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.*

3 Definitions

NOTE – Throughout this Recommendation | Technical Report the term entity may refer to a human being, an organisation, a hardware component or a piece of software.

For the purpose of this Recommendation | Technical Report the definitions given in CCITT Rec. X.800 and ISO 7498-2 apply: access control, accountability, audit, audit trail log, availability, confidentiality, data integrity, decipherment, digital signature, encipherment, entity authentication, integrity, key, key management, notarisation, non-repudiation, security audit, security audit trail and signature.

For the purpose of this Recommendation | Technical Report the definitions given in ISO 8402 apply: audit/ assessment.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.509 | ISO/IEC 9594-8 apply: attribute certificate, certificate and certification authority (CA).

For the purpose of this Recommendation | Technical Report the definition given in ISO/IEC 9798-1 applies: token.

For the purpose of this Recommendation | Technical Report the definition given in ISO/IEC 9798-5 applies: accreditation authority.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.810 | ISO/IEC 10181-1 apply: private key, public key, seal, secret key and trusted third party.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.811 | ISO/IEC 10181-2 apply: authentication certificate and authentication information (AI).

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.813 | ISO/IEC 10181-4 apply: evidence generator and notary.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC 11770-1 apply: asymmetric cryptographic technique, symmetric cryptographic technique and time stamp.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC TR 13335-1 apply: asset, authenticity, impact, IT security, IT security policy, reliability, residual risk, risk, risk analysis, risk management, safeguard, system integrity, threat and vulnerability.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC 13888-1 apply: non-repudiation of approval, non-repudiation of creation, non-repudiation of delivery, non-repudiation of knowledge, non-repudiation of origin, non-repudiation of receipt, non-repudiation of sending, non-repudiation of submission, and non-repudiation of transport.

For the purpose of this Recommendation | Technical Report the following additional definitions apply:

3.1 attribute Authority (AA): An entity trusted by one or more entities to create and sign attribute certificates. Note that a CA may also be an AA.

3.2 registration Authority (RA): An entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both.

4 General Aspects

A Trusted Third Party (TTP) is an organisation or its agent that provides one or more security services, and is trusted by other entities with respect to activities related to these security services.

A TTP is used to offer value-added services to entities wishing to enhance the trust and business confidence in the services that they receive and to facilitate secure communications between business trading partners. TTPs need to offer value with regard to confidentiality, integrity and availability of the services and information involved in the communications between business applications. TTPs should be able to interoperate with each other and with the entities.

Entities should be able to choose which TTP they will use to provide the required services. Also, TTPs should be able to choose the entities to which they will provide services.

To be effective, TTPs generally should:

a) operate within a legal framework which is consistent among the participating entities;

b) offer a range of services, with minimum services clearly defined;

c) have defined policies, in particular a public security policy;

d) be managed and operated in a secure and reliable manner, based on an information security management system and trustworthy IT systems;

e) conform to national and international standards, where applicable;

f) follow an accepted best code of practice;

g) publish practice statements;

h) record and archive all evidence relevant to their services;

i) allow for independent arbitration, without compromising security;

j) be independent and impartial in their operation, (e.g. accreditation rules); and

k) assume responsibility of liability within defined limits for availability and quality of service.

4.1 Basis of Security Assurance and Trust

The use of a TTP and its services depends on the fundamental observation that the services provided by the TTP will be trusted by other TTPs and entities. This trust results from the confidence that the TTP is managed correctly and its services are operated securely. Therefore it should give assurance that the TTP itself and the services it provides are according to the defined policies. Especially, the security policy should cover all security aspects related to the management of the TTP and the operation of the services.

The confidence can be established through evidence of the management and operational TTP aspects. Evidence should be given that the management aspects are proper and sufficient to completely achieve the objectives, that the management system is effective, suitable to minimise risks and to counter threats, and the safeguards are documented and understood by personnel, not outdated or superseded and are implemented properly.

