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)

Contents Page

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

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.

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:

0 (+) 0 = 0
0 (+) 1 = 1
1 (+) 0 = 1
1 (+) 1 = 0

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.

3.1.14 **plaintext:** Unenciphered data.

3.1.15 **requestor:** The entity requesting sign-on.

3.1.16 **Time Variant Parameter (TVP):** A random or pseudorandom value that is never intentionally repeated during the cryptoperiod of the key.

3.1.17 **variant of a key:** A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.

3.2 Abbreviations

The following abbreviations are used in this International Standard.

Abbreviation	Meaning	Description
CSM	Cryptographic Service Message	A message for transporting keys or related information used to control a keying relationship.
DATA	Data	The input of the CRYPTO function. For example, the result of the COMBINE function.
ECB	Electronic Code Book	A mode of implementing the encipherment algorithm.
ERF	Error Field	The field which identifies error conditions detected in a previous CSM.
GS1	Type 1 GSF	GSF of type 1 authentication with a current PAI.
GS2	Type 2 GSF	GSF of type 2 authentication.
GS3	Type 3 GSF	GSF of type 3 authentication.
GSF	GENERAL SECURITY Function	It is used to protect the PAI and to authenticate the user or the node in the sign-on process.
GSN	New GSF	GSF of type 1 authentication with a new PAI
INF	Information	Any user defined information as a parameter of the COMBINE function.
INPUT	Input	The input of the SELECT function. For example, the result of the CRYPTO function.
IV	Initialization Vector	Starting point for an encipherment/decipherment process.
K	Key	A key.
MAC	Message Authentication Code	A code in a message between a sender and a receiver used to validate the source and part or all of the text of the message. The code is the result of an agreed calculation.
MCL	Message Type	The tag for the field that defines the type of CSM.
MID	Message Identifier	See 3.1.10.
ORG	Originator	Identity of the sender of the CSM.
PAI	Personal Authenticating Information	See 3.1.13.
PCM	Grantor-generated PAI Change Messages	One of the four message classes used in the sign-on authentication CSM.
RCV	Recipient	Identity of the recipient of the CSM.
SOE	Sign-on Error Message	One of the four message classes used in the sign-on authentication CSM
SOM	Sign-on Message	One of the four message classes used in the sign-on authentication CSM.
TTM	TVP Transmission Message	One of the four message classes used in the sign-on authentication CSM.
TVP	Time Variant Parameter	See 3.1.16.
USR	User	Identity of the user requesting access

4 Sign-on authentication

This clause specifies the basic functions and processes required to accomplish sign-on authentication in accordance with this International Standard.

Three types of sign-on authentication are addressed by this Standard:

a) Type 1 : The authentication of a user via PAI.

b) Type 2 : The authentication of a user via a user-unique key.

c) Type 3 : The authentication of a node via a node-unique key.

Note 1 The last two types of authentication are very similar, the only fundamental differences derive from the granularity of the cryptographic keys used

Using type 1 authentication, the key granularity may pertain to users, nodes, or organizations. The key granularity relates to the user when type 2 authentication is used, and the key granularity relates to a node when type 3 authentication is used.

Each communication pair shall have a cryptographic capability and share a cryptographic key (and an Initialization Vector, IV, if required) distributed in accordance with ISO 8732. A PAI is required for type 1 authentication only.

All message authentication procedures specified in this International Standard shall conform to the requirements of ISO 8730 All key management procedures carried out in accordance with this International Standard shall conform to the requirement of ISO 8732 When transmitted the PAI shall be enciphered.

4.1 Basic functions

This section defines the basic functions which are used to protect the PAI and to authenticate the users or the nodes in the sign-on process.

