INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.113

(05/97)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

Operation, numbering, routing and mobile services – International operation – General provisions concerning Administrations

---

Validation procedures for the international telecommunications charge card service

ITU-T Recommendation E.113

(Previously CCITT Recommendation)

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

OPERATION, NUMBERING, ROUTING AND MOBILE SERVICES	
INTERNATIONAL OPERATION	E.100–E.229
Definitions	E.100–E.103
General provisions concerning Administrations	**E.104–E.119**
General provisions concerning users	E.120–E.139
Operation of international telephone services	E.140–E.159
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.199
Maritime mobile service and public land mobile service	E.200–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	E.230–E.299
Charging in the international telephone service	E.230–E.249
Procedures for remuneration of Administrations for facilities made available	E.250–E.259
Measuring and recording call durations for accounting purposes	E.260–E.269
Establishment and exchange of international accounts	E.270–E.299
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	E.300–E.329
General	E.300–E.319
Phototelegraphy	E.320–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.399
QUALITY OF SERVICE, NETWORK MANAGEMENT AND TRAFFIC ENGINEERING	
NETWORK MANAGEMENT	E.400–E.489
TRAFFIC ENGINEERING	E.490–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	E.800–E.899

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION E.113

VALIDATION PROCEDURES FOR THE INTERNATIONAL TELECOMMUNICATIONS CHARGE CARD SERVICE

Summary

The expanded use and the increased number of charge cards require Card Issuers (or authorized agents) to implement adequate security against fraudulent use.

Therefore, a critical facet in the provision of such a system is the ability to ensure the validity of the card and its authorized use in a uniform manner. The purpose of this Recommendation is to define the procedures for the validation process between Administrations. This validation process makes no attempt to specify any equipment, facilities and data transmission techniques.

Source

ITU-T Recommendation E.113 was revised by ITU-T Study Group 1 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 26th of May 1997.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had/had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Introduction

Work is progressing to develop the international telecommunications charge card service as defined in Recommendation E.116.

The expanded use and the increased number of charge cards require Card Issuers (or authorized agents) to implement adequate security against fraudulent use.

Therefore, a critical facet in the provision of such a system is the ability to ensure the validity of the card and its authorized use in a uniform manner. The purpose of this Recommendation is to define the procedures for the validation process between Administrations. This validation process makes no attempt to specify any equipment, facilities and data transmission techniques.

It should be recognized that the procedures for validation of telecommunications charge cards between Administrations will vary, based on such factors as the capabilities of the card systems, bilateral agreements, and the manner in which the card is presented. Flexibility in this process must be maintained in order to maximize participation of Administrations where automated interfaces may not exist or may not be uniformly available. Where such automated interfaces exist, a defined uniform implementation is desirable.

Recommendation E.113[1]

VALIDATION PROCEDURES FOR THE INTERNATIONAL TELECOMMUNICATIONS CHARGE CARD SERVICE

(Melbourne, 1988; revised in 1993 and 1997)

1 Methods of validation

There are several methods to test the validity of charge cards. These may be divided into two general categories – full validation and limited validation.

Full validation requires checking the card number against the Card Issuer's database, as well as real-time communication between the Card Acceptor and the Card Issuer. Full validation is more thorough than other methods and is practical for automated or semi-automated charge card systems.

Limited validation may involve one or more techniques, such as a special character, a code, or a check against a partial database, as determined by the Card Issuer and outlined in a service agreement. Limited validation methods minimize the need for communication between Administrations.

2 Full validation procedures

2.1 Validation information flow

The information from the card and/or the user is presented to a terminal having access to an Administration's telecommunication charge card system. That system should then communicate with the Card Issuer to validate the card and authorize its use.

The validation information flow comprises three messages:

– authorization request;

– request response;

– call disposition.

