UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

# UIT-T E.113

(05/97)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE E: EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

Explotación, numeración, encaminamiento y servicio móvil – Explotación de las relaciones internacionales – Disposiciones de carácter general relativas a las Administraciones

---

# Procedimientos de validación para el servicio de tarjeta con cargo a cuenta para telecomunicaciones internacionales

Recomendación UIT-T E.113

(Anteriormente Recomendación del CCITT)

---

RECOMENDACIONES DE LA SERIE E DEL UIT-T

## EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

| | |
|---|---|
| ***EXPLOTACIÓN, NUMERACIÓN, ENCAMINAMIENTO Y SERVICIO MÓVIL*** | |
| EXPLOTACIÓN DE LAS RELACIONES INTERNACIONALES | E.100–E.229 |
| Definiciones | E.100–E.103 |
| **Disposiciones de carácter general relativas a las Administraciones** | **E.104–E.119** |
| Disposiciones de carácter general relativas a los usuarios | E.120–E.139 |
| Explotación de las relaciones telefónicas internacionales | E.140–E.159 |
| Plan de numeración del servicio telefónico internacional | E.160–E.169 |
| Plan de encaminamiento internacional | E.170–E.179 |
| Tonos utilizados en los sistemas nacionales de señalización | E.180–E.199 |
| Servicio móvil marítimo y servicio móvil terrestre público | E.200–E.229 |
| DISPOSICIONES OPERACIONALES RELATIVAS A LA TASACIÓN Y A LA CONTABILIDAD EN EL SERVICIO TELEFÓNICO INTERNACIONAL | E.230–E.299 |
| Tasación en el servicio internacional | E.230–E.249 |
| Procedimientos de remuneración de los medios puestos a disposición entre Administraciones | E.250–E.259 |
| Medidas y registro de la duración de las conferencias a efectos de la contabilidad | E.260–E.269 |
| Establecimiento e intercambio de las cuentas internacionales | E.270–E.299 |
| UTILIZACIÓN DE LA RED TELEFÓNICA INTERNACIONAL PARA APLICACIONES NO TELEFÓNICAS | E.300–E.329 |
| Generalidades | E.300–E.319 |
| Telefotografía | E.320–E.329 |
| DISPOSICIONES DE LA RDSI RELATIVAS A LOS USUARIOS | E.330–E.399 |
| ***CALIDAD DE SERVICIO, GESTIÓN DE LA RED E INGENIERÍA DE TRÁFICO*** | |
| GESTIÓN DE LA RED TELEFÓNICA INTERNACIONAL | E.400–E.489 |
| INGENIERÍA DE TRÁFICO | E.490–E.799 |
| CALIDAD DE LOS SERVICIOS DE TELECOMUNICACIÓN: CONCEPTOS, MODELOS, OBJETIVOS, PLANIFICACIÓN DE LA SEGURIDAD DE FUNCIONAMIENTO | E.800–E.899 |

*Para más información, véase la Lista de Recomendaciones del UIT-T.*

**RECOMENDACIÓN UIT-T E.113**

# PROCEDIMIENTOS DE VALIDACIÓN PARA EL SERVICIO DE TARJETA CON CARGO A CUENTA PARA TELECOMUNICACIONES INTERNACIONALES


## Resumen

La utilización generalizada y el creciente número de tarjetas con cargo a cuenta requiere que los expedidores de tarjetas (o sus representantes autorizados) apliquen medidas de seguridad adecuadas contra el uso fraudulento.

Por tanto, un aspecto crítico en la provisión de este sistema es la capacidad de asegurar la validez de la tarjeta y su utilización autorizada de una manera uniforme. El objetivo de esta Recomendación es definir los procedimientos para el proceso de validación entre Administraciones. En este proceso, no se trata de especificar equipos, facilidades ni técnicas de transmisión de datos.


## Orígenes

La Recomendación UIT-T E.113, ha sido revisada por la Comisión de Estudio 1 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 26 de mayo de 1997.

# PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución N.° 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido/no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

# ÍNDICE

## Introducción

Se está trabajando en el desarrollo del servicio de tarjeta con cargo a cuenta para telecomunicaciones internacionales definido en la Recomendación E.116.

La utilización generalizada y el creciente número de tarjetas con cargo a cuenta requiere que los expedidores de tarjetas (o sus representantes autorizados) apliquen medidas de seguridad adecuadas contra el uso fraudulento.

Por tanto, un aspecto crítico en la provisión de este sistema es la capacidad de asegurar la validez de la tarjeta y su utilización autorizada de una manera uniforme. El objetivo de esta Recomendación es definir los procedimientos para el proceso de validación entre Administraciones. En este proceso, no se trata de especificar equipos, facilidades ni técnicas de transmisión de datos.

Debe reconocerse que los procedimientos de validación entre Administraciones de las tarjetas con cargo a cuenta para telecomunicaciones variarán según factores tales como las capacidades de los sistemas de tarjetas, acuerdos bilaterales y la forma en que se presentan éstas. Debe mantenerse la flexibilidad de este proceso a fin de maximizar la participación de las Administraciones cuando se carezca de interfaces automatizadas o no estén uniformemente disponibles. Cuando existan interfaces automatizadas, es conveniente una implantación uniforme y definida.

**Recomendación E.113**[1]

# PROCEDIMIENTOS DE VALIDACIÓN PARA EL SERVICIO DE TARJETA CON CARGO A CUENTA PARA TELECOMUNICACIONES INTERNACIONALES

*(Melbourne, 1988; revisada en 1993 y 1997)*

## 1 Métodos de validación

Existen varios métodos para comprobar la validez de las tarjetas con cargo a cuenta, que pueden dividirse en dos categorías generales: validación completa y validación limitada.

La validación completa requiere la comprobación del número de la tarjeta con la base de datos del expedidor de la misma, así como una comunicación en tiempo real entre el aceptador y el expedidor de la tarjeta. La validación completa es más detallada que otros métodos y resulta práctica con los sistemas de tarjetas de cuenta automatizados o semiautomatizados.

La validación limitada puede exigir una o más técnicas, como por ejemplo, un carácter especial, un código o una verificación con una base de datos parcial determinada por el expedidor de la tarjeta y definida en un acuerdo de servicio. Los métodos de validación limitada reducen al mínimo la necesidad de comunicación entre las Administraciones.

## 2 Procedimientos de validación completa

### 2.1 Flujo de información de validación

La información de la tarjeta y/o del usuario se presenta a un terminal que tiene acceso al sistema local de tarjetas con cargo a cuenta para telecomunicaciones de una Administración. Dicho sistema debe comunicar con el expedidor de la tarjeta para validarla y autorizar su utilización.

El flujo de información de validación comprende tres mensajes:

– petición de autorización;

– respuesta a la petición;

– disposiciones para la llamada.

La petición de autorización es un mensaje enviado por el aceptador de la tarjeta al expedidor de la tarjeta, que proporciona detalles sobre un intento de utilizar una tarjeta con cargo a cuenta de telecomunicación. Esto permite al expedidor de la tarjeta interrogar a sus propios sistemas internos a fin de responder al aceptador. El expedidor de la tarjeta debe comunicar seguidamente con el aceptador dándole una respuesta positiva o negativa (indicando en este último caso los motivos específicos por los que no se concede la autorización) a la petición de autorización. Este mensaje se define aquí como la respuesta a la petición. A continuación debe devolverse al usuario de la tarjeta información en la medida de lo posible, según las capacidades del sistema telefónico de la Administración de que se trate, sobre la situación del intento de llamada. Tras completar una llamada o un intento de llamada, y a reserva de los acuerdos existentes entre las Administraciones y los expedidores de tarjetas, el aceptador de la tarjeta enviará oportunamente al expedidor de la misma un tercer mensaje denominado disposiciones para la llamada. Este mensaje contendrá información que permita evaluar de forma más completa la actividad de la llamada.

