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 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

Table of Figures

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.*

- ISO/IEC TR 13335-2:1997, *Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security.*
- ISO/IEC TR 13335-3:1998, *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security.*
- ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards.*
- ISO/IEC 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General.*
- ISO/IEC 13888-2:1998, *Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques.*
- ISO/IEC 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.*
- ISO/IEC WD 15443, *Information technology – Security techniques – A framework for IT security assurance.*