INTERNATIONAL TELECOMMUNICATION UNION

ITU-T E.113

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/93)

TELEPHONE NETWORK AND ISDN

OPERATION, NUMBERING, ROUTING AND MOBILE SERVICE

VALIDATION PROCEDURES FOR THE INTERNATIONAL TELECOMMUNICATIONS CHARGE CARD SERVICE

ITU-T Recommendation E.113

(Previously "CCITT Recommendation")

FOREWORD

The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the International Telecommunication Union. 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, established the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

ITU-T Recommendation E.113 was revised by the ITU-T Study Group I (1988-1993) and was approved by the WTSC (Helsinki, March 1-12, 1993).

NOTES

1 As a consequence of a reform process within the International Telecommunication Union (ITU), the CCITT ceased to exist as of 28 February 1993. In its place, the ITU Telecommunication Standardization Sector (ITU-T) was created as of 1 March 1993. Similarly, in this reform process, the CCIR and the IFRB have been replaced by the Radiocommunication Sector.

In order not to delay publication of this Recommendation, no change has been made in the text to references containing the acronyms "CCITT, CCIR, or IFRB" or their associated entities such as Plenary Assembly, Secretariat, etc. Future editions of this Recommendation will contain the proper terminology related to the new ITU structure.

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

© ITU 1993

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

Recommendation E.113[1)]

VALIDATION PROCEDURES FOR THE INTERNATIONAL TELECOMMUNICATIONS CHARGE CARD SERVICE

(Melbourne, 1988; revised Helsinki, 1993)

Preamble

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.

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 data base, 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 data base, 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.

---

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

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.

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	O	–	–
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

NOTES

1 Optional items are subject to agreements between Administrations.

2 Required if implemented by the Card Issuer.

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 data base.

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 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, when available, 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 for, the call.

2.2.9 Called telephone number (optional)

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.

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 data base 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 combination with each other. These include, but are not limited to:

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;

d) checking against a negative file or black list.

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.