4.1.1 The COMBINE function : COMBINE (TVP,PAI,INF)

The COMBINE function combines up to three input values (i.e. TVP, PAI, and INF) into a single value. When the key is not changed for each sign-on, the TVP is required. PAI is required for type 1 authentication only. INF represents any user defined information. At least one parameter is always required

When either TVP or PAI are used, each shall be selected from a set of not less than one million possible values. The value of the TVP shall affect the left-most bits of the output of the COMBINE function. The output of the COMBINE function shall be a value space sufficient to ensure that at least one million values are equally probable over the life of the set of valid values.[1)]

For example, COMBINE(TVP,PAI) may be defined to equal TVP(+)PAI where (+) is the modulo-2 addition operation and INF is not used.

1) The value space of the TVP is reduced by each value used It is essential that this space remains sufficiently large to ensure that the population of valid TVPs remains above the one-in-a-million threshold For systems that operate close to that threshold, a mechanism should be provided to force a key change whenever the threshold is crossed

4.1.2 The CRYPTO function: CRYPTO(IV,K,DATA)

The CRYPTO function cryptographically transforms the input DATA (e.g. the result of the COMBINE function), using the key K, and optionally the Initialization Vector IV. When encipherment is used, the encipherment method shall either conform to ISO 10126 or be the Electronic Code Book (ECB) Mode of Operation described in ISO 8372. ECB shall only be used when DATA is less than or equal to 64 bits. An IV is not used for ECB encipherment. When message authentication is used, the authentication method shall conform to ISO 8730, with the TVP serving the same purpose as the combination of the message identifier (MID) and the date of message origination (Date).

When both message authentication and encipherment are used, different keys (or a key and its variant) shall be used by the CRYPTO function.

When encipherment other than ECB is used, either the TVP shall be kept secret (e.g. enciphered) or the DATA parameter shall be authenticated under a different key (or its variant) prior to encipherment

4.1.3 The SELECT function: SELECT(INPUT)

The SELECT function selects and returns all or part of the data from INPUT (e.g. the result of the CRYPTO function) This facilitates compression of messages.

The SELECT function shall be chosen so that the chance of any change in the TVP or PAI not affecting the output of the SELECT function shall be less than or equal to one in one million. When the TVP and PAI are not used and keys are changed on each sign-on, then the SELECT function shall be chosen so that the chance of obtaining the same SELECT function output after a key change shall be less than or equal to one in a million.

For example, SELECT(INPUT) may be defined to equal any n bits of INPUT.

4.1.4 GENERAL SECURITY function: GSF(IV,K,TVP,PAI,INF)

The GENERAL SECURITY function (GSF), which is used to protect the PAI and to authenticate the users or the nodes in the sign-on process, is formed by composing the previously described functions as follows:

GSF(IV,K,TVP,PAI,INF) =
SELECT(CRYPTO(IV,K,COMBINE(TVP,PAI,INF)))

The output of the GSF shall have at least one million possible values.

Note 2 There are cases where more than one single GSF may be necessary during a sign-on sequence (e g two different invocations of GSF may be necessary when user changes PAI)

4.2 Authentication process

In order to accomplish sign-on authentication, a message containing the results of the GSF function is sent from the requestor to the grantor.

Each communicating pair shall share a cryptographic key and an IV (if required). Both the requestor and the grantor shall know the values of the TVP (if used) and the INF (if used). The grantor shall verify that the parameters used in the GSF are correct. This may be confirmed by comparing the result of GSF against the GSF value received in the message sent from the requestor. Alternatively, when an invertible GSF is used, the grantor can apply the inverted function to the GSF value received in the message to obtain the parameters which can then be used to compare with the expected values.

4.3 Authentication of a user via PAI (Type 1 authentication)

When a user is to be authenticated using type 1 authentication a PAI shall be used and the CRYPTO function shall be enciphered if PAI is transmitted.

For example, where the TVP and PAI are less than or equal to 64 bits, one can set:

COMBINE (TVP,PAI,INF) = TVP(+)PAI,
where INF is not used;

CRYPTO (IV,K,DATA) = eK(DATA),
where DATA is enciphered by a key, K, using a cryptographic key in the ECB mode;

SELECT (INPUT) = INPUT,
where SELECT is the identity.

