
**Banking — Security and other financial
services — Framework for security in
financial systems**

*Banque — Sécurité et autres services financiers — Cadre pour la sécurité
dans les systèmes financiers*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TR 17944:2002](#)

[https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-
c11ac10820c6/iso-tr-17944-2002](https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002)



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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TR 17944:2002](https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002)

<https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002>

© ISO 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword.....	iv
Introduction.....	v
1 Scope	1
2 Areas for standardization	1
2.1 General.....	1
2.2 Identification and authentication	1
2.3 Data integrity.....	3
2.4 Privacy and confidentiality	4
2.5 Non-repudiation	4
2.6 Availability of service	5
2.7 Accountability and audit.....	6
2.8 Interoperability.....	7
2.9 Security management	8
2.10 Cryptographic algorithms.....	10
3 Open issues	11
Annex A (informative) Complementary information.....	12
Bibliography.....	13

ITIH STANDARD PREVIEW
 (standards.iteh.ai)

[ISO/TR 17944:2002](https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002)

<https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002>

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 3.

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.

In exceptional circumstances, 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), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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

ISO/TR 17944 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Security management and general banking operations*.

<https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002>

Introduction

The main goal of this Technical Report is to give guidance to Technical Committee ISO/TC 68, *Banking, securities and other financial services*, on the areas for standardization in the financial industry on IT security. Technical Committee ISO/TC 68 can, on the basis of this Technical Report, take initiatives to review, update or rewrite existing standards and/or to prepare new standards in these areas.

The financial industry has a basic need for securing financial transactions. For reasons of interoperability, certification and availability of off-the-shelf products, standards are necessary. These standards will be in the fields of cryptography, key management, application programming interfaces (API), protocols etc.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/TR 17944:2002](https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002)

<https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 17944:2002

<https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac10820c6/iso-tr-17944-2002>

Banking — Security and other financial services — Framework for security in financial systems

1 Scope

This Technical Report provides a framework for standards dealing with security that are deemed necessary for the financial industry.

This Technical Report consists of an inventory of the key security issues which arise in the financial industry and, for each of these issues, the titles of the relevant existing standards are given.

2 Areas for standardization

2.1 General

In the financial industry, the need for IT security signifies the use of standards in the fields of tokens, devices, cryptography, key management, application programming interfaces (API), protocols etc. These different fields can be grouped on the basis of business needs in the following basic areas.

In most areas, various standards are already available. In other areas standards are either being developed or there is a need for (new) standards. In clause 2, the main areas for standardization in IT security for financial institution are mentioned; Tables 1 to 9 contain the available (and sometimes necessary) standards in these areas, first the International Standards from ISO itself, followed by relevant standards from other standards organizations¹⁾. Based on the missing standards in these tables, clause 3 summarizes the open issues for standardization.

NOTE For further details on the mentioned standards, the referenced standards organization can be contacted (see annex 1).

2.2 Identification and authentication

The identity of all entities involved in a financial transaction has to be established. Authentication ensures that the identity of an entity is that which is claimed. A financial institution has to be certain that only authorized users can access their IT systems.

Mechanisms used for identification and authentication are based on the use of identifiers, tokens, pass-phrases, personal identification numbers (PIN), biometrics, digital signatures and certificates.

1) The references in this Technical Report to non-ISO standards are for informative purposes only; they should be the result of a consensus procedure and should be published or publicly available. References to non-ISO standards do not constitute an endorsement by ISO of these non-ISO standards.

2.3 Data integrity

Data integrity is the property that data has not been altered or destroyed in an unauthorized manner. Within the financial industry, data integrity is a necessary requirement.

Mechanisms used to ensure data integrity are based on message authentication, hash-functions and digital signatures.

Table 2 — Data integrity

What is required	What is available	Title/Description
Message authentication	ISO 8730	<i>Banking — Requirements for message authentication (wholesale)</i>
	ISO/IEC 9797	<i>Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher Part 2: Mechanisms using a dedicated hash-function</i>
	ISO 9807:1991	<i>Banking and related financial services — Requirements for message authentication (retail)</i>
	ISO 16609 ^a	<i>Banking — Requirements for message authentication using symmetric techniques</i>
	ANSI X9.71-2000	Keyed Hash Message Authentication Code (MAC)
Hash-functions	ISO/IEC 10118	<i>Information technology — Security techniques — Hash-functions — Part 1: General Part 2: Hash-functions using an n-bit block cipher Part 3: Dedicated hash-functions Part 4: Hash-functions using modular arithmetic</i>
^a To be published.		

2.4 Privacy and confidentiality

Privacy is the right of an individual to have his personal information kept confidential. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Privacy and confidentiality is more and more becoming an issue in the financial industry.

The mechanism used to ensure privacy and confidentiality is encipherment.

Table 3 — Privacy and confidentiality

What is required	What is available	Title/Description
Encipherment	ISO 10126	<i>Banking — Procedures for message encipherment (wholesale) — Part 1: General principles Part 2: DEA algorithm</i>

2.5 Non-repudiation

Repudiation (denial) of a financial transaction is to be prevented.

The mechanisms used to prevent repudiation are based on time stamping, digital signatures, certificates and public key infrastructures (PKI).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Table 4 — Non-repudiation

What is required	What is available	Title/Description
Non-repudiation	ISO/IEC 13888 https://standards.iteh.ai/catalog/standards/sist/15942632-250e-4c54-b69a-c11ac1062000/iso-tr-17944-2002	<i>Information technology — Security techniques — Non-repudiation — Part 1: General Part 2: Mechanisms using symmetric techniques Part 3: Mechanisms using asymmetric techniques</i>
Time stamping	ISO/IEC 18014 ^a ETSI TS 101 861-2001	<i>Information technology — Security techniques — Time-stamping services — Part 1: Framework Part 2: Mechanisms producing independent tokens Part 3: Mechanisms producing linked tokens</i> Time stamping profile

Table 4 (continued)

What is required	What is available	Title/Description
Digital signatures	ISO/IEC 9796	<i>Information technology — Security techniques — Digital signature scheme giving message recovery —</i> <i>Part 1: Mechanisms using redundancy</i> <i>Part 2: Integer factorization based mechanisms^a</i> <i>Part 3: Discrete logarithm based mechanisms</i>
	ISO/IEC 14888	<i>Information technology — Security techniques — Digital signatures with appendix —</i> <i>Part 1: General</i> <i>Part 2: Identity-based mechanisms</i> <i>Part 3: Certificate-based mechanisms</i>
	ANSI X9.31	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
	ETSI TS 101 733	Electronic Signature Formats
Certificates	ANSI X9.55-1997	Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists
	ANSI X9.68:2-2001	Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems: Part 2: Domain Certificate Syntax
	ETSI TS 101 862-2000	Qualified certificate profile
Public key infrastructure (PKI)	ANSI X9.77-2001	Public Key Infrastructure Protocols
	ANSI X9.79-2001	Public Key Infrastructure (PKI) Practices and Policy Framework
	ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates
^a To be published.		

2.6 Availability of service

Availability is the property of being accessible and usable upon demand by an authorized entity. For financial institutions, the availability of services is important for their continuity and for the image of the financial industry as a whole.

Mechanisms used to ensure availability are based on redundancy, back-up, off-site storage, back-up locations and disaster recovery planning.

Table 5 — Availability of service

What is required	What is available	Title/Description
Back-up	—	—
Disaster recovery	NIST 800-34-2002	Special Publication: Contingency Planning Guide for Information Technology Systems — Recommendations of the National Institute of Standards and Technology (draft)