Second edition
2009-10-15

Certificate management for financial services —

Part 1: Public key certificates

Gestion de certificats pour les services financiers —

Partie 1: Certificats de clé publique

Reference number
ISO 15782-1:2009(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.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO 15782-1 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 15782-1:2003), which has been technically revised.

ISO 15782 consists of the following parts, under the general title *Certificate management for financial services*:

— *Part 1: Public key certificates*

— *Part 2: Certificate extensions*

Introduction

This part of ISO 15782 adopts ISO/IEC 9594-8 for the financial services industry and defines certificate management procedures and data elements.

Detailed requirements for the financial industry for the individual extensions are given in ISO 15782-2.

While the techniques specified in this part of ISO 15782 are designed to maintain the integrity of financial messages and support the service of non-repudiation, this part of ISO 15782 does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented, with these controls including the application of appropriate audit tests in order to validate compliance.

The binding association between the identity of the owner of a public key and that key is documented in order to prove the ownership of the corresponding private key. This binding is called a public key certificate. Public key certificates are generated by a trusted entity known as a Certification Authority (CA).

The proper implementation of this part of ISO 15782 is intended to provide assurances of the binding of the identity of an entity to the key used by that entity to sign documents, including wire transfers and contracts.

This part of ISO 15782 defines a certificate management framework for authentication, including the authentication of keys for encryption. The techniques specified by this part of ISO 15782 can be used when initiating a business relationship between legal entities (entities).