In this case, GSF(IV,K,TVP,PAI,INF) = eK(TVP(+)PAI),
where TVP(+)PAI is enciphered by K using a cryptographic key in the ECB mode.

A grantor who possesses TVP, PAI, and K may encipher TVP(+)PAI and compare the calculated result against the result received from the requestor. The user is explicitly authenticated by means of the PAI used in the GSF.

Note 3 In this example, the grantor can decipher the received GSF value to obtain the PAI which can then be compared against the stored PAI. This is possible because the GSF is chosen to be invertible.

4.4 Authentication of a user via a user-unique key (Type 2 authentication)

When a user is authenticated using type 2 authentication, the key shall be unique for the user.

For example, where the TVP and PAI are less than or equal to 64 bits, one can set:

COMBINE(TVP,PAI,INF) = TVP,
where PAI and INF are not used;

CRYPTO(IV,K,DATA) = eK(DATA),
where DATA is enciphered by a key, K, using a cryptographic key in the ECB mode;

SELECT(INPUT) = INPUT,
where SELECT is the identity.

In this case, GSF(IV,K,TVP,PAI,INF) = eK(TVP),
where TVP is enciphered by K using a cryptographic key in the ECB mode.

A grantor who possesses TVP and K may encipher TVP and compare the calculated result against the result received from the requestor. The user is implicitly authenticated by means of the user-unique key used in the GSF.

Note 4 In this example, the grantor can decipher the received GSF value to obtain the TVP which can then be compared against the stored TVP. This is possible because the GSF is chosen to be invertible.

4.5 Authentication of a node via a node-unique key (Type 3 authentication)

When a node is authenticated using type 3 authentication, the key shall be unique for the node. This method is identical to the method in 4.4 except for the granularity of the keys.

For example, where the TVP and PAI are less than or equal to 64 bits, one can set:

COMBINE(TVP,PAI,INF) = TVP,
where PAI and INF are not used;

CRYPTO(IV,K,DATA) = eK(DATA),
where DATA is enciphered by a key, K, using a cryptographic key in the ECB mode;

SELECT(INPUT) = INPUT,
where SELECT is the identity.

In this case, GSF(IV,K,TVP,PAI,INF) = eK(TVP),
where TVP is enciphered by K using a cryptographic key in the ECB mode.

A grantor who possesses TVP and K may encipher TVP and compare the calculated result against the result received from the requestor. The node is implicitly authenticated by means of the node-unique key used in the GSF.

Note 5 In this example, the grantor can decipher the received GSF value to obtain the TVP which can then be compared against the stored TVP. This is possible because the GSF is chosen to be invertible.

4.6 Bi-directional authentication

Authentication may be performed in both directions between two nodes or between a user and a node. In this case a message containing a GSF shall be sent in each direction Greater security is provided when information contained in the first message is included as a parameter in the COMBINE function of the message in the reverse direction.

When the same key is used in both directions, care should be taken to ensure that the transmitted TVP cannot be played back successfully to its sender.

5 Protection

A procedure claiming conformance to this International Standard, shall provide protection to the following measurable extent:

i) the chance of a replay of a previously valid sign-on message resulting in a successful unauthorized sign-on shall be no more than one in one million;

ii) the chance of a modification of a previously valid sign-on message resulting in a successful unauthorized sign-on shall be no more than one in one million;

iii) the chance of an unauthorized party being successfully authenticated as an authorized user in any single attempt shall be no more than one in one million;

iv) when transmitted, the PAI shall be enciphered, and be used to verify the identity of the user;

v) disclosure of one party's PAI shall not compromise another party's sign-on.

6 Protocol specification for interoperability

This clause provides an example of a protocol which meets the requirements of this International Standard. While other protocols may meet the requirements of this International Standard, the specific protocol described below is intended to be used to promote interoperability of implementations This protocol uses the TVP as a "challenge" from the grantor to the requestor, and requires a "response" containing the result of the GSF operating on that TVP. This protocol also defines interoperable error messages.

