TECHNICAL REPORT

ISO/TR 17944

First edition
2002-08-01

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

Reference number
ISO/TR 17944:2002(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.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

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*.

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.

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 organizations[1)]. 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.

Table 1 — Identification and authentication

What is required	What is available	Title/Description
Identification and authentication	ISO/IEC 9798	*Information technology — Security techniques — Entity authentication —*
		Part 1: General
		Part 2: Mechanisms using symmetric encipherment algorithms
		Part 3: Mechanisms using digital signature techniques
		Part 4: Mechanisms using a cryptographic check function
		Part 5: Mechanisms using zero knowledge techniques
	ISO 11131:1992	*Banking and related financial services — Sign-on authentication*
	ISO/IEC 9594-8:2001	*Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*
Business entity identifier	—	—
Tokens	ISO 10202	*Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards —*
		Part 1: Card life cycle
		Part 2: Transaction process
		Part 3: Cryptographic key relationships
		Part 4: Secure application modules
		Part 5: Use of algorithms
		Part 6: Cardholder verification
		Part 7: Key management
		Part 8: General principles and overview
	EBS 111-1999	European Banking Standard: The Interoperable Financial Sector Electronic Purse
Pass-phrases	—	—
Personal Identification Numbers (PIN)	ISO 9564	*Banking — Personal Identification Number (PIN) management and security —*
		Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems
		Part 2: Approved algorithm(s) for PIN encipherment
		Part 3: PIN protection requirements for offline PIN handling in ATM and POS systems [a]
	ISO/TR 9564	*Part 4: Best practices for PIN handling in open networks* [a]
	EBS 105-1998	PIN-based POS systems (version 2) —
		Part 1: Minimum Criteria for Certification Procedures
		Part 2: POS Systems with Online PIN Verification — Minimum Security and Evaluation Criteria
		Part 3: POS Systems with Offline PIN Verification — Minimum Security and Evaluation Criteria
Biometrics	ANSI X9.84-2001	Biometric Information Management and Security

[a] To be published.

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	*Banking — Requirements for message authentication (wholesale)*
	ISO/IEC 9797	*Information technology — Security techniques — Message Authentication Codes (MACs) —* *Part 1: Mechanisms using a block cipher* *Part 2: Mechanisms using a dedicated hash-function*
	ISO 9807:1991	*Banking and related financial services — Requirements for message authentication (retail)*
	ISO 16609 [a]	*Banking — Requirements for message authentication using symmetric techniques*
	ANSI X9.71-2000	Keyed Hash Message Authentication Code (MAC)
Hash-functions	ISO/IEC 10118	*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*

[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	*Banking — Procedures for message encipherment (wholesale) —* *Part 1: General principles* *Part 2: DEA algorithm*

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).

Table 4 — Non-repudiation

What is required	What is available	Title/Description
Non-repudiation	ISO/IEC 13888	*Information technology — Security techniques — Non-repudiation —* *Part 1: General* *Part 2: Mechanisms using symmetric techniques* *Part 3: Mechanisms using asymmetric techniques*
Time stamping	ISO/IEC 18014 [a] ETSI TS 101 861-2001	*Information technology — Security techniques — Time-stamping services —* *Part 1: Framework* *Part 2: Mechanisms producing independent tokens* *Part 3: Mechanisms producing linked tokens* Time stamping profile

Table 4 (*continued*)

What is required	What is available	Title/Description
Digital signatures	ISO/IEC 9796	*Information technology — Security techniques — Digital signature scheme giving message recovery —* *Part 1: Mechanisms using redundancy* *Part 2: Integer factorization based mechanisms* [a] *Part 3: Discrete logarithm based mechanisms*
	ISO/IEC 14888	*Information technology — Security techniques — Digital signatures with appendix —* *Part 1: General* *Part 2: Identity-based mechanisms* *Part 3: Certificate-based mechanisms*
	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	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)

2.7 Accountability and audit

Accountability is the property that ensures that the actions of an entity may be traced uniquely to the entity. For obvious reasons, financial institutions have to be able to prove the validity of transactions to their customers and to third parties. The different security measures, procedures and products are to be of a sound security level. A minimum set of safeguards have to be established for a system or organization.

Mechanisms used for accountability and audit are based audit trails, logs, functionality classes, protection profiles, evaluation criteria etc.

