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)

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.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.