The protocol specifies use of Cryptographic Service Messages (CSM) consisting of four different message classes: TVP Transmission Message (TTM), Sign-on Message (SOM), Grantor-generated PAI Change Message (PCM), and Sign-on Error Message (SOE), respectively.

The protocol provides for three different types of authentication: user authentication via PAI, user authentication via user-unique key, and node authentication via node-unique key. Interoperable implementations as illustrated in this clause shall have the capability of performing all three types of authentication.

The protocol assumes that previous activity has established a connection and an implicit request for access. This previous activity may also have established a "claimed" identity requiring authentication. If available, this claimed identity may allow the grantor to determine the appropriate type of authentication from the three types described above.

6.1 Requirements

The following requirements apply to each of the messages in 6.3 to 6.7.

a) The encipherment specified is the ECB mode of encipherment as defined in ISO 8372. Hexadecimal filtering is used as defined in ISO 10126.

b) A random or pseudorandom TVP of 64 bits is required.

c) A PAI of 32 to 64 bits is required. If the PAI is less than 64 bits, the PAI field is padded with zeros from the right to form 64 bits.

6.2 Notation

The following notation shall be used to specify the protocol.

a) The character set for Cryptographic Service Messages shall be the following characters: digits (0-9), letters (A-Z), comma (,), period (.), space (b), solidus (/), hyphen (-), asterisk (*), open and close parentheses ((&)). The character (b) shall only be used in a message to separate fields. The character (.) shall only be used in a field to separate subfields (if required).

b) The presence of a Cryptographic Service Message is denoted by the financial message field tag, "CSM".

c) The contents of each message shall begin with an open parenthesis "(" and end with a close parenthesis ")"

d) Field tags shall be separated from field contents by a solidus "/".

e) Fields shall be separated by a space (b).

f) For illustration, plaintext fields are represented by "ppp"; fields containing output of the GSF are represented by "fff"

g) It is the responsibility of the implementor to ensure that no delimiters (e.g., "b" and ".") appear in the user defined fields (e.g., ORG, RCV).

h) ORG and RCV are the parties sharing the cryptographic key in use. ORG and RCV may refer to the user or the node, in the case of user authentication via PAI. ORG and RCV refer to nodes in the case of node authentication via node-unique key. ORG and RCV refer to a user or a node in the case of user authentication via user-unique keys.

6.3 Transmission of TVP

A TVP is required to prevent a replay of the messages described in 6.4, 6.5 and 6.6. The TVP used by the requestor shall exactly match the one sent by the grantor in the TVP Transmission Message (TTM).

6.3.1 Message format

CSM(MCL/TTMbRCV/ppbORG/pppbTVP/pppb)

MCL	Message type
TTM	TVP Transmission Message
RCV	Identity of the recipient of the message
ORG	Identity of the sender of the message
TVP	The value of TVP with hexadecimal filtering applied

6.3.2 GSF function

The GSF function is not applied to this message.

6.3.3 Processing

As shown in figure 1, this message is sent from the grantor to the requestor with the value of the TVP. This is the TVP that shall be used in the next message between the requestor and grantor.

Requestor	Grantor
	<--CSM(MCL/TTMbRCV/pppbORG/pppbTVP/pppb)

Figure 1

If a message is received with an invalid TVP an error message may be sent depending on prior agreements (see 6.7).

6.4 Authentication of a user via PAI

This protocol meets the requirements of this International Standard and corresponds to the method of authentication described in 4.3.

6.4.1 Message format

For this type of sign-on authentication, there are two additional message classes involved: Sign-on Message (SOM) and Grantor-generated PAI Change Message (PCM).

