
**Information technology — Security
techniques — Entity authentication —**

Part 3:
Mechanisms using digital signature techniques

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

Partie 3: Mécanismes utilisant des techniques de signature numériques

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 9798-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-3:1993), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-3 (1st edition) will be compliant with ISO/IEC 9798-3 (2nd edition).

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*

Further parts may follow.

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

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, 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