To gain confidence in the management and operational aspects a TTP especially should provide evidence that:

a) there is an appropriate Security Policy in place;

b) security problems have been addressed by a combination of correctly implemented security procedures and mechanisms;

c) the operations are being carried out correctly and in keeping with a clearly defined set of roles and responsibilities;

d) the interfaces and procedures for communicating with entities are appropriate for the functions to be performed and are correctly used;

e) rules and regulations are followed by management and staff, and are consistent with a stated or targeted level of trustworthiness;

f) the quality of the processes, operations and working practices have been suitably accredited;

g) the TTP meets its contractual obligations according to a formal contract with its users;

h) there is a clear understanding and acceptance of the liability aspects;

i) compliance with laws and regulations is maintained and audited;

j) known threats and safeguards to mitigate those threats are clearly identified;

k) a Threat and Risk Assessment is done initially and reviewed/updated on a regular basis to ensure that confidentiality, integrity, availability and reliability requirements are met;

l) proper organisational and personnel measures are met;

m) the trustworthiness of the TTP can be relied upon and that it can be checked and verified, and

n) that the TTP is monitored by some type of administrative authority to oversee that its operation is within its accreditation rules.

Details are discussed in clause 5, Management and Operational Aspects of a TTP.

Different types of business and different applications will require different levels of trust and may require different levels of strength for the applied protection mechanisms and procedures. For example, the level of trust required for the authentication of administrative transactions may be different from that required for financial transactions, which may be different from that required in some military applications. Different levels of trust result from different security policies and standards and how well they are correctly implemented.

4.2 Interaction between a TTP and Entities Using its Services

From a communication point of view the location of the TTP and entities can be arranged in different configurations: in-line, on-line and off-line. An example of each configuration is given in 4.2.1 through 4.2.3.

Some TTP services may be based on different configurations, therefore the configuration that is adopted will influence the services the TTP will be capable of fulfilling, e.g. timeliness of the exchange, denial of service, recording of proof, and their characteristics, such as delay of revocation of a certificate.

4.2.1 In-line TTP Services

An in-line TTP is needed when two or more entities belong to different security domains and do not use the same security mechanisms. In this case the entities are unable to operate direct, secure exchanges. However, a TTP positioned directly in the communication path between the entities can facilitate secure exchanges between these entities as illustrated in Figure 1.

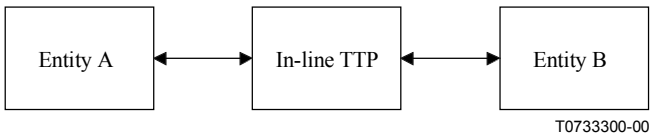

Figure 1 – In-line TTP Service Between Entities

In-line TTP services may include authentication, translation and privilege attribute services, and the TTP may play a role in providing non-repudiation, access control, key recovery, confidentiality and integrity services of transmitted data.

4.2.2 On-line TTP Services

When one or both entities request an on-line TTP to provide or register security-related information, the TTP is involved in all first time secure exchanges between the entities. However, the TTP is not required for follow-up exchanges and is not positioned in the communication path between the entities as illustrated in Figure 2.

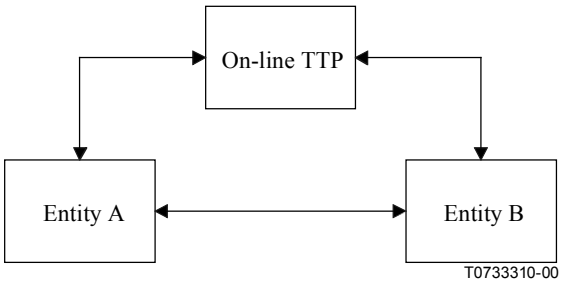

Figure 2 – On-line TTP Service Between Entities

On-line TTP services may include authentication, certification and privilege attribute services, and the TTP may play a role in providing non-repudiation, access control, key management, delivery of messages, time stamping, confidentiality and integrity services.

4.2.3 Off-line TTP Services

A third type of configuration for the provision of TTP services is Off-line. The TTP does not interact directly with the entities during the process of secure exchanges between the entities. Instead data generated previously by the TTP is used by the entities as illustrated in Figure 3 with the dotted lines.

