INTERNATIONAL STANDARD

ISO/IEC 27099

First edition
2022-07

Information technology — Public key infrastructure — Practices and policy framework

Reference number
ISO/IEC 27099:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The business objective of a public key infrastructure (PKI) is to establish and manage trust relationships. The services provided by the PKI should maintain that trust and organizational and technical security measures for an appropriate security level have to be defined and implemented for all entities participating in a PKI.

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

Industry relies on several time-honoured methods of electronically identifying, authorizing, and authenticating entities and protecting transactions. These methods include, but are not limited to, personal identification numbers (PINs) and message authentication codes (MACs) for retail and wholesale transactions, user IDs and passwords for network and computer access, and key management for network connectivity. Over the past 30 years, industry has developed risk management processes and policies to support the use of these technologies.

The ubiquitous use of online services in public networks and the needs of the industry in general to provide safe, private, and reliable 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 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 adherence to standard practices can be ascertained.

Applications serving 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 document.

This document provides a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures. The degree to which any entity in a transaction can rely on the implementation of public key infrastructure standards and the extent of interoperability between PKI-based systems will depend partly on factors relative to policy and practices defined in this document.

In some regions or countries there is a legislative framework which defines requirements for operation of PKI and other related trust services to achieve a recognized level of trust for a specific purpose commonly called “qualified”.

This document is derived from ISO 21188:2018, which content has been generalized in this document to be applicable to any application domain and to take into account general standards for information security. See Annex E for a description of major changes to ISO 21188:2018 clauses that have been made in order to produce this document.

Information technology — Public key infrastructure — Practices and policy framework

1 Scope

This document sets out a framework of requirements to manage information security for Public key infrastructure (PKI) trust service providers through certificate policies, certificate practice statements, and, where applicable, their internal underpinning by an information security management system (ISMS). The framework of requirements includes the assessment and treatment of information security risks, tailored to meet the agreed service requirements of its users as specified through the certificate policy. This document is also intended to help trust service providers to support multiple certificate policies.

This document addresses the life cycle of public key certificates that are used for digital signatures, authentication, or key establishment for data encryption. It does not address authentication methods, non-repudiation requirements, or key management protocols based on the use of public key certificates. For the purposes of this document, the term "certificate" refers to public key certificates. This document is not applicable to attribute certificates.

This document uses concepts and requirements of an ISMS as defined in the ISO/IEC 27000 family of standards. It uses the code of practice for information security controls as defined in ISO/IEC 27002. Specific PKI requirements (e.g. certificate content, identity proofing, certificate revocation handling) are not addressed directly by an ISMS such as defined by ISO/IEC 27001 [26].

The use of an ISMS or equivalent is adapted to the application of PKI service requirements specified in the certificate policy as described in this document.

A PKI trust service provider is a special class of trust service for the use of public key certificates.

This document draws a distinction between PKI systems used in closed, open and contractual environments. This document is intended to facilitate the implementation of operational, baseline controls and practices in a contractual environment. While the focus of this document is on the contractual environment, application of this document to open or closed environments is not specifically precluded.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 9594-8, *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*