En las subcláusulas 2.2, 2.3 y 2.4 se describen los componentes funcionales de los mensajes de *petición de autorización*, *respuesta a la petición* y *disposiciones para la llamada*, respectivamente.

En el cuadro 1 se muestra un resumen de los componentes funcionales y se indican los componentes que se requieren y los que pueden ser facultativos. En el anexo A se ofrece orientación relativa a la seguridad para la validación en redes X.25.

---

[1] Esta Recomendación sustituye a la actual Recomendación E.113 del fascículo II.2 del *Libro Azul*.

**Cuadro 1/E.113 – Resumen de los componentes de información de validación (véase la nota 1)**

| Componente | Mensajes | | |
|---|---|---|---|
| | **Petición de autorización** | **Respuesta a la petición** | **Disposiciones para la llamada (nota 3)** |
| Identificador del tipo de mensaje | R | R | R |
| Identificador de referencia del mensaje | R | R | R |
| Número de cuenta primario | R | O | R |
| Identificador del aceptador de la tarjeta | R | – | – |
| Fecha de caducidad | O | – | – |
| Número de identificación personal (PIN) | R (nota 2) | – | – |
| Identificador del servicio | O | – | – |
| Número telefónico llamante | O | – | – |
| Número telefónico llamado | R | – | – |
| Sello de fecha y hora | O | – | – |
| Código de respuesta | – | R | – |
| Número de subcuenta del cliente | – | O | – |
| Indicador de restricciones | – | O | – |
| Número o números especificados | – | O | – |
| Código de disposiciones para la llamada | – | – | R |
| Inicio de la llamada | – | – | R |
| Fin de la comunicación | – | – | R |
| Importe estimado de la comunicación | – | – | O |
| Duración de la llamada | – | – | O |
| Indicador de mensaje de disposición para la llamada | – | – | O |

R Requerido (*required*)

O Facultativo (*optional*)

NOTA 1 – Los elementos optativos están sujetos a acuerdos entre las Administraciones.

NOTA 2 – Requerido si es utilizado por el expedidor de la tarjeta.

NOTA 3 – Todo mensaje es optativo y está sujeto a acuerdos entre las Administraciones (véase 2.4).

## 2.2 Petición de autorización

A continuación se describen los componentes básicos de una petición del aceptador de la tarjeta al expedidor de la tarjeta para validar una tarjeta con cargo a cuenta y autorizar su utilización.

### 2.2.1 Identificador del tipo de mensaje (requerido)

Este mensaje debe incluir un identificador del tipo de mensaje que proporciona el aceptador de la tarjeta para identificar el mensaje ante el expedidor de la tarjeta como la petición de autorización.

### 2.2.2 Identificador de referencia del mensaje (requerido)

Este mensaje debe incluir un identificador de referencia del mensaje. Su finalidad es relacionar exclusivamente este mensaje con una transacción de validación específica.

### 2.2.3 Número de cuenta primario (requerido)

El número de cuenta primario de la tarjeta (19 caracteres visibles como máximo) definido en la Recomendación E.118 debe incluirse en este mensaje según fue obtenido de la tarjeta o del usuario. Parte del número de cuenta primario, el número de identificación del expedidor, puede ser utilizado por el aceptador de la tarjeta para identificar la tarjeta y encaminar la petición de autorización a la base de datos adecuada.

### 2.2.4 Identificador del aceptador/expedidor de la tarjeta (requerido)

En este mensaje debe figurar el identificador del aceptador de la tarjeta, que puede ser utilizado por el expedidor de la tarjeta para identificar a la Administración que acepta la tarjeta con cargo a cuenta para telecomunicaciones. El identificador del aceptador de la tarjeta debe llevar el número de identificación del expedidor del aceptador de la tarjeta.