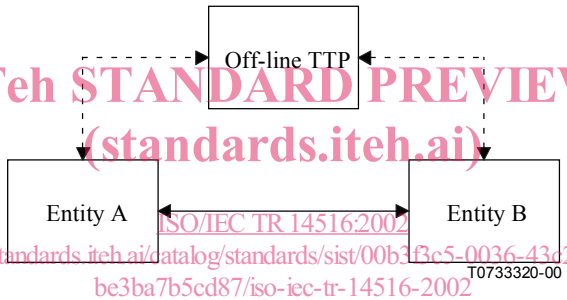

Figure 3 – Off-line TTP Service Between Entities

Off-line TTP services may include authentication, certification, privilege attribute, non-repudiation, key distribution and key recovery services.

4.3 Interworking of TTP Services

A TTP can offer several services, which are described in clause 7. All services may be provided by a single TTP or they may be provided by more than one TTP. The services can also be provided from one or more locations. In the latter case the tasks and duties should be defined and stated in a formal contract, and the technical and organisational impacts should be taken into account. Depending on the TTP architecture (responsibility and location) there may be additional requirements, especially security related ones, that should be considered by the TTP management.

NOTE – Each service may have specific security requirements that should be fulfilled. Where possible, it is generally recommended to split the management and operational aspects of a TTP into general and specific aspects related to each service. A modular structured management system is much more easily handled if changes occur, especially the identification of security critical impacts when changes are made.

5 Management and Operational Aspects of a TTP

For the management and operation of a TTP there should exist an umbrella strategy which takes into account the issues in the following subclauses. The commitment of a TTP to provide security related services should take the form of a formal documented policy. It is recommended that a TTP should use guidelines for the protection of its services. General guidelines for the management of IT security (GMITS) can be found in ISO/IEC TR 13335-1, 13335-2, 13335-3 and 13335-4 in Annexes A-H of 13335-4.

Depending on the services provided by a TTP there are a lot of decisions that have to be made. There is a need not only to define policies for the services, but also to define more specific policies, such as signature creation and validation policies. Both will lead to technical implications and consequences that should be considered in advance. Additionally there are dependencies between technical and non-technical equipment, e.g. the provision of directory services via the Online Certificate Status Protocol or the Certificate Revocation List. All those factors will lead to technical implementations and consequences that should be reflected in advance. An example of a security policy which deals with public key certificates can be found in RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

5.1 Legal Issues

In addition to the basic accuracy of the particular services provided, e.g. accurate time for a time stamping authority, a TTP will inherit broad-ranging responsibilities from the expectations of its users. These responsibilities will include flawless provisions for confidentiality, integrity, availability, access control, accountability, authenticity, reliability, privacy, ethical (such as legitimate use), legal (i.e. laws and regulations), techniques and mechanisms, and financial aspects. Accidental or deliberate breaches of these responsibilities by a TTP may lead to substantial loses by its users, who will attempt to recover these losses from the TTP. In order to manage the expectations of its users and limit its liability, a clearly defined, legally binding contract between the TTP and its users should be established. As a minimum this contract should address the legal issues for the following topics:

a) liability;

b) privacy, especially with the respect to data protection law;

c) copyright and intellectual property;

d) use of cryptography;

e) lawful interception and lawful access;

f) legality of a binding service such as digital signatures;

g) anonymity of entities;

h) right to investigate, e.g. credentials;

i) legislative and regulatory requirements applicable to the jurisdiction and industry;

j) the types of service to be provided;

k) access arrangements including permitted methods of access, procedures by which users can be authorised (and authorised users changed);

l) procedures for problem resolution (including authorised points of contact);

m) responsibilities concerning hardware and software requirements, management and change control; and

n) arrangements for reporting, notification, and investigation of security incidents.

The TTP's commitments and liability should be consistent with its financial capacity and warrants or pledges it received from other entities. Entities should have a commitment that the information they provide to a TTP is protected from disclosure, unless otherwise specified within their contract. Legal demands for protecting personal information have to be met by a TTP, especially those relating to the appropriate technical and organisational protection of databases containing personal data.