CSM(MCL/SOMbRCV/ppbORG/pppbUSR/pppbGS1/ffffbGSN/ffffb)

SOM	Sign-on Message
RCV	Identity of the recipient of the message
ORG	Identity of the sender of the message
USR	Identity of the user requesting access (the requestor identity, i.e. userid). The contents of this field can be null if the claimed identity is already known.
GS1	User PAI modulo-2 added with TVP and enciphered and then applied with the hexadecimal filtering
GSN	The new user PAI modulo-2 added with the TVP+1 and enciphered and then applied with the hexadecimal filtering. The contents of this field can be null if it is a request for a new value to be generated by the other entity.

Note This GSN is used only for Sign-on Messages which include a PAI change.

CSM(MCL/PCMbRCV/pppbORG/pppbGSN/ffffb)

MCL	Message type
PCM	Grantor-generated PAI Change Message
RCV	Identity of the recipient of the message
ORG	Identity of the sender of the message
GSN	The new user PAI modulo-2 added with the TVP+1 and enciphered and then applied with the hexadecimal filtering. The contents of this field can be null if it is a request for a new value to be generated by the other entity.

6.4.2 GSF function

The GSF function is applied to create the GS1 and the GSN fields.

GS1 = SELECT(CRYPTO(K,COMBINE(TVP,PAI)))
= eK(TVP(+)PAI)

GSN = SELECT(CRYPTO(K,COMBINE(TVP+1,new PAI)))
= eK(TVP+1(+)new PAI)

where:

a) The SELECT function is the identity.

b) For this operation, K is the key shared between RCV and ORG. CRYPTO is defined as ECB mode of operation in ISO 8372.

Note 6 No IV is required in ECB mode

c) The COMBINE function is the modulo-2 addition of both fields after padding with zeros.

6.4.3 Processing sign-on requests

Sign-on requests can be conveniently classified into two different categories: routine requests, and requests with PAI changes.

6.4.3.1 Processing routine sign-on requests

Figure 2 shows the sign-on process with a user PAI. The grantor transmits the TVP to the requestor in the TTM message. The requestor then uses the TVP to prepare the GS1 field in the SOM message to be transmitted to the grantor. Upon receipt of the SOM message, the grantor compares the received GS1 value to the calculated GS1 value.

Alternatively, the grantor can decipher the received GS1 value to obtain the TVP(+)PAI value, and hence the PAI value which can then be used to compare against the expected PAI value. If they compare favourably, then the authentication is complete.

Requestor	Grantor
	<--CSM(MCL/TTTMbRCV/pppbORG/pppbTVP/pppb)
CSM(MCL/SOMbRCV/pppb/ORG/pppbUSR/pppbGS1/ffffb)-->	

Figure 2

6.4.3.2 Processing sign-on requests with PAI change

The four PAI change cases are:

a) Requestor initiates a PAI change and supplies a new PAI value.

b) Grantor initiates a PAI change and requires the requestor to supply a new PAI.

c) Requestor initiates a PAI change and requests that the grantor supply the needed value.

d) Grantor initiates a PAI change and supplies the needed value.

Note 7 The accidental or deliberate alteration during transit of a GSN constructed from a new PAI would lead to the loss of PAI synchronisation between the grantor and requestor In order to minimise the possibility of such an occurrence, bodies implementing the protocols described here should consider the use of message integrity and message origin authentication techniques to protect messages containing GSNs constructed from new PAIs

6.4.3.2.1 PAI change (requestor-initiated, requestor-supplied)

Refer to figure 3. The TVP is provided by the grantor (The requestor determines that a new PAI is required.) The

requestor then uses the TVP and the TVP+1 to prepare the GS1 and GSN fields respectively. The grantor compares the received GS1 value to the calculated GS1 value. (Alternatively, the grantor can decipher the received GS1 value to obtain the TVP(+)PAI value, and hence the PAI value which can then be used to compare against the expected PAI value.) If they compare favourably, then the requestor is authenticated to the grantor. The grantor deciphers the received GSN value to obtain the new PAI for the requestor.