### 2.2.5 Fecha de caducidad (facultativo)

La fecha de caducidad de la tarjeta, si se especifica, podrá incluirse en este mensaje. La inclusión de esta información no exime al aceptador de la tarjeta, dentro de las posibilidades del sistema local de tarjetas con cargo a cuenta, de confirmar que la tarjeta no ha caducado.

### 2.2.6 Número de identificación personal (PIN, personal identification number) (requerido)

La utilización de un PIN queda a discreción del expedidor de la tarjeta. Éste puede utilizar dicha información para autenticar al usuario y, en su caso, autorizar la utilización de la tarjeta. Si existe un número de identificación personal, debe incluirse en este mensaje y preferentemente cifrado. Para los expedidores de tarjetas de telecomunicaciones, se recomienda que la longitud máxima del PIN sea de seis cifras; los expedidores de tarjetas de otras industrias pueden utilizar números PIN de mayor longitud.

### 2.2.7 Identificador del servicio (facultativo)

El mensaje debe incluir una indicación del servicio que se carga al usuario en su tarjeta con cargo a cuenta de telecomunicación. Esta información permitirá al expedidor de la tarjeta controlar cualesquiera restricciones relativas al servicio que se carga a su tarjeta con cargo a cuenta. La información debe indicar el servicio portador y cualesquiera servicios suplementarios que intervengan en la transacción.

### 2.2.8 Número telefónico llamante (facultativo)

En este mensaje debe incluirse el número internacional completo del teléfono llamante, cuando se dispone de él. De manera alternativa, puede proporcionarse el indicativo de país de la UIT cuando no se disponga del número telefónico llamante. La utilización de este dato está sujeta a acuerdos bilaterales entre Administraciones. Algunas Administraciones necesitan esta información para controlar la utilización restringida de algunas tarjetas, y los expedidores de las tarjetas, para cerciorarse de la existencia de acuerdos bilaterales al efecto, con vistas a la facturación, cobro y liquidación de la comunicación. También se utiliza para la detección de fraudes.

### 2.2.9 Número telefónico llamado (requerido)

Debe incluirse en el mensaje el número internacional completo del teléfono llamado. El empleo de esta información está sujeto a acuerdos bilaterales entre Administraciones. Algunas Administraciones necesitan esta información para controlar la utilización restringida de algunas tarjetas, y también los expedidores de las tarjetas, para cerciorarse de la existencia de acuerdos bilaterales al efecto con vistas a la facturación, cobro y liquidación de la comunicación. También se utiliza para la detección de fraudes.

### 2.2.10 Sello de fecha y hora (facultativo)

El mensaje debe incluir un sello de fecha y hora. Esta información debe incluir el mes, día, hora, minuto y segundo, en tiempo universal coordinado (UTC, *coordinated universal time*), en que la *petición de autorización* se introduce en el sistema.

## 2.3 Respuesta a la petición

A continuación se describen los componentes básicos de la respuesta que da el expedidor de la tarjeta a una *petición de autorización*.

### 2.3.1 Identificador del tipo de mensaje (requerido)

En este mensaje debe incluirse un identificador del tipo de mensaje proporcionado por el expedidor de la tarjeta para identificar este mensaje al aceptador de la tarjeta como respuesta a la petición.

### 2.3.2 Identificador de referencia del mensaje (requerido)

En este mensaje debe incluirse un identificador de referencia del mensaje. Su finalidad es relacionar en forma unívoca este mensaje con una transacción de validación específica.

### 2.3.3 Número de cuenta primario (facultativo)

En este mensaje debe incluirse el número de cuenta primario descrito en 2.2.3. Aparece aquí para cerrar la operación entre la *petición de autorización* y la *respuesta a la petición*.