The authorization request is a message from the Card Acceptor to the Card Issuer which provides details of an attempt to use a telecommunication charge card. This allows the Card Issuer to query its own internal systems to respond to the Card Acceptor. The Card Issuer should then communicate with the Card Acceptor to provide either a positive or negative response (with a specific indication as to why the authorization should not be granted) to the authorization request. This message is defined herein as the request response. Feedback should then be given to the user of the card as to the status of the call attempt to the extent possible within the capabilities of the particular Administration's telephone system. A third message denoted as the call disposition would be sent, subject to agreements between Administrations and Card Issuers, by the Card Acceptor to the Card Issuer in a timely manner after completion of a call or call attempt. It would contain information to allow a more complete estimate of call activity.

Subclauses 2.2, 2.3 and 2.4 describe the functional components of the *authorization request*, the *request response*, and the *call disposition* messages respectively.

Table 1 validation provides a summary of the functional components and indicates the components which are required and those which are optional. Annex A provides security guidance for validation over X.25 networks.

---

[1] This Recommendation replaces existing Recommendation E.113, Fascicle II.2 *Blue Book*.

Table 1/E.113 – Validation information component summary (Note 1)

Component	Messages		
	Authorization request	**Request response**	**Call disposition (Note 3)**
Message type identifier	R	R	R
Message reference identifier	R	R	R
Primary account number	R	O	R
Card Acceptor identifier	R	–	–
Expiry date	O	–	–
PIN	R (Note 2)	–	–
Service identifier	O	–	–
Calling telephone number	O	–	–
Called telephone number	R	–	–
Time and date stamp	O	–	–
Response code	–	R	–
Customer sub-account number	–	O	–
Restriction indicator	–	O	–
Specified number(s)	–	O	–
Call disposition code	–	–	R
Call start time	–	–	R
Call end time	–	–	R
Estimated call charge	–	–	O
Call duration	–	–	O
Call disposition message indicator	–	–	O

R Required

O Optional

NOTE 1 – Optional items are subject to agreements between Administrations.

NOTE 2 – Required if implemented by the Card Issuer.

NOTE 3 – This entire message is optional and is subject to agreements between Administrations (see 2.4).

2.2 Authorization request

The following describes the basic component of a request from the Card Acceptor to the Card Issuer to validate a charge card and authorize its use.

2.2.1 Message type identifier (required)

A message type identifier should be included in this message. It is provided by the Card Accept or to identify this message to the Card Issuer as the authorization request.

2.2.2 Message reference identifier (required)

A message reference identifier should be included in this message. Its purpose is to uniquely relate this message to a specific validation transaction.

2.2.3 Primary account number (required)

The primary account number (19 visible characters – maximum) of the card as defined in Recommendation E.118 should be included in this message as it was obtained from the card or the user. Part of the primary account number, the issuer identification number, can be used by the Card Acceptor to identify the card and to route the authorization request to the appropriate database.

2.2.4 Card Acceptor issuer identifier (required)

The Card Acceptor identifier should be included in this message and can be used by the Card Issuer to identify the Administration accepting the telecommunication card. The Card Acceptor identifier should contain the issuer identification number of the Card Acceptor.

2.2.5 Expiry date (optional)

The expiry date of the card, if one is specified, may be included in this message. The inclusion of this information should not relieve the Card Acceptor, within the capabilities of its local charge card system, from ensuring that the card has not expired.

2.2.6 Personal Identification Number (PIN) (required)

The use of a PIN is left to the discretion of the Card Issuer. This information can be used by the Card Issuer to authenticate the user and, as applicable, authorize the use of the card. If the Card Issuer has implemented a PIN, it should be included in this message and preferably be encrypted. For telecommunication Card Issuers, it is recommended that the maximum length of the PIN be 6 digits; Card Issuers from other industries may implement PINs of longer length.

2.2.7 Service identifier (optional)

An indication of the service for which the user is charging against their telecommunication charge card should be included in the message. This information will allow the Card Issuer to manage any service-related restrictions against the charge card being used. The information should denote the bearer service and any supplementary services involved in the transaction.

