INTERNATIONAL STANDARD

ISO/IEC 10181-4

First edition
1997-04-01

Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de non-répudiation

Reference number
ISO/IEC 10181-4:1997(E)

Contents

		Page
1	Scope	1
2	Normative references	2
	2.1 Identical Recommendations | International Standards	2
	2.2 Paired Recommendations | International Standards equivalent in technical content	2
3	Definitions	2
	3.1 Basic Reference Model definitions	2
	3.2 Security Architecture definitions	2
	3.3 Security Frameworks Overview definitions	3
	3.4 Additional definitions	3
4	Abbreviations	4
5	General discussion of Non-repudiation	4
	5.1 Basic concepts of Non-repudiation	4
	5.2 Roles of a Trusted Third Party	5
	5.3 Phases of Non-repudiation	5
	5.4 Some forms of Non-repudiation services	7
	5.5 Examples of OSI Non-repudiation evidence	8
6	Non-repudiation policies	8
7	Information and facilities	9
	7.1 Information	9
	7.2 Non-repudiation facilities	10
8	Non-repudiation mechanisms	12
	8.1 Non-repudiation using a TTP security token (secure envelope)	12
	8.2 Non-repudiation using security tokens and tamper-resistant modules	13
	8.3 Non-repudiation using a digital signature	13
	8.4 Non-repudiation using Time Stamping	13
	8.5 Non-repudiation using an in-line Trusted Third Party	14
	8.6 Non-repudiation using a Notary	14
	8.7 Threats to Non-repudiation	14

© ISO/IEC 1997

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

9 Interactions with other security services and mechanisms 16
9.1 Authentication 16
9.2 Access Control 16
9.3 Confidentiality 16
9.4 Integrity 16
9.5 Audit 16
Annex A – Non-repudiation in OSI Basic Reference Model 17
Annex B – Non-repudiation Facilities Outline 18
Annex C – Non-repudiation in store and forward systems 19
Annex D – Recovery in a Non-repudiation service 20
Annex E – Interaction with the Directory 22
Annex F – Bibliography 23