### 2.3.4 Código de respuesta (requerido)

Este mensaje debe incluir un código de respuesta que indique el resultado de la *petición de autorización*. Las definiciones específicas y sus correspondientes códigos quedan en estudios. Las posibles condiciones de respuesta son:

– servicio aprobado;

– servicio aprobado de forma limitada: véanse 2.3.6 y 2.3.7;

– servicio denegado: por límite de crédito excedido o por falta de pago;

– servicio denegado: el número de la cuenta o la combinación número de cuenta/PIN no son válidos;

– servicio denegado: PIN incorrecto (pueden autorizarse nuevas tentativas de reintroducción);

– servicio denegado: se exceden las tentativas permitidas para el PIN (cada Administración expedidora de tarjetas debe fijar un límite, por ejemplo, tres tentativas);

– servicio denegado: tarjeta caducada;

– servicio denegado: el número de cuenta o la combinación número de cuenta/PIN son restringidos;

– servicio denegado: no está permitido el servicio a ese número de cuenta;

– servicio denegado: no esta permitida la llamada desde esa estación (por ejemplo, no existe acuerdo entre el expedidor de la tarjeta y el aceptador de la misma);

– servicio denegado: no hay acceso a la base de datos del expedidor de la tarjeta para la validación;

– servicio denegado: la tentativa de validación se ha realizado ante un expedidor de tarjetas erróneo;

– error en el formato del mensaje (por ejemplo, mensaje ininteligible);

– tipo de mensaje no procesable debido a información inexistente o incompleta.

La utilización de códigos de respuesta particulares y la adopción de medidas respecto de los mismos están sujetas a acuerdos entre las Administraciones interesadas. Para algunas de las condiciones de respuesta mencionadas deben definirse límites separados para los intentos sucesivos.

La información devuelta al usuario de la tarjeta no debe ayudar a un usuario fraudulento a realizar nuevas tentativas de utilización no autorizada de la tarjeta de crédito.

#### 2.3.5 Número de subcuenta del cliente (facultativo)

El número de subcuenta del cliente permite al titular de la tarjeta controlar los gastos de telecomunicación cuando un número de cuenta primario tiene asociados varios PIN. La utilización de este elemento está sujeta a acuerdos entre las Administraciones y esta información debe almacenarse para incluirse posteriormente en la factura de forma que el cliente pueda situar adecuadamente dichos gastos.

#### 2.3.6 Indicador de restricciones (facultativo)

Indica al aceptador de la tarjeta que su utilización está restringida, señalando la índole de la restricción. El empleo de este indicador está sujeto a acuerdos entre Administraciones y se ofrece como suplemento al código de respuesta descrito anteriormente para controlar las tarjetas restringidas.

#### 2.3.7 Número o números especificados (facultativo)

Un titular de tarjeta puede tener limitada su utilización para llamar únicamente a uno o más números específicos. Si el número al que se ha llamado no corresponde al número de cuenta de la tarjeta, este elemento pasará dicho número o números restringidos al aceptador de la tarjeta. El empleo de este elemento está sujeto a acuerdos entre Administraciones y se ofrece como suplemento al código de respuesta indicado anteriormente para controlar las tarjetas restringidas.

### 2.4 Disposiciones para la llamada (facultativo)

A continuación se describen los componentes básicos de la respuesta del aceptador de la tarjeta al expedidor de la tarjeta, para que su utilización quede reflejada en el límite del crédito del cliente y para recoger otros datos estadísticos a fin de satisfacer las necesidades de explotación.

La principal finalidad de este mensaje adicional es permitir, en el momento oportuno, un mejor control del posible uso fraudulento de la tarjeta con cargo a cuenta. No tiene por objeto sustituir los mecanismos de facturación y liquidación que se definan en otras Recomendaciones.

#### 2.4.1 Identificador de tipo de mensaje (requerido)

En este mensaje debe incluirse un identificador del tipo de mensaje que proporciona el aceptador de la tarjeta para identificar el mensaje ante el expedidor de la tarjeta como la disposición de la llamada.

#### 2.4.2 Identificador de referencia del mensaje (requerido)

En este mensaje debe incluirse un identificador de referencia del mensaje. Su finalidad es la de relacionar exclusivamente este mensaje con una transacción válida específica.

