

INTERNATIONAL STANDARD

ISO
11131

First edition
1992-09-15

Banking and related financial services — Sign-on authentication

*Banque et services financiers liés aux opérations bancaires —
Authentification par signature*



Reference number
ISO 11131-1992(E)



Documents
Document Sharing Hub

Contents	Page
1 Scope	1
2 Normative references	1
3 Definitions and abbreviations	1
4 Sign-on authentication	3
5 Protection	4
6 Protocol specification for interoperability	5
Annex	
A Limitations of this International Standard	10

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.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75% approval by the member bodies voting.

International Standard 11131 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC2, *Operations and procedures*.

The technical normative elements of this International Standard are based on ANSI X9.26.

Annex A of this International Standard is for information only.

Introduction

Financial institutions are making increased use of electronic communications technology to provide services to their customers that are more timely, error free, and tailored to the needs of the individual customer. Such technology is increasingly providing the ability for the customer to directly access (or sign-on to) a financial institution's applications residing on the institution's computers. Specific examples of this include funds transfer and cash management services.

Historically, the standard method adopted by the financial industry to provide direct access to a service provider's system, has been the use of an individual identifier for each user (userid) in combination with a secret password.

There are, however, limitations on the effectiveness of these password systems. The presentation of a password in the clear to authenticate a user can be compromised in many ways. For example, it can be guessed, eavesdropped, or openly displayed. Two possible threats are masquerade and replay:

- Masquerade is the impersonation of an entity by presenting the stolen password; masquerade is usually accompanied by other attacks, such as data modification.
- Replay is the re-presentation of a recorded valid exchange at a later date, to produce an unauthorized effect.

A secure sign-on procedure where both parties share a common secret key, will need to fulfil a number of conditions, including the following:

- a) maintain the integrity of the hardware and software of the nodes in the authentication system;
- b) maintain the integrity of the authentication information (eg assignment of user identifiers (userids), password selection, password changing, means for discontinuing access, audit of unsuccessful sign-on attempts) between requestor and grantor;
- c) maintain the continuity of the authentication throughout the session after a successful sign-on;
- d) maintain the auditability of unsuccessful sign-on attempts;
- e) ensure the integrity of the key management system against compromise and misuse;
- f) ensure the confidentiality of the transferred authentication information;
- g) provision of means for detection of a replay through the verification of the authentication information.

Banking and related financial services — Sign-on authentication

1 Scope

This International Standard achieves the realization of conditions (f) and (g) in the introduction. It specifies three types of sign-on authentication between entities requesting access and entities capable of granting access:

- a) Authentication of a user via Personal Authentication Information (PAI) such as a password;
- b) Authentication of a user via a user-unique key;
- c) Authentication of a node via a node-unique key.

This International Standard is designed for use with symmetric (secret key) algorithms, where requestor and grantor use the same key.

Clause 6 gives an example of a protocol which meets the requirements of this International Standard, conformance with which enables interoperability to be achieved. Annex A identifies the limitations of this International Standard.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8372: 1987, *Information processing - Modes of operation for a 64-bit block cipher algorithm*.

ISO 8730: 1990, *Banking - Requirements for message authentication (wholesale)*.

ISO 8732: 1988, *Banking - Key management (wholesale)*.

ISO 10126-1: 1991, *Banking - Procedures for message encipherment (wholesale) - Part 1: General principles*.

ISO 10126-2: 1991, *Banking - Procedures for message encipherment (wholesale) - Part 2: DEA algorithm*.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this International Standard, the following definitions apply.

3.1.1 authentication key: A cryptographic key used for authentication.

3.1.2 ciphertext: Enciphered information.

3.1.3 cryptoperiod: A defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys for a given system may remain in effect.

3.1.4 decipherment: A process of transforming ciphertext (unreadable) into plaintext (readable).

3.1.5 encipherment: A process of transforming plaintext (readable) into ciphertext (unreadable) for security or privacy.

3.1.6 cryptographic key: A key used to encipher or decipher data.

3.1.7 grantor: The entity being asked to grant access privileges.

3.1.8 key granularity: The number of individuals represented by a key, e.g., the finest granularity is one individual represented by one key; a coarser granularity is a node key.

3.1.9 message authentication: The verification of the source, uniqueness and integrity of a message.

3.1.10 Message Identifier (MID): A field used uniquely to identify a financial message or transaction (e.g. sending bank's transaction reference).

3.1.11 modulo 2 addition: A mathematical operation, symbol (+), defined as:

$$\begin{aligned} 0 (+) 0 &= 0 \\ 0 (+) 1 &= 1 \\ 1 (+) 0 &= 1 \\ 1 (+) 1 &= 0 \end{aligned}$$

Modulo 2 addition of blocks of bits indicates bit by bit addition without carry.

3.1.12 node: A device capable of sending or receiving data whose identification will be unambiguous for authentication purposes.

3.1.13 Personal Authenticating Information (PAI): Information used to authenticate a user's identity. The information can be derived from something the user knows (e.g. a secret password), something the user has (e.g. exclusive possession of a badge), something the user is (e.g. a fingerprint), or any combination of the three.