2.2.8 Calling telephone number (optional)

The full international calling telephone number, where available, should be included in this message. As an alternative, the ITU country code may be provided where the calling telephone number is not available. The use of this information is subject to agreements between Administrations. This information is necessary for some Administrations to manage the restricted use of some cards as well as for Card Issuers to ensure that the proper agreements exist to bill, collect, and settle the call. It is also used in the detection of fraud.

2.2.9 Called telephone number (required)

The full international called telephone number should be included in this message. The use of this information is subject to agreements between Administrations. This information is necessary for some Administrations to manage the restricted use of some cards as well as for Card Issuers to ensure that the proper agreements exist to bill, collect and settle the call. It is also used in the detection of fraud.

2.2.10 Time and date stamp (optional)

A time and date stamp should be included in this message. This information should contain the month, day, hour, minute and second in Coordinated Universal Time (UTC), that the *authorization request* is entered into the system.

2.3 Request response

The following describes the basic components of the response from the Card Issuer to an *authorization request.*

2.3.1 Message type identifier (required)

A message type identifier should be included in this message. It is provided by the Card Issuer to identify this message to the Card Acceptor as the request response.

2.3.2 Message reference identifier (required)

A message reference identifier should be included in this message. Its purpose is uniquely to relate this message to a specific validation transaction.

2.3.3 Primary account number (optional)

The primary account number as described in 2.2.3 should be included in this message. It is provided here for closure between the *authorization request* and the *request response*.

2.3.4 Response code (required)

The response code should be included in this message to indicate the result of the *authorization request*. Specific definitions and their corresponding codes are left for further study. Possible conditions for responses may include:

– service approved;

– service approved on a limited basis: see 2.3.6 and 2.3.7;

– service denied: credit threshold exceeded or due to non-payment;

– service denied: invalid account number or invalid account number/PIN combination;

– service denied: incorrect PIN (subsequent attempts to re-enter may be allowable);

– service denied: allowable PIN tries exceeded (each Card Issuer may set limit: e.g. three tries);

– service denied: expired card;

– service denied: restricted account number or account number/PIN combination;

– service denied: service not permitted to this account number;

– service denied: call not permitted from station (i.e. no agreement between Card Issuer and Card Acceptor);

– service denied: Card Issuer validation database is unavailable;

– service denied: validation attempt on wrong Card Issuer;

– error in message format (i.e. message garbled);

– message type not processable due to missing or incomplete information.

Use of, and action on, particular response codes are subject to agreements between concerned Administrations. For some of the above response conditions, separate retry thresholds should be defined.

Any feedback provided to the card user should not assist a fraudulent user in subsequent attempts at unauthorized use of the credit card.

2.3.5 Customer sub-account number (optional)

The customer sub-account number is used to provide the card holder with telecommunication expense control where multiple PIN numbers are associated with a single primary account number. The use of this item is subject to agreement between Administrations and this information is intended to be stored for subsequent inclusion in the billing record so that the billed customer may properly allocate expenses.

2.3.6 Restriction indicator (optional)

The restriction indicator tells the Card Acceptor that the card being used is restricted and provides the nature of the restriction. The use of this item is subject to agreement between Administrations and is provided as a supplement to the response code described above to manage restricted cards.

2.3.7 Specified numbers (optional)

A card holder may be restricted to using the card to call only one or more specified numbers. If the called number is not related to the card's account number, this component would pass that restricted number(s) to the Card Acceptor. The use of this component is subject to agreement between Administrations and is provided as a supplement to the response code described above to manage restricted cards.

2.4 Call disposition (optional)

The following describes the basic components of a response from the Card Acceptor to the Card Issuer to track usage of the card against the customer's credit limit, and gather other statistics to meet operational needs.

The main purpose of this additional message is to provide, on a timely basis, better control over potential fraudulent use of the charge card. It is not meant as a substitute for billing and settlement mechanisms which may be defined by other Recommendations.