Requestor	Grantor
	<--CSM(MCL/TTMbRCV/pppbORG/pppbTVP/pppb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/ffffbGSN/ffffb)-->	

Figure 3

6.4.3.2.2 PAI change (grantor-initiated, requestor-supplied)

Refer to figure 4. The TVP is provided by the grantor. The requestor then uses the TVP to prepare the GS1 field as a routine sign-on request. The grantor compares the received GS1 value to the calculated GS1 value. (Alternatively, the grantor can decipher the received GS1 value to obtain the TVP(+)PAI value, and hence the PAI value which can then be used to compare against the expected PAI value.) If they compare favourably, then the requestor is authenticated to the grantor. The grantor determines that PAI change is needed, and sends a PCM message with a null GSN. The requestor detects the PAI change requests by examining the null GSN. The requestor supplies the new PAI in the GSN field of a new SOM message calculated with TVP+1. The grantor deciphers the received GSN value to obtain the new PAI for the requestor.

Requestor	Grantor
	<--CSM/MCL/TTMbRCV/pppbORG/pppbTVP/pppb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/ffffb)-->	
	<--CSM(MCL/PCMbRCV/pppbORG/pppbGSN/b)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/bGSN/ffffb)-->	

Figure 4

6.4.3.2.3 PAI change (requestor-initiated, grantor-supplied)

Refer to figure 5. The TVP is provided by the grantor The requestor then uses the TVP to prepare the GS1 in the SOM message. The requestor determines that a new PAI is required. In the same SOM message, the requestor uses a null GSN to request a new PAI value. The grantor compares the received GS1 value to the calculated GS1 value. (Alternatively, the grantor can decipher the received GS1 value to obtain the TVP(+)PAI value, and hence the PAI value which can then be used to compare against the expected PAI value.) If they compare favourably, then the requestor is authenticated to the grantor. In response to the request for a new PAI value, the grantor uses the TVP+1 and the newly generated PAI to prepare the GSN in the PCM message. Upon receipt of this PCM message, if the requestor decides to accept the new PAI just received, the requestor then returns the GSN value just received in a new SOM message to confirm the knowledge of the new PAI.

Requestor	Grantor
	<--CSM(MCL/TTMbRCV/pppbORG/pppbTVP/pppb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/ffffbGSN/b)-->	
	<--CSM(MCL/PCMbRCV/pppbORG/pppbGSN/ffffb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/bGSN/ffffb)-->	

Figure 5

In response to the PCM message received from the grantor, if the requestor decides to reject the new PAI just received, the requestor may send a sign-on error message (SOE) with an N in the ERF field to signify that the new PAI value is not acceptable. The grantor can send a new PCM message in response to this SOE message; again uses the TVP+1 and another newly generated PAI to prepare the GSN And the process repeats again.

6.4.3.2.4 PAI change (grantor-initiated, grantor-supplied)

Refer to figure 6. The TVP is provided by the grantor The requestor then uses TVP to prepare the GS1 in the SOM message. The grantor compares the received GS1 value to the calculated GS1 value. (Alternatively, the grantor can decipher the received GS1 value to obtain the TVP(+)PAI value, and hence the PAI value which can then be used to compare against the expected PAI value.) If they compare favourably, then the requestor is authenticated to the grantor. The grantor determines that a new PAI is required The grantor then uses the TVP+1 and the newly generated PAI to prepare the GSN in the PCM message. Upon receipt of this PCM message, if the requestor decides to accept the new PAI just received, the requestor then returns the received GSN value in a new SOM message to confirm the knowledge of the new PAI.

In response to the PCM message received from the grantor, if the requestor decides to reject the new PAI just received, the requestor may send a sign-on error message (SOE) with an N in the ERF field to signify that the new PAI value is not acceptable. The grantor can send a new PCM message in response to this SOE message; again uses the TVP+1 and another newly generated PAI to prepare the GSN. And the process repeats again.