#### 2.4.3 Número de cuenta primario (requerido)

En este mensaje debe incluirse el número de cuenta primario que se describe en 2.2.3. Aparece aquí para cerrar la operación entre los mensajes *petición de autorización* y *disposiciones para la llamada*.

#### 2.4.4 Código de disposiciones para la llamada (requerido)

El código de disposiciones para la llamada debe incluirse en el mensaje PARA INDICAR SI Y COMO se completó o no se completó la llamada.

– llamada automatizada a la Administración expedidora de la tarjeta;

– llamada de teléfono a teléfono por operadora a la Administración expedidora de la tarjeta;

– llamada de persona a persona por operadora a la Administración expedidora de la tarjeta;

– llamada automatizada a un tercer país;

– llamada de teléfono a teléfono por operadora a un tercer país;

– llamada de persona a persona por operadora a un tercer país;

– llamada automatizada dentro del país aceptador de la tarjeta;

– llamada de teléfono a teléfono por operadora dentro del país aceptador de la tarjeta;

– llamada de persona a persona por operadora dentro del país aceptador de la tarjeta;

– no estimable;

– llamada gratuita;

– tarifa invariable, por ejemplo, por una petición de información;

– ad hoc (encaminada por facilidades distintas de las del expedidor de la tarjeta).

#### 2.4.5 Inicio de la llamada (requerido)

Este mensaje debe incluir la fecha y la hora de comienzo de la llamada. Si el código de disposición de la llamada indica que la comunicación no se ha establecido, este elemento de información debe indicar la fecha y la hora de esta tentativa fallida. La información incluirá el mes, día, hora y minuto, en tiempo universal coordinado (UTC).

#### 2.4.6 Fin de la comunicación (requerido)

Este mensaje debe indicar la fecha y la hora de fin de la comunicación. Esta información incluirá el mes, día, hora y minuto, en tiempo UTC. Este parámetro podrá omitirse si se incluye 2.4.7 en el mensaje.

#### 2.4.7 Duración de la llamada (facultativo)

Este mensaje debe incluir la duración de la llamada, en minutos. Este parámetro podrá omitirse si se incluye 2.4.6 en el mensaje.

#### 2.4.8 Importe estimado de la comunicación (facultativo)

Este mensaje debe incluir el importe estimado de la comunicación. El importe debe calcularse en derechos especiales de giro.

#### 2.4.9 Indicador de mensaje de disposiciones para la llamada (facultativo)

Este campo especifica si el mensaje de disposiciones para la llamada está siendo enviado al final de la llamada o a intervalos durante la misma.

## 3 Procedimientos de validación limitada

El usuario presenta la información de la tarjeta a una operadora. Para validar, de forma limitada, el número de la tarjeta, también se presenta la información adicional definida por el expedidor de la tarjeta. La operadora, mediante un conjunto de operaciones definidas por el expedidor de la tarjeta, lleva a cabo esta función de validación. Se recomienda a las Administraciones que, en la medida posible, automaticen las operaciones en el sistema de operadora o en un dispositivo adjunto. Las operaciones definidas no deben ser tan complicadas como para que su puesta en práctica exija la automatización.

### 3.1 Tipos de procedimientos de validación limitada

Existen diversos tipos de procedimientos de validación que pueden emplearse por separado o combinados entre sí. Si no se utiliza la validación positiva, se recomienda decididamente la confrontación con un fichero negativo o lista negra. Si esto no es posible, se debe utilizar como mínimo uno de los siguientes procedimientos de validación:

a) concordancia de las cifras "X" e "Y" en el número de la tarjeta;

b) concordancia de las cifras "X" en el número de la tarjeta y de las cifras "Y" en el número de identificación personal (PIN) u otra información de identificación personal (por ejemplo, el "código de autorización") que comprende un dispositivo de comprobación de validación;

c) verificación de la cifra de comprobación de paridad utilizando la fórmula de Luhn o algún otro algoritmo definido. Obsérvese que no se pretende que la verificación de la cifra de comprobación de paridad sea el único medio de llevar a cabo la validación limitada; el algoritmo es suficientemente complicado para exigir el cálculo automatizado de la cifra.

