

TECHNICAL REPORT

**ISO/IEC
TR
14516**

First edition
2002-06-15

Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour l'emploi et la gestion des services TTP*



Reference number
ISO/IEC TR 14516:2002(E)

© ISO/IEC 2002

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2002

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 either ISO at the address below or ISO's member body in the country of the requester.

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.ch
Web www.iso.ch

Printed in Switzerland

CONTENTS

	<i>Page</i>
1 Scope	1
2 References.....	1
2.1 Identical Recommendations International Standards.....	1
2.2 Paired Recommendations International Standards equivalent in technical content.....	1
2.3 Additional References	1
3 Definitions.....	2
4 General Aspects.....	3
4.1 Basis of Security Assurance and Trust.....	3
4.2 Interaction between a TTP and Entities Using its Services	4
4.2.1 In-line TTP Services	4
4.2.2 On-line TTP Services.....	4
4.2.3 Off-line TTP Services.....	5
4.3 Interworking of TTP Services	5
5 Management and Operational Aspects of a TTP	5
5.1 Legal Issues	6
5.2 Contractual Obligations.....	6
5.3 Responsibilities.....	7
5.4 Security Policy.....	7
5.4.1 Security Policy Elements	8
5.4.2 Standards.....	8
5.4.3 Directives and Procedures.....	8
5.4.4 Risk Management	8
5.4.5 Selection of Safeguards.....	9
5.4.5.1 Physical and Environmental Measures	9
5.4.5.2 Organisational and Personnel Measures	9
5.4.5.3 IT Specific Measures.....	9
5.4.6 Implementation Aspects of IT Security.....	10
5.4.6.1 Awareness and Training	10
5.4.6.2 Trustworthiness and Assurance.....	10
5.4.6.3 Accreditation of TTP Certification Bodies.....	11
5.4.7 Operational Aspects of IT Security.....	11
5.4.7.1 Audit/Assessment.....	11
5.4.7.2 Incident Handling.....	12
5.4.7.3 Contingency Planning.....	12
5.5 Quality of Service	12
5.6 Ethics	12
5.7 Fees	12
6 Interworking.....	12
6.1 TTP-Users	13
6.2 User-User	13
6.3 TTP-TTP	13
6.4 TTP-Law Enforcement Agency.....	14
7 Major Categories of TTP Services.....	14
7.1 Time Stamping Service	14
7.1.1 Time Stamping Authority.....	14
7.2 Non-repudiation Services	15
7.3 Key Management Services	16
7.3.1 Key Generation Service	16
7.3.2 Key Registration Service.....	16
7.3.3 Key Certification Service.....	16
7.3.4 Key Distribution Service.....	17
7.3.5 Key Installation Service.....	17
7.3.6 Key Storage Service.....	17
7.3.7 Key Derivation Service.....	17
7.3.8 Key Archiving Service.....	17

7.3.9	Key Revocation Service	17
7.3.10	Key Destruction Service	17
7.4	Certificate Management Services	18
7.4.1	Public Key Certificate Service	18
7.4.2	Privilege Attribute Service	18
7.4.3	On-line Authentication Service Based on Certificates	19
7.4.4	Revocation of Certificates Service	19
7.5	Electronic Notary Public Services	19
7.5.1	Evidence Generation Service	20
7.5.2	Evidence Storage Service	20
7.5.3	Arbitration Service	20
7.5.4	Notary Authority	20
7.6	Electronic Digital Archiving Service	21
7.7	Other Services	22
7.7.1	Directory Service	22
7.7.2	Identification and Authentication Service	23
7.7.2.1	On-line Authentication Service	23
7.7.2.2	Off-line Authentication Service	25
7.7.2.3	In-line Authentication Service	25
7.7.3	In-line Translation Service	25
7.7.4	Recovery Services	25
7.7.4.1	Key Recovery Services	25
7.7.4.2	Data Recovery Services	26
7.7.5	Personalisation Service	26
7.7.6	Access Control Service	26
7.7.7	Incident Reporting and Alert Management Service	26
	Annex A – Security Requirements for Management of TTPs	28
	Annex B – Aspects of CA management	29
B.1	Example of Registration Process Procedures	29
B.2	An example of requirements for Certification Authorities	29
B.3	Certification Policy and Certification Practice Statement (CPS)	31
	Annex C – Bibliography	32

