This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

STANDARD

10181-1

First edition
1996-08-01

Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadre pour la sécurité dans les systèmes ouverts: Présentation

Reference number
ISO/IEC 10181-1:1996(E)

This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

CONTENTS

		Page
1	Scope	1
2	Normative references	1
2.1	Identical Recommendations | International Standards	1
2.2	Paired Recommendations | International Standards equivalent in technical content	1
3	Definitions	2
3.1	Basic Reference Model definitions	2
3.2	Security architecture definitions	2
3.3	Additional definitions	2
4	Abbreviations	4
5	Notation	4
6	Organization	4
6.1	Part 1 – Overview	4
6.2	Part 2 – Authentication	4
6.3	Part 3 – Access control	5
6.4	Part 4 – Non-repudiation	5
6.5	Part 5 – Confidentiality	5
6.6	Part 6 – Integrity	6
6.7	Part 7 – Security audit and alarms	6
6.8	Key management	6
7	Common concepts	6
7.1	Security information	7
7.2	Security domain	7
7.2.1	Security policy and security policy rules	7
7.2.2	Security domain authority	8
7.2.3	Inter-relationships among security domains	8
7.2.4	Establishment of secure interaction rules	9
7.2.5	Inter-domain security information transfer	9
7.3	Security policy considerations for specific security services	9
7.4	Trusted entities	9
7.5	Trust	10
7.6	Trusted third parties	10
8	Generic security information	10
8.1	Security labels	10
8.2	Cryptographic checkvalues	11
8.3	Security certificates	11
8.3.1	Introduction to security certificates	11
8.3.2	Verification and chaining of security certificates	12
8.3.3	Revocation of security certificates	12
8.3.4	Re-use of security certificates	12
8.3.5	Security certificate structure	12
8.4	Security tokens	13

© ISO/IEC 1996

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 micro-film, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

9 Generic security facilities 13
9.1 Management related facilities 13
9.1.1 Install SI 13
9.1.2 Deinstall SI 13
9.1.3 Change SI 13
9.1.4 Validate SI 14
9.1.5 Invalidate SI 14
9.1.6 Disable/Re-enable security service 14
9.1.7 Enrol 14
9.1.8 Un-enrol 14
9.1.9 Distribute SI 14
9.1.10 List SI 14
9.2 Operational related facilities 14
9.2.1 Identify trusted security authorities 14
9.2.2 Identify secure interaction rules 14
9.2.3 Acquire SI 14
9.2.4 Generate SI 14
9.2.5 Verify SI 15
10 Interactions between security mechanisms 15
11 Denial of service and availability 15
12 Other requirements 16
Annex A – Some examples of protection mechanisms for security certificates 17
A.1 Protection using an OSI communications security service 17
A.2 Protection using a parameter within the security certificate 17
A.2.1 The authentication method 17
A.2.2 The secret key method 17
A.2.3 The public key method 18
A.2.4 The one-way function method 18
A.3 Protection of the internal and external parameters while in transit 18
A.3.1 Transfer of internal parameters to the issuing security authority 18
A.3.2 Transfer of external parameters among entities 18
A.4 Use of security certificates by single entities or by groups of entities 19
A.5 Linking a security certificate with accesses 19
Annex B – Bibliography 20

This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

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 10181-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.810.

ISO/IEC 10181 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Security frameworks for open systems*:

— *Part 1: Overview*

— *Part 2: Authentication framework*

— *Part 3: Access control framework*

— *Part 4: Non-repudiation framework*

— *Part 5: Confidentiality framework*

— *Part 6: Integrity framework*

— *Part 7: Security audit and alarms framework*

Annexes A and B of this part of ISO/IEC 10181 are for information only.

This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

Introduction

Many applications have requirements for security to protect against threats to the communication of information. Some commonly known threats, together with the security services and mechanisms that can be used to protect against them are described in CCITT Rec. X.800 | ISO 7498-2.

This Recommendation | International Standard defines the framework within which security services for open systems are specified.

This is a preview of "ISO/IEC 10181-1:1996". Click here to purchase the full version from the ANSI store.

This page intentionally left blank