### 3.2 Ubicación de la información de identificación personal

No es necesario introducir en la tarjeta la información de identificación personal. Cuando dicha información se incluye en la tarjeta, debe ser identificada claramente al usuario mediante un término tal como "código de autorización". Puede estar compuesta de uno o más caracteres (letras o cifras). Debe indicarse al usuario de la tarjeta que tiene que proporcionar el número de identificación personal a la operadora cuando se lo solicite.

## Anexo A

## Seguridad durante la validación en una red X.25

**A.1** Hay algunos proveedores de servicio de tarjeta que realizan la validación de la tarjeta en una red X.25. En este anexo se examinan los riesgos asociados a este proceso y se proponen procedimientos de protección.

En general, la validación se lleva a cabo enviando una petición a la(s) base(s) de datos de validación. La petición de validación incluirá, como mínimo, el número de cuenta primario (PAN, *primary account number*), el número PIN y el número de destino. La(s) base(s) de datos de validación comprobará(n) el PAN y su formato, y el número PIN. Normalmente comprobarán el número de destino con relación a los números permitidos (tanto para el cliente como para el servicio). Si se satisfacen todas las comprobaciones, la base de datos de validación devolverá una respuesta positiva. Si hay un fallo, normalmente devolverá un código de error que indica la naturaleza del fallo.

La red de validación tiene riesgos derivados de las amenazas siguientes:

- Modificación – Una respuesta de validación podría modificarse para arrojar una respuesta positiva permitiendo así que tenga lugar una llamada no válida.
- Pérdida de confidencialidad – Las peticiones de validación podrían ser supervisadas y determinarse los PAN y los PIN. Estos números válidos podrían ser utilizados para realizar llamadas no autorizadas.
- Rechazo de servicio – Podría rechazarse el acceso a la base de datos de validación en razón del fallo de las peticiones de validación. Si el servicio pudo operar en una modalidad de validación limitada, podrían realizarse llamadas no autorizadas. También se podría exceder el umbral fijado de antemano sin activar alarmas (en función de la modalidad de operación del servicio).

Como protección contra esta amenaza, el proceso de validación debe aspirar a satisfacer los requisitos siguientes:

- no debe ser posible leer una petición de validación sin autorización;
- no debe ser posible modificar una petición o respuesta de validación sin detección;
- no debe ser posible inundar la red de mensajes desde una dirección de usuario de red (NUA, *network user address*) fuera del grupo de bases de datos de validación.

Son varias las medidas que pueden adoptarse para sustentar los requisitos citados.

- *Grupo cerrado de usuarios* (*CUG, closer user group*)

  Un CUG permite a un número de elementos predefinido comunicarse por la red sin proporcionar acceso a otras partes. Un CUG constituye un medio bastante simple y razonablemente efectivo para limitar el acceso y reducir al mínimo la oportunidad de inundar la red desde fuera del grupo de usuarios. El CUG no protege en modo alguno la red contra la extracción ilegal o modificación de los datos.

- *Cifrado*

  El cifrado protege la red contra la extracción furtiva de datos y proporciona cierta protección a la modificación. Sería muy difícil modificar los datos cifrados sin que se detecte después del descifrado.

- *Autenticación*

  La autenticación permitiría que se detecte todo cambio en las peticiones y respuestas de validación y proporcionaría verificación de la identidad de los emisores.

## A.2 Recomendaciones

La vulnerabilidad más importante se relaciona con la extracción furtiva de datos. Por ello se recomienda que las peticiones de validación estén cifradas. El cifrado de las respuestas de validación también contribuirá a la protección contra la modificación. La respuesta de validación debería concatenarse con ciertos datos aleatorios. Si la respuesta de validación es muy breve y tiene escasa variabilidad, por ejemplo "1" ó "0", la salida cifrada será más fácil de predecir. El protocolo X.25 contribuirá a la detección de las modificaciones mediante las sumas de verificación estándar.

*No se recomienda la autenticación pues el nivel de seguridad adicional no está realmente garantizado.*

Debe crearse, en lo posible, un grupo cerrado de usuarios pues contribuirá a la protección contra el acceso externo no autorizado a la red, pudiendo producir la interrupción de la red y quizás el rechazo del servicio.

Conviene aplicar el cifrado al nivel de paquetes, es decir de capa de red o de capa de aplicación. El cifrado de capa de red exigirá unidades de cifrado X.25 especializadas. El cifrado de la capa de aplicación puede llevarse a cabo al nivel de soporte físico o de soporte lógico.

La opción recomendada es el cifrado a nivel de la aplicación, pues permite:

- Un rápido cambio del algoritmo de cifrado si se considera que está en peligro.
- Que el cifrado pueda variarse más fácilmente cuando así lo exijan las disposiciones del país de destino. Por ejemplo, en Francia no se permite normalmente el cifrado y el Gobierno de los Estados Unidos puede exigir la presentación del algoritmo en claro.

Existen dos tipos básicos de algoritmo de cifrado para este tipo de aplicaciones:

- Un algoritmo asimétrico (como RSA) en el que se utiliza una clave para cifrar los datos y otra clave diferente (únicamente conocida por el destinatario legítimo) para descifrar los datos.
- Un algoritmo simétrico (como DES) en el que se utiliza la misma clave para cifrar y descifrar los datos. La clave debe ser conocida únicamente por el emisor y por el destinatario legítimo.

Si sólo participa un reducido número de partes, lo apropiado sería un algoritmo simétrico. Sin embargo, para el uso de una tarjeta con cargo a cuenta para telecomunicaciones internacionales, es probable que concurran muchas partes. Se recomienda un algoritmo asimétrico al menos cuando se intercambian claves.

Un órgano independiente debe mantener una guía de claves certificadas para casos de arbitraje y para asegurar una fuente de claves verificable.

## A.3 Procedimientos de seguridad de la validación

Se recomiendan las siguientes prácticas:

1) Deben utilizarse grupos cerrados de usuarios para controlar el acceso a la red X.25.
2) El cifrado debe aplicarse a nivel de la aplicación.
3) Debe utilizarse un algoritmo de cifrado asimétrico para el intercambio de claves.
4) El cifrado puede limitarse a los datos sensibles. Debe cifrarse por lo menos lo siguiente:
   - el PAN;
   - el PIN;
   - el número de destino;
   - la respuesta "sí"/"no" del sistema de validación.

   Se recomienda que se cifre asimismo el número de origen para proporcionar un nivel de confidencialidad adicional.
5) Si para el descifrado de los datos se utiliza un algoritmo simétrico:
   - las claves deben cambiarse cada 100 validaciones;
   - los datos seudoaleatorios (por ejemplo el tiempo en centésimas de segundo) deben concatenarse con la respuesta de validación.
6) El cifrado debe agregar no más de 50 milisegundos a cada petición/respuesta de validación.
7) Debe designarse un único órgano independiente que mantenga el depósito de la clave pública. La organización designada debe ejercer el arbitraje si surgen disputas en relación a claves certificadas.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie B | Medios de expresión: definiciones, símbolos, clasificación |
| Serie C | Estadísticas generales de telecomunicaciones |
| Serie D | Principios generales de tarificación |
| **Serie E** | **Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos** |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y multimedios |
| Serie I | Red digital de servicios integrados |
| Serie J | Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios |
| Serie K | Protección contra las interferencias |
| Serie L | Construcción, instalación y protección de los cables y otros elementos de planta exterior |
| Serie M | RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de transmisión telefónica, instalaciones telefónicas y redes locales |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos y comunicación entre sistemas abiertos