Table of Figures

Figure 1 – In-line TTP Service Between Entities	4
Figure 2 – On-line TTP Service Between Entities	5
Figure 3 – Off-line TTP Service Between Entities	5
Figure 4 – Interworking of TTPs in Different Domains	13
Figure 5 – Example of Non-repudiation Architecture	16
Figure 6 – Link Between an Attribute Certificate and a Public Key Certificate	19
Figure 7 – Directory Service Architecture	23
Figure 8 – Example for On-line Authentication Services	24
Figure 9 – Example for In-line TTP Authentication Service	25
Figure 10 – Example of Alert Management Service	27

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 3.

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.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 14516, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.842.

Introduction

Achievement of adequate levels of business confidence in the operation of IT systems is underpinned by the provision of practical and appropriate legal and technical controls. Business must have confidence that IT systems will offer positive advantages and that such systems can be relied upon to sustain business obligations and create business opportunities.

An exchange of information between two entities implies an element of trust, e.g. with the recipient assuming that the identity of the sender is in fact the sender, and in turn, the sender assuming that the identity of the recipient is in fact the recipient for whom the information is intended. This "implied element of trust" may not be enough and may require the use of a Trusted Third Party (TTP) to facilitate the trusted exchange of information.

The role of TTPs includes providing assurance that business and other trustworthy (e.g. governmental activities) messages and transactions are being transferred to the intended recipient, at the correct location, that messages are received in a timely and accurate manner, and that for any business dispute that may arise, there exist appropriate methods for the creation and delivery of the required evidence for proof of what happened. Services provided by TTPs may include those necessary for key management, certificate management, identification and authentication support, privilege attribute service, non-repudiation, time stamping services, electronic public notary services, and directory services. TTPs may provide some or all of these services.

A TTP has to be designed, implemented and operated to provide assurance in the security services it provides, and to satisfy applicable legal and regulatory requirements. The types and levels of protection adopted or required will vary according to the type of service provided and the context within which the business application is operating.

The objectives of this Recommendation | Technical Report are to provide:

- a) Guidelines to TTP managers, developers and operations' personnel and to assist them in the use and management of TTPs; and
- b) Guidance to entities regarding the services performed by TTPs, and the respective roles and responsibilities of TTPs and entities using their services.

Additional aspects covered by this Recommendation | Technical Report are to provide:

- a) An overview of the description of services provided;
- b) An understanding of the role of TTPs and their functional features;
- c) To provide a basis for the mutual recognition of services provided by different TTPs; and
- d) Guidance of interworking between entities and TTPs.

TECHNICAL REPORT

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDELINES FOR THE USE AND MANAGEMENT OF TRUSTED THIRD PARTY SERVICES

1 Scope

Associated with the provision and operation of a Trusted Third Party (TTP) are a number of security-related issues for which general guidance is necessary to assist business entities, developers and providers of systems and services, etc. This includes guidance on issues regarding the roles, positions and relationships of TTPs and the entities using TTP services, the generic security requirements, who should provide what type of security, what the possible security solutions are, and the operational use and management of TTP service security.

This Recommendation | Technical Report provides guidance for the use and management of TTPs, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. It is intended primarily for system managers, developers, TTP operators and enterprise users to select those TTP services needed for particular requirements, their subsequent management, use and operational deployment, and the establishment of a Security Policy within a TTP. It is not intended to be used as a basis for a formal assessment of a TTP or a comparison of TTPs.

This Recommendation | Technical Report identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public. Each of these major categories consists of several services which logically belong together.

2 References

2.1 Identical Recommendations | International Standards

- IT U-T Recommendation X.509 (2001) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

2.3 Additional References

- ISO/IEC 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General*.
- ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*.
- ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*.
- ISO/IEC 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.
- ISO/IEC TR 13335-1:1996, *Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security*.