INTERNATIONAL STANDARD

ISO 21188

First edition
2006-05-01

Public key infrastructure for financial services — Practices and policy framework

Infrastructure de clé publique pour services financiers — Pratique et cadre politique

Reference number
ISO 21188:2006(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 21188 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

Introduction

Institutions and intermediaries are building infrastructures to provide new electronic financial transaction capabilities for consumers, corporations and government entities. As the volume of electronic financial transactions continues to grow, advanced security technology using digital signatures and authority systems can become part of the financial transaction process. Financial transaction systems incorporating advanced security technology have requirements to ensure the privacy, authenticity and integrity of financial transactions conducted over communications networks.

The financial services industry relies on several time-honoured methods of electronically identifying, authorizing and authenticating entities and protecting financial transactions. These methods include, but are not limited to, Personal Identification Numbers (PINs) and Message Authentication Codes (MACs) for retail and wholesale financial transactions, user IDs and passwords for network and computer access, and key management for network connectivity. Over the last twenty years the financial services industry has developed risk management processes and policies to support the use of these technologies in financial applications.

The expanded use of Internet technologies by the financial services industry and the needs of the industry in general to provide safe, private and reliable financial transaction and computing systems have given rise to advanced security technology incorporating public key cryptography. Public key cryptography requires a business-optimized infrastructure of technology, management and policy (a public key infrastructure or PKI, as defined in this document) to satisfy requirements of electronic identification, authentication, message integrity protection and authorization in financial application systems. The use of standard practices for electronic identification, authentication and authorization in a PKI ensures more consistent and predictable security in these systems and confidence in electronic communications. Confidence (e.g. trust) can be achieved when compliance to standard practices can be ascertained.

Applications serving the financial services industry can be developed with digital signature and PKI capabilities. The safety and the soundness of these applications are based, in part, on implementations and practices designed to ensure the overall integrity of the infrastructure. Users of authority-based systems that electronically bind the identity of individuals and other entities to cryptographic materials (e.g. cryptographic keys) benefit from standard risk management systems and the base of auditable practices defined in this International Standard.

Members of the International Organization of Standardization Technical Committee 68 have made a commitment to public key technology by developing technical standards and guidelines for digital signatures, key management, certificate management and data encryption. ISO 15782 parts 1 and 2 define a certificate management system for financial industry use, but does not include certificate policy and certification practices requirements. This International Standard complements ISO 15782 parts 1 and 2 by providing a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures. For implementers of these International Standards, the degree to which any entity in a financial transaction can rely on the implementation of public key infrastructure standards and the extent of interoperability between PKI-based systems using these International Standards will depend partly on factors relative to policy and practices defined in this document.

Public key infrastructure for financial services — Practices and policy framework

1 Scope

This International Standard sets out a framework of requirements to manage a PKI through certificate policies and certification practice statements and to enable the use of public key certificates in the financial services industry. It also defines control objectives and supporting procedures to manage risks.

This International Standard draws a distinction between PKI systems used in open, closed and contractual environments. It further defines the operational practices relative to financial services industry accepted information systems control objectives. This International Standard is intended to help implementers to define PKI practices that can support multiple certificate policies that include the use of digital signature, remote authentication and data encryption.

This International Standard facilitates the implementation of operational, baseline PKI control practices that satisfy the requirements for the financial services industry in a contractual environment. While the focus of this International Standard is on the contractual environment, application of this document to other environments is not specifically precluded. For the purposes of this document, the term “certificate” refers to public key certificates. Attribute certificates are outside the scope of this International Standard.

This International Standard is targeted for several audiences having dissimilar needs and therefore the use of this document will have a different focus for each.

Business Managers and Analysts are those who require information regarding using PKI technology in their evolving businesses (e.g., electronic commerce) and should focus on Clauses 1 to 6.

Technical Designers and Implementers are those who are writing their certificate policy(ies) and certification practice statement(s) and should focus on Clauses 6 to 8 and Annexes A to F.

Operational Management and Auditors are those who are responsible for day-to-day operations of the PKI and validating compliance to this document and should focus on Clauses 6 to 8.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7810, *Identification cards — Physical characteristics*

ISO/IEC 7811, *Identification cards — Recording technique* (parts 1 to 5)

ISO/IEC 7813, *Identification cards — Financial transaction cards*

ISO/IEC 7816, *Identification cards — Integrated circuit cards* (parts 1 to 12 and 15)

ISO/IEC 9594-8:1995, *Information Technology — Open Systems Interconnection — The Directory: Authentication Framework*

ISO/IEC 9834-1:1993, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General procedures — Part 1*

ISO 10202, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards* (eight parts)

ISO/IEC 10646-1, *Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane*

ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security (three parts)*

ISO 15782-1:2003, *Certificate management for financial services — Part 1: Public key certificates*

ISO 15782-2, *Banking — Certificate Management — Part 2: Certificate Extensions*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

ISO 18014-2, *Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens*

ISO 18014-3, *Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens*

ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

ISO 18033, *Information technology — Security techniques — Encryption algorithms* (parts 1 to 4)

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
activation data
data values, other than keys, which are required to operate cryptographic modules and which need to be protected (e.g. a PIN, a pass phrase, a biometric, or a manually held key share)

3.2
authentication
verification of an individual's claimed identity:

a) at registration, the act of evaluating end entities' (i.e., subscribers') credentials as evidence for their claimed identity;

b) during use, the act of comparing electronically submitted identity and credentials (i.e., user ID and password) with stored values to prove identity

3.3
authentication data
information used to verify the claimed identity of an entity, such as an individual, defined role, corporation or institution

3.4
card bureau
agent of the **CA** (3.18) or **RA** (3.46) that personalizes an **ICC** (3.32) containing the subscriber's private key (as a minimum)