Issy les Moulineaux Cedex 9, France	US 5 140 634, EP 0 311 470, EP 0 666 664
Philips International B.V. Corporate Patents and Trademarks P.O. Box 220 5600 AE Eindhoven, The Netherlands	US 5 140 634, EP 0 311 470
France Telecom claims that Patent Applications are pending in relation to Clauses 6 (GQ2) and 8 (GPS2). The Patent numbers will be provided when available. ISO/IEC will then request the appropriate statement.	

Information technology — Security techniques — Entity authentication —

Part 5: Mechanisms using zero-knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using zero-knowledge techniques:

— mechanisms based on identities and providing unilateral authentication;

— mechanisms based on integer factorization and providing unilateral authentication;

— mechanisms based on discrete logarithms with respect to numbers that are either prime or composite, and providing unilateral authentication;

— mechanisms based on asymmetric encryption systems and providing either unilateral authentication, or mutual authentication;

— mechanisms based on discrete logarithms on elliptic curves and providing unilateral authentication.

These mechanisms are constructed using the principles of zero-knowledge techniques, but they are not necessarily zero-knowledge according to the strict definition for every choice of parameters.

2 Terms and definitions

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

2.1
accreditation exponent
secret number related to the verification exponent and used in the production of private keys

2.2
adaptation parameter
public key specific to the modulus and used in the definition of public keys in the GQ2 mechanisms

2.3
asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation)

2.4
asymmetric encryption system
system based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption