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)

© 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.

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.