Requestor	Grantor
	<--CSM(MCL/TTMbRCV/pppbORG/pppbTVP/pppb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/ffffb)-->	
	<--CSM(MCL/PCMbRCV/pppbORG/pppbGSN/ffffb)
CSM(MCL/SOMbRCV/pppbORG/pppbUSR/pppbGS1/bGSN/ffffb)-->	

Figure 6

In any PAI change sequence (all four cases), it is recommended that the requestor and grantor do not update their new PAI until the entire sequence is complete. The sequence can be aborted due to error at any point, in which case, return to the initial conditions is useful to facilitate error recovery. After the completion of any PAI change sequence, it is recommended that the grantor sends a new TVP to the requestor as a new challenge for verifying the new PAI with the routine sign-on process as described in section 6.4.3.1.

6.5 Authentication of a user via a user-unique key

This protocol meets the requirements of this International Standard and corresponds to the method of authentication described in 4.4.

6.5.1 Message format

For this type of sign-on authentication the following SOM message shall be used in addition to the TTM message:

CSM(MCL/SOMbRCV/ppbORG/pppbGS2/fffb)

SOM Sign-on Message
RCV Identity of the recipient of the message
ORG Identity of the sender of the message (in this case, the user identity, i.e. userid)
GS2 TVP enciphered under the user-unique key and then applied with the hexadecimal filtering

6.5.2 GSF function

The GSF function is applied to the GS2 field.

GS2 = SELECT(CRYPTO(K,COMBINE(TVP)))
= eK(TVP)

where:

a) The SELECT is the identity.

b) K is the key shared between the requestor and the grantor. The CRYPTO is defined as ECB mode of operation as in ISO 8372.

Note 8 In ECB mode, no IV is required

c) The COMBINE function is the identity.

6.5.3 Processing

The process is shown in figure 7. A TTM message is sent from the grantor to the requestor containing the expected TVP value. The requestor then uses ECB to encipher the TVP value and places it in the GS2 field of the SOM message. Upon receipt, the grantor compares the received GS2 value to the calculated GS2 value. (Alternatively, the grantor can decipher the received GS2 value to obtain the TVP value which can then be used to compare against the expected TVP value.) If they compare favourably, then the requestor has been authenticated to the grantor.

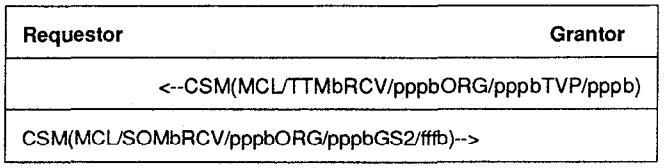

Figure 7

6.6 Authentication of a node via a node unique key

This protocol meets the requirements of this International Standard and corresponds to the method of authentication described in 4.5.

6.6.1 Message format

For this type of sign-on authentication the following SOM message shall be used in addition to the TTM message:

CSM(MCL/SOMbRCV/pppbORG/pppbGS3/fffb)

SOM Sign-on Message
RCV Identity of the recipient of the message (in this case, a node identity)
ORG Identity of the sender of the message (in this case, a node identity)
GS3 TVP enciphered under the node-unique key and then applied with the hexadecimal filtering

6.6.2 GSF function

This function is the same as the GSF function of 6.5.2 except the key used in the CRYPTO function is a node-unique key shared between the originator and recipient.

The GSF function is applied to the GS3 field.

GS3 = SELECT(CRYPTO(K,COMBINE(TVP)))
= eK(TVP)

where:

a) The SELECT function is the identity.

b) K is the key shared between the requestor and the grantor. The CRYPTO is defined as ECB mode of operation as in ISO 8372.

Note 9 In ECB mode, no IV is required

c) The COMBINE function is the identity.

