TECHNICAL REPORT

ISO/TR 13569

Second edition
1997-10-01

AMENDMENT 1
1998-12-15

Banking and related financial services — Information security guidelines

AMENDMENT 1:

Banque et services financiers liés aux opérations bancaires — Lignes directrices pour la sécurité de l'information

AMENDEMENT 1

Reference number
ISO/TR 13569:1997/Amd.1:1998(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

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.

The main task of ISO technical committees is to prepare International Standards. In exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the necessary support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Amendment 1 to ISO/TR 13569:1997, which is a Technical Report of type 3, was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Security management and general banking operations*.

Introduction

ISO/TR 13569 was last published in 1997. In the intervening months, technologies have advanced which present new risks or opportunities. This Amendment is intended to bring up-to-date information to readers of ISO/TR 13569:1997. A review of ISO/TR 13569:1997 did not yield any controls that are no longer appropriate; therefore an Amendment, rather than a new version, was proposed.

Banking and related financial services — Information security guidelines

AMENDMENT 1

1 Reference

ISO/TR 13569:1997, *Banking and related financial services — Information security guidelines.*

2 Definition

2.1 Y2k

The year 2000; also taken to mean the problem in information processing systems in recognizing a "00" as meaning the year 2000 and not the year 1900.

3 Access Control

The original editions of ISO/TR 13569, particularly subclause 7.2, focused on access control issues within the organization at a time when technology for certificates was not fully mature. The number of external connections to financial institutions' computers continues to grow and International Standards on composition and use of digital certificates now give institutions a choice of access control technology.

3.1 Internal or External users

Institutions should have access control policies in place that address access to their systems by employees, by contractor, and by customers. In most cases, these policies will have significantly different concerns depending on the relationship with the party seeking access. The policies should either have separate sections dealing with each class of person, or be unambiguous with respect to what controls apply in each case.

3.1.1 Use of Certificates

A digital certificate is a digital message, which may vouch for the identity of a user. A certificate may contain additional information that may be used to describe privileges of that user, an expiration date, or any other data which may be useful. A digital certificate is issued by a certificate authority(CA), who is relied upon to confirm identity and associate data before issuing the certificate. The CA also provides trusted information to those who desire to verify the legitimacy of a certificate. See 8.3 for more discussion of certificate management. International Standards supporting certificate use are being developed. These include:

CD 15782-1 Public Key Certificates

CD-15782-2 Attribute Certificates

CD-15782-3 Certificate Extensions

Use of a certificate to identify a user may replace userid and password as identification control to allow sign-on to systems, and access to information or privileges, if

a) the certificate is validated using information securely received from a certification authority recognized and trusted by the institution.

b) for select applications, the certificate should be checked against a certificate revocation list, or an "active account" list prior to access being granted.

3.2 Biometrics

Biometrics technology, called out in ISO/TR 13569:1997, 7.2.1, has advanced in the last few years and products with higher accuracy and lower costs have made biometric verification of identity closer to viability. However, the rates of error associated with current technology make biometrics-only controls infeasible at this time. Care should be taken to ensure that use of biometric information does not cause a higher than acceptable rejection rate in applications where rejections are costly, e.g. retail customers... Biometrics information may be used in conjunction with other access control mechanisms where additional security is required and rejection issues are considered.

3.3 Web Services

Identification of users accessing the institution via the web poses special challenges. If a suitable source of digital certificates exists, identifying customers via those certificates is possible. Without a suitable certificate authority, acquiring and servicing new customers via the web remains imprudent. The sale of products via the web with payment through credit card or other payment system is not a customer service for the purpose of this paragraph.

4 Cryptography — Key length recommendations

Clause 8 of ISO/TR 13569:1997 covers cryptography. ISO TC 68/SC 2 requested that the next version of ISO/TR 13569:1997 include minimum key sizes for various cryptographic systems. There is general consensus that for confidentiality purposes, 80 bit key length for block cipher systems is appropriate as a general guideline. It is also widely held view that 80 bit block cipher keys are equivalent in strength to 160 bit elliptic curve and 1024 public key systems.

There are also widely held assumptions on how much computation power is required to recover these keys through searching key space or solving an underlying mathematical problem. The cost of computation is also well known and has dropped by half every eighteen months and this is expected to continue.

A financial institution should chose products that are based on national or ISO standards and have key sizes that are both based on commercial availability and are acceptable from a risk perspective. They should do so to maintain the appearance of prudent practice, since key size debates are often vocal and public. Although a financial institution may want to use products that are widely available, no institution should be perceived as using inadequate cryptography.

However, depending on the application and the risk exposure involved, a financial institution may be justified in choosing key lengths far shorter or longer than those mentioned above. Financial institutions should consider the key lengths provided as appropriate as a general guideline for confidentiality applications and set minimum key lengths by application taking into consideration the following factors:

Time: Length of time a key will be active.

Reuse: The number of time this key will be used (preferably only once).

Value and period of validity: Assets protected by the key and the time they require protiection.

Speed and Processing demands.

Compensating controls if any.

It should be noted that setting a minimum key length should be done as part of an overall security program. For example, institutions should implement cryptographic controls in a way which limits the monetary and image loss that would accrue from any single key compromise.