2.4.1 Message type identifier (required)

A message type identifier should be included in this message. It is provided by the Card Acceptor to identify this message to the Card Issuer as the call disposition.

2.4.2 Message reference identifier (required)

A message reference identifier should be included in this message. Its purpose is uniquely to relate this message to a specific validation transaction.

2.4.3 Primary account number (required)

The primary account number as described in 2.2.3 should be included in this message. It is provided here for closure between the *authorization request* and the *call disposition*.

2.4.4 Call disposition code (required)

The call disposition code should be included in the message TO INDICATE WHETHER AND HOW, the call WAS completed, or uncompleted.

– automated call to the Card Issuing Administration;

– operator station call to the Card Issuing Administration;

– operator person call to the Card Issuing Administration;

– automated call to a third country;

– operator station call to a third country;

– operator person call to a third country;

– automated call within the Card Acceptor's country;

– operator station call within the Card Acceptor's country;

– operator person call within the Card Acceptor's country;

– unrateable;

– free call;

– fixed charges, e.g. inquiry charges;

– ad hoc (routed through facilities other than via Card Issuer).

2.4.5 Call start time (required)

The date and time at which the call started should be included in this message. If the call disposition code indicates that this call failed, this item of information should indicate the date and time of such failure. The information should contain the month, day, hour and minute in Coordinated Universal Time (UTC).

2.4.6 Call end time (required)

The date and time at which the call ended should be included in this message. This information should contain the month, day, hour and minute in UTC. This parameter may be omitted if 2.4.7 is included in the message.

2.4.7 Call duration (optional)

The duration of the call, in minutes, should be included in this message. This parameter may be omitted if 2.4.6 is included in the message.

2.4.8 Estimated call charge (optional)

The estimated call charge should be included in this message. The charge should be calculated in SDRs.

2.4.9 Call disposition message indicator (optional)

This field specifies whether the call disposition message is being sent at the end of the call or at intervals during the call.

3 Limited validation procedures

The information from the card is presented by the user to an operator. Additional information, defined by the Card Issuer, is also presented to validate, on a limited basis, the card number. The operator, through a set of procedures defined by the Card Issuer, performs this validation function. To the extent possible, Administrations are encouraged to automate the procedures within the operator system or an adjunct device. However, the defined procedures should not be so complicated as to require such automation in order to be practical.

3.1 Types of limited validation procedures

There are several types of validation procedures which might be employed either by themselves or in conjunction with each other. If positive validation is not used, it is strongly recommended that checking against a negative file or black list be employed. If this is not possible then a minimum of one of the following validation procedures must be used:

a) matching of "X" and "Y" digits within the card number;

b) matching of "X" digits in the card number and "Y" digits in the Personal Identification Number (PIN) or other personal identifying information (e.g. the "Authorization Code") that comprise a validation check device;

c) verifying the parity check digit using either the Luhn formula or some other defined algorithm. Note that the verification of the parity check digit is not intended to be the sole means of performing limited validation; the algorithm is sufficiently complicated as to require the automated calculation of the digit.

3.2 Location of personal identifying information

The personal identifying information need not be placed on the card. When such information is included on the card, it should be clearly identified to the user by a term such as "Authorization Code". It may be composed of one or more characters (letters or digits). The user of the card should be instructed to supply the personal identifying information when asked by the operator.

Annex A

Security during validation over an X.25 network

A.1 There are a number of Card Service providers that perform card validation across an X.25 network. This Annex reviews the risks associated with the process and proposes procedures for protection.

In general, validation is performed by sending a validation request to the validation database(s). The request will usually include, as a minimum, the Primary Account Number (PAN), the PIN number and the destination number. The validation database(s) will check the PAN and its format and the PIN number. It will usually check the destination number against allowed numbers (both for the customer and the service). If all checks are satisfied, then the validation database will return a positive response. If there is a failure, then it will usually return an error code indicating the nature of the failure.