Electronic commerce is international by nature and TTPs should comply with all legal obligations with respect to national and international laws, regulations and treaties. Compliance with some of these obligations may have a significant impact on the design or the implementation of a TTP.

The concepts of liability, and the basic legal framework may differ from nation to nation. Therefore, general guidance will need to be adapted to meet the needs of individual legal systems. In cases where national legislation regarding TTPs is not consistent across national boundaries, TTPs who wish to allow their users to communicate across these boundaries, should have a special contractual agreement in place to address cross-jurisdictional differences.

When TTPs are interworking across national boundaries they have to be aware of the legal consequences in such an environment with regard to the potential differences or incompatibilities between their security policies and practice statements.

5.2 Contractual Obligations

Formal contracts between a TTP and entities using its services should clearly state the responsibilities of the TTP, the quality of the service to be provided, as well as the responsibilities of the entities using TTP services.

The contract should explain the managerial and organisational policy of the TTP, as well as the operational procedures. The TTP should also issue a Practice Statement that describes what entities may expect from the TTP services in order to clearly define publicly the operational aspects and requirements, quality of service, ethical issues, and subscriber's fees.

The contract should specify provisions clearly describing how the TTP complies with relevant legislation and regulations. The contract should specify the jurisdiction of operation and the jurisdiction under which disputes will be resolved.

Accidental or deliberate errors by a TTP may lead to substantial damage to business. In order to have sufficient confidence to use TTP services, the contract should define the limits of the TTP's liability with its users. Where applicable, the liability should be covered by an appropriate insurance contract in case of a dispute. The required coverage should be defined in the contract between the TTP and its users.

The contract should include a list of all matters concerning liabilities between the TTP and its users so that the users can access adequate professional advice in order to obtain appropriate legal assistance on any matter arising from the provision and use of the TTP's services.

The contract should describe the intended uses of the service and its service parameters, and should enable the service to be withdrawn if either contracting party is using it improperly or illegally.

The contract could have provisions that clearly state that an independent and impartial party (arbitrator) may be requested to assist in dispute resolution between the TTP and its users.

The contract should specify how the privacy of personal and other sensitive information will be protected, and the circumstances under which disclosure may occur.

5.3 Responsibilities

A TTP should define the extent to which responsibility is taken for the secure operation of its service. In addition, the TTP should delineate the extent of the liabilities that may be accepted in respect of security breaches.

The responsibilities of the TTP, as well as those of the user, should be clearly stated in any formal contract that is set up between the user and the TTP. Most responsibilities should be part of a contract, and some should at least be defined as a matter of business, while others should be standard qualities of service.

Other documents, such as those containing the definition of the services to be provided, the service agreement and any technical annexes included as attachments to the contract, also determine respective responsibilities of the various entities involved. These documents form part of the overall contractual agreement.

5.4 Security Policy

A TTP undertakes certain obligations in offering and operating security related services, based on confidence and trust in the services being offered, and a formal documented security policy for the organisation offering the service.

A TTP's security policy is a vital instrument to describe all essential and important activities in order to establish trust, and to gain confidence in the management of the TTP and the operation of its services. Therefore, a TTP security policy should not only cover specific security issues but also contain all TTP service related aspects. The development and maintenance of a TTP's security policy should be done in a systematic and logical manner.

As discussed in ISO/IEC TR 13335-3, Annex A, a TTP's security policy should consist of two parts:

a) a general security policy which expresses concisely the non-technical aspects regarding security and confidence in the TTP services; and

b) a technical security policy which expresses concisely all technical aspects regarding security related functionality and trust together with descriptions of routines, procedures, etc. related to technical aspects.

A rigorous security related evaluation of current TTP services verifies the confidence in the technical systems according to the measure of confidence in the TTP's security policy.

A TTP's security policy is of vital importance in maintenance of confidence between systems, in specifying the basis for continuous (internal) review and periodical (internal and external) audit of security, and confidence to the systems and the organisation which operates the service.

The commitment of a TTP to provide a security related service should take the form of a formal and documented security policy. The security policy should identify all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats. It should describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted.