

JTC 1

INTERNATIONAL STANDARD

ISO/IEC
9798-1

First edition
1991-09-01

Information technology — Security techniques — Entity authentication mechanisms —

Part 1: General model

*Technologies de l'information — Techniques de sécurité — Mécanismes
d'authentification d'entités —*

Partie 1: Modèle général



Reference number
ISO/IEC 9798-1:1991 (E)
AVA Documents
Document Sharing Hub

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. 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.

International Standard ISO/IEC 9798-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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

- *Part 1: General model*
- *Part 2: Entity authentication using symmetric techniques*
- *Part 3: Entity authentication using a public key algorithm*

Annex A of this part of ISO/IEC 9798 is for information only.

© ISO/IEC 1991

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Introduction

Entity authentication mechanisms allow the verification, of an entity's claimed identity, by another entity.

The authenticity of the entity can be ascertained only for the instant of the authentication exchange. To guarantee the authenticity of subsequent communicated data, the authentication exchange must be used in conjunction with a secure means of communication (e.g. an integrity service).

An impersonator may replay, at a later date, a valid authentication exchange (this is a form of masquerade). To prevent such a replay, a time variant parameter, such as a time stamp, a sequence number, or a challenge may be used.

Generally, for authentication purposes, the entities generate and exchange standardized messages, called tokens. It takes at least the exchange of one token for one of the entities to be authenticated by the other entity and at least the exchange of two tokens for mutual authentication. An additional token may be needed, if a challenge has to be sent to initiate the authentication exchange. Unilateral authentication provides one entity with assurance of the other's identity but not vice versa. Mutual authentication provides both entities with assurance of each other's identity.