Table 6 — Accountability and audit

What is required	What is available	Title/Description
Functionality classes	ISO 10181	*Information technology — Open Systems Interconnection — Security frameworks for open systems:* *Overview* *Authentication framework* *Access control framework* *Non-repudiation framework* *Confidentiality framework*
	ANSI X9.45-1999	Enhanced Management Controls Using Digital Signatures and Attribute Certificates
Protection profiles	ISO/IEC 15292	*Information technology — Security techniques — Protection Profile registration procedures*
	ISO/IEC 15446 [a]	*Information technology — Security techniques — Guide on the production of Protection profiles and Security Targets*
	ANSI X9.79	*Part 2:* Protection profiles for certificates issuing and management systems (draft)
Evaluation criteria	ISO 13491	*Banking — Secure cryptographic devices (retail) —* *Part 1: Concepts, requirements and evaluation methods* *Part 2: Security compliance checklists for devices used in magnetic stripe card systems*
	ISO/IEC 15408	*Information technology — Security techniques — Evaluation criteria for IT security —* *Part 1: Introduction and general model* *Part 2: Security functional requirements* *Part 3: Security assurance requirements*
	ANSI X9.66	Cryptographic device security
	ANSI X9.74	Conformance testing for certificate path processing

[a] To be published.

2.8 Interoperability

For the financial industry, interoperability is becoming an important issue both in the wholesale as well as in the retail environment.

Mechanisms used for interoperability are data element, protocol and interface standards. It should be noted, however, that interoperability is a much broader issue than the existence of standards alone.

Table 7 — Interoperability

What is required	What is available	Title/Description
Interoperability	EMV2000	Integrated circuit card specification for payment systems Book 1: Application independent icc to terminal interface requirements Book 2: Security and key management Book 3: Application specification Book 4: Cardholder, attendant, and acquirer interface requirements
	SET	Secure Electronic Transaction Specification Book 1: Business Description Book 2: Programmer's Guide Book 3: Formal Protocol Definition
Data element	ISO 9362	*Banking — Banking telecommunication messages — Bank identifier codes*
	ISO 13616	*Banking and related financial services — International Bank Account Number (IBAN)*
Protocol	ISO 7064 [a]	*Information technology — Security techniques — Data processing — Check character systems*
	ISO 8583	*Financial transaction card originated messages — Interchange message specifications —* *Part 1: Messages, data elements and code values* [a] *Part 2: Application and registration procedures for Institution Identification Codes (IIC)* *Part 3: Maintenance procedures for messages, data elements and code values* [a]
	ISO 9992	*Financial transaction cards — Messages between the integrated circuit card and the card accepting device —* *Part 1: Concepts and structures* *Part 2: Functions, messages (commands and responses), data elements and structures*
	ISO 15668	*Banking — Secure file transfer (retail)*
Interface	ISO 7813:2001	*Identification cards — Financial transaction cards*

[a] To be published.

2.9 Security management

The security measures used by financial institutions have to be managed. Some general standards in the area of key management and certificate management are required to ensure a basic minimum level of security.

Table 8 — Security management

What is required	What is available	Title/Description
Security management	ISO/IEC TR 13335	*Information technology — Guidelines for the management of IT Security —* *Part 1: Concepts and models for IT Security* *Part 2: Managing and planning IT Security* *Part 3: Techniques for the management of IT Security* *Part 4: Selection of safeguards* *Part 5: Management guidance on network security*
	ISO/TR 13569	*Banking and related financial services — Information security guidelines*
	ISO/IEC 15443 [a]	*Information technology — Security techniques — A framework for IT security assurance*
	ISO/IEC 15816	*Information technology — Security techniques — Security information objects for access control*
	ISO/IEC 15947 [a]	*Information technology — Security techniques — IT intrusion detection framework*
	ANSI X9.41	Security Services Management for the Financial Services Industry
	BS 7799	Information Security Management
	ECBS TR 406	Guideline on Algorithm Usage and Key Management
Key management	ISO 8732	*Banking — Key management (wholesale)*
	ISO 11568	*Banking — Key management (retail) —* *Part 1: Introduction to key management* *Part 2: Key management techniques for symmetric ciphers* *Part 3: Key life cycle for symmetric ciphers* *Part 4: Key management techniques using public key cryptosystems* *Part 5: Key life cycle for public key cryptosystems* *Part 6: Key management schemes*
	ISO/IEC 11770	*Information technology — Security techniques — Key management* *Part 1: Framework* *Part 2: Mechanisms using symmetric techniques* *Part 3: Mechanisms using asymmetric techniques*