The validation network is at risk from the following threats:

- Modification – A validation response could be modified to produce a positive response thus enabling an invalid call to take place.
- Loss of confidentiality – Validation requests could be monitored and PANs and PINs determined. These valid numbers could be used to make unauthorized calls.
- Denial of service – Access to the validation database could be denied causing failure of validation requests. If the service was able to operate in a limited validation mode, unauthorized calls could be made. It may also be possible to exceed pre-set threshold without triggering any alarms (depending upon the mode of operation of the service).

To protect against these threats, the validation process should aim to satisfy the following requirements:

- it should not be possible to read a validation request without authorization;
- it should not be possible to modify a validation request or response without detection;
- it should not be possible to flood the network with messages from a Network User Address (NUA) outside the group of validation databases.

There are a number of measures that may be taken to support the above requirements:

- *Closed User Group (CUG)*

  A CUG enables a pre-defined number of elements to communicate across the network without providing access to other parties. A CUG provides a fairly simple and reasonably effective means for limiting access and would minimize the opportunity for flooding the network from outside the user group. The CUG does not protect the data from eavesdropping or modification in any way.

- *Encryption*

  Encryption will help protect against eavesdropping and provides some protection against modification. It would be very difficult to change the encrypted data without it being detected after decryption.

- *Authentication*

  Authentication would enable change in the validation requests and responses to be detected and would provide verification of the sender’s identity.

A.2 Recommendations

The most significant vulnerability relates to eavesdropping. It is therefore recommended that validation requests are encrypted. Encryption of the validation responses will also help protect against modification. The validation response should be concatenated with some random data. If the validation response is very short and has little variability, i.e. "1" or "0" then the encrypted output will be easier to predict. The X.25 protocol will aid detection of modification through the standard checksums.

Authentication is not recommended as the additional level of security is not really warranted.

A closed user group should be set up if possible as it will help to protect against unauthorized external access to network that might result in disruption of the network and possibly denial of service.

Encryption may be best applied at packet level, i.e. the network layer or at application layer. Network layer encryption will require dedicated X.25 encryption units. Application layer encryption may be implemented in either hardware or software.

Application level encryption is the recommended options as it will enable:

- The encryption algorithm to be changed rapidly if it is believed to be compromised.
- The encryption to be more easily varied where the regulations of the destination country dictate. For example, encryption is not usually permitted in France and the US Government may require the algorithm to be downgraded.

These are two basic types of encryption algorithm for applications of this type:

- An asymmetric algorithm (such as RSA) where one key is used to encrypt the data and a different key (known only to the genuine recipient) is used to decrypt the data.
- A symmetric algorithm (such as DES) where the same key is used to encrypt and decrypt the data. The key should only be known to the sender and the genuine recipient.

If there are only a small number of parties involved then a symmetric algorithm would be appropriate. However, for the international use of a telecommunications charge card, it is likely that many parties could be involved. An asymmetric algorithm is recommended at least when exchanging keys.

A directory of certified keys should be retained by a separate body in case of arbitration and to ensure a verifiable source of keys.

A.3 Validation security procedures

The following practices are recommended:

1) Closed user groups should be used to control access to the X.25 network.
2) Encryption should be applied at application level.
3) An asymmetric encryption algorithm should be used for exchange of keys.
4) Encryption may be restricted to the sensitive data. As a minimum, the following should be encrypted:
   - the PAN;
   - the PIN;
   - the destination number;
   - the "yes"/"no" response from the validation system.

   It is recommended that the originating number is also encrypted to provide an extra level of confidentiality.
5) If a symmetric algorithm is used for encryption of the data then:
   - the keys should be changed for every 100 validations;
   - pseudorandom data (e.g. time in hundredths of seconds) should be concatenated with the validation response.
6) Encryption should add no longer than 50 msec to each validation request/response.
7) A single independent body should be appointed to hold the public key repository. The appointed organization should be the arbitrator in the event of a dispute relating to certified keys.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	**Overall network operation, telephone service, service operation and human factors**
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communication
Series Z	Programming languages