6.6.3 Processing

The process is shown in figure 8. A TTM is sent from the grantor to the requestor containing the expected TVP value. The requestor then uses ECB to encipher the TVP to form the GS3 value and transmits it back to the grantor. Upon receipt, the grantor compares the received GS3 value to the calculated GS3 value. (Alternatively, the grantor can decipher the received GS3 value to obtain the TVP value which can then be used to compare against the expected TVP value.) If they compare favourably, then the requestor has been authenticated to the grantor.

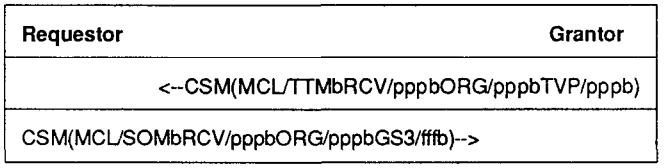

Figure 8

6.7 Error recovery

A special message class, namely, Sign-on Error Message (SOE), is designated for error messages. This SOE message shall also be used for signifying that the new PAI value generated by the grantor is not acceptable by the requestor as described in 6.4.3.2.3 and 6.4.3.2.4.

6.7.1 Message format

The format of the SOE message is shown below:

CSM(MCL/SOEbRCV/pppbORG/pppbERF/pppb)

SOE	Sign-on Error Message
RCV	Identity of the recipient of the message
ORG	Identity of the originator of the message
ERF	Error Field

The content of the Error Field shall be represented by up to 16 characters with the following values and definitions respectively:

A	Abort Sign-on process
B	Unrecognized message class
C*	Cannot process
D	Too many sign-on attempts
E*	Facility inoperative
F*	Format Error
G	Password Change not allowed
H	USR not recognized (Supplying this error message reduces the number of attempts needed in an exhaustive attack)
I	Invalid Sign-on
J	GS1 not valid
K	GSN not valid
L	GS2 not valid
M	GS3 not valid
N	The PAI generated by the grantor is not acceptable by the requestor
O	The PAI expired
P-S	Reserved for future standardization.
T-Z	Available for specific implementations
*	Error code as in ISO 8732

6.7.2 GSF function

No GSF function is applied in this message.

6.7.3 Processing

All error messages are processed by one message class, namely, SOE. On most occasions (with the exception described in 6.4.3.2), the receipt of a SOE message will cause the sign-on sequence to be aborted and error recovery attempted. Error recovery is outside the scope of this International Standard and may be implementation or policy specific.

While the protocol specifies interoperable interpretation of these error messages, it is left to administrators to decide whether such messages are actually generated.

Annex A

(informative)

Limitations of this International Standard

A.1 Scope of protection provided by this International Standard

The protection provided by procedures in conformance with this International Standard is only valid:

a) against attackers who do not have knowledge of the key(s);

b) between the cryptographic processes themselves. No protection is provided against an attack which takes place before the encipherment or after the decipherment processes. Similarly, no means of detecting any modification of the MAC, either before its appendment to the message, or after its verification, is provided;

c) in the case where both encipherment and authentication are being performed, then only when these processes are completed in a secure manner without the possibility of undetected intervention or disruption between either process;

d) where node integrity is maintained.

This International Standard does not prevent an attacker from taking control of a session using an active wire tap after an authenticated sign-on has been successfully completed.

A.2 Warning to users

The requirement (see clause 5) that the chance of unauthorized sign-on attempts by replay, modification, or chance authentication be no greater than one in one million, refers to single attempts only. An appropriate mechanism to limit the number of attempts or challenges needs to be in place. These requirements also dictate that the number of available TVP or PAI be in excess of one million. Due care will have to be taken to ensure that all values of TVP or PAI are equally probable, or, at a minimum, that the chance of each potential value being selected, guessed or generated, is less than one in one million. For this reason, user selected passwords, which are highly predictable, might not be consistent with this International Standard.

UDC 336.717:336.722.24

Descriptors: banking, banking documents, signature, coded representation, algorithms, authentication

Price based on 10 pages