Table 8 *(continued)*

What is required	What is available	Title/Description
Key management	ISO 13492	*Banking — Key management related data element (retail)*
	ANSI X9.42-2001	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
	ANSI X9.44-2000	Key Establishment Using Factoring-Based Public Key Cryptography for the Financial Services Industry (draft)
	ANSI X9.63-2001	Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography
	ANSI X9.70	Management of Symmetric Keys Using Public Key Algorithms
	ECBS TR 405	Key Recovery in Financial Systems
Certificate management	ISO 15782	*Banking — Certificate management —* *Part 1: Public Key Certificates* [a] *Part 2: Certificate extensions*
	ANSI X9.57-1997	Public Key Cryptography for the Financial Services Industry: Certificate Management
	ANSI X9.79-2001	Public Key Infrastructure (PKI) Practices and Policy Framework
	ECBS TR 402-1997	Certification Authorities (version 2)
	IEFT RFC 2527:1999	Internet X.509 Public Key Infrastructure Certificate and CRL Framework
Trusted third party management	ISO/IEC TR 14516	*Information technology — Security techniques — Guidelines on the use and management of Trusted Third Party services*
	ISO/IEC 15945	*Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[a] To be published.

2.10 Cryptographic algorithms

The security measures used by financial institutions are mostly based on cryptographic techniques. For reasons of interoperability and basic security levels, some general standards in the area of cryptography are required.

Table 9 — Cryptographic algorithms

What is required	What is available	Title/Description
General	ISO/IEC 9979	*Information technology — Security techniques — Procedures for the registration of cryptographic algorithms*
	ANSI X9.82 [a]	Random Bit Generation
	ANSI X9.80-2001	Prime Number Generation
	ANSI TR 9	Abstract syntax notation & encoding rules for financial industry standards
Symmetric	ISO 8372	*Information processing — Modes of operation for a 64-bit block cipher algorithm*
	ISO/IEC 10116	*Information technology — Security techniques — Modes of operation for an n-bit block cipher*
	ANSI X9.52-1998	Triple Data Encryption Algorithm Modes of Operation
	ANSI X9 TG-19	Modes of Operation Validation System for Triple Data Encryption Algorithm
	FIPS PUB 197	Advanced Encryption Standard
Asymmetric	ANSI X9.30-1	Public Key Cryptography for the Financial Services Industry: Part 1 The Digital Signature Algorithm
	ANSI X9.31	Digital Signature Using Reversible Public Key Cryptography
	ANSI X9.76	Partial Key Refreshing Mechanism for Threshold Digital Signatures
Elliptic curve	ISO/IEC 15946	*Information technology — Security techniques — Cryptographic techniques based on elliptic curves —* *Part 1: General* *Part 2: Digital signatures* *Part 3: Key establishment* *Part 4: Digital signatures giving message recovery* [a]
	ANSI X9 TG-17	Technical Guideline on Elliptic Curve Arithmetic
	ANSI X9.62-1998	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)
	ANSI X9.63	Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography

[a] To be published.

3 Open issues

Table 10 summarizes those items from the various tables in clause 2 given in the “What is required” column for which the “What is available” column gives either nothing or no available ISO standard.

Table 10 — Summary of unavailability

What is required	What is available	Additional remarks
Pass-phrases	Unavailable	
Biometrics	Unavailable	See X9.84-2001 (ISO NWI proposed)
Certificates	No ISO standard available	ANSI X9.79 standards available (ISO NWI proposed)
Public key infrastructure (PKI)	No ISO standard available	ANSI X9.79 standards available (ISO NWI proposed)
Back-up	Unavailable	
Disaster recovery	No ISO standard available	NIST Special Publication (draft) available
Interoperability	No ISO standard available	
Asymmetric algorithms	No ISO standard available	ANSI X9 standards available

Annex A
(informative)

Complementary information

Further details concerning the standards mentioned in this document can be obtained from the following sources.

International Organization for Standardization
Central Secretariat
Case postale 56
CH-1211 Genève 20
Switzerland
Tel: +41 22 749 0111
Fax: +41 22 733 3430
E-mail: clivio@iso.org

International Organization for Standardization
ISO/TC 68 Secretariat
c/o American Bankers Association
1120 Connecticut Avenue, NW
Washington, D.C. 20036
United States of America
Tel: +1 202 663 5284
Fax: +1 202 828 4540
E-mail: cfuller@aba.com

American National Standards Institute
ASC X9 Secretariat
c/o American Bankers Association
1120 Connecticut Avenue, NW
Washington, D.C. 20036
United States of America
Tel: +1 202 663 5284
Fax: +1 202 828 4540
E-mail: cfuller@aba.com

European Committee for Banking Standards
Secretary General
Avenue de Tervueren 12
B-1040 Brussels
Belgium
Tel: +32 2 733 3533
Fax: +32 2 736 4988
E-mail: ecbs@ecbs.org

Bibliography

[1] ISO/IEC TR 13335 (all parts), *Information technology — Guidelines for the management of IT Security —*

ICS 03.060; 35.240.40

Price based on 13 pages