INTERNATIONAL STANDARD

ISO/IEC 15945

First edition
2002-02-01

Information technology — Security techniques — Specification of TTP services to support the application of digital signatures

Technologies de l'information — Techniques de sécurité — Spécifications des services TTP pour supporter l'application des signatures numériques

Reference number
ISO/IEC 15945:2002(E)

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 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

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.

Attention is drawn to the possibility that some of the elements of this International Standard 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 15945 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.843.

Annexes A to C of this International Standard are for information only.

Introduction

Today the development of information technology, as well as that of the worldwide communication infrastructure, opens the possibility to implement electronic commerce in economically relevant dimensions. Digital signatures are an important technique to add security to these commercial applications and to other application fields with a need for legally effective electronic transactions.

Digital signatures are suitable to assure the integrity of data and the authentication of participants in transactions. They can supply an analogue of the handwritten signature for digital orders, offers and contracts. The most important property of digital signatures in this context is that a person who signed a document cannot successfully deny this fact. This property is called "non-repudiation of creation" of a document.

In several countries and in international contexts, legislation concerning digital signatures is being pushed forward with the aim to support the development of electronic commerce and other application fields with a need for legally effective electronic transactions.

A number of standards exist that specify digital signatures, as well as their use for different purposes, like non-repudiation or authentication. A number of commercial applications, as well as TTPs offering services in connection with digital signatures, are implemented or planned. Interoperability of these TTPs, among each other and with the commercial applications, is needed for an economically and legally effective worldwide use of digital signatures.

The goal of this Recommendation | International Standard is to define the services required to support the application of digital signatures for non-repudiation of creation. Since the use of digital signature mechanisms for non-repudiation of creation of a document implies integrity of the document and authenticity of the creator, the services described in this Recommendation | International Standard can also be combined to implement integrity and authenticity services. This is done in a way to promote interoperability among TTPs as well as between TTPs and commercial applications.

NOTE – There is no inherent reason why every TTP planning to support the application of digital signatures should be required to offer all of these services. It is possible that a number of TTPs offering different services cooperate in supporting the use of digital signatures. But, from the view of the potential commercial applications, the whole range of the services may be required and interoperability becomes even more important in this scenario. This is an additional justification to collect all these services together in one document.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – SPECIFICATION OF TTP SERVICES TO SUPPORT THE APPLICATION OF DIGITAL SIGNATURES

1 Scope

This Recommendation | International Standard will define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents.

This Recommendation | International Standard will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.

Definitions of technical services and protocols are required to allow for the implementation of TTP services and related commercial applications.

This Recommendation | International Standard focuses on:

- implementation and interoperability;
- service specifications; and
- technical requirements.

This Recommendation | International Standard does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in ITU-T Rec. X.842 | ISO/IEC TR 14516, *Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services*.

NOTE 1 – Because interoperability is the main issue of this Recommendation | International Standard, the following restrictions hold:

i) Only those services which may be offered by a TTP, either to end entities or to another TTP, are covered in this Recommendation | International Standard.

ii) Only those services which may be requested and/or delivered by means of standardizable digital messages are covered.

iii) Only those services for which widely acceptable standardized messages can be agreed upon at the time this Recommendation | International Standard is published are specified in detail.

Further services will be specified in separate documents when widely acceptable standardized messages are available for them. In particular, time stamping services will be defined in a separate document.

NOTE 2 – The data structures and messages in this Recommendation | International Standard will be specified in accordance to RFC documents, RFC 2510 and RFC 2511 (for certificate management services) and to RFC 2560 (for OCSP services). The certificate request format also allows interoperability with PKCS#10. See Annex C for references to the documents mentioned in this Note.

NOTE 3 – Other standardization efforts for TTP services in specific environments and applications, like SET or EDIFACT, exist. These are outside of the scope of this Recommendation | International Standard.

NOTE 4 – This Recommendation | International Standard defines technical specifications for services. These specifications are independent of policies, specific legal regulations, and organizational models (which, for example, might define how duties and responsibilities are shared between Certification Authorities and Registration Authorities). Of course, the policy of TTPs offering the services described in this Recommendation | International Standard will need to specify how legal regulations and the other aspects mentioned before will be fulfilled by the TTP. In particular, the policy has to specify how the validity of digital signatures and certificates is determined.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1998, *Information technology – Open Systems Interconnection – The Directory: Models*.
- ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6:1998, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- 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 Additional references

- ISO/IEC 9796-2:1997, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function*.
- ISO/IEC 9796-3:2000, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.
- ISO/IEC 10118-1:1994, *Information technology – Security techniques – Hash-functions – Part 1: General*.
- ISO/IEC 10118-2:1994, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm*.
- ISO/IEC 10118-3:1998, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.
- 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 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 14888-1:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

– ISO/IEC 14888-2:1999, *Information technology – Security techniques – Digital signatures with appendix – Part 2: Identity-based mechanisms*.

– ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

– ISO/IEC 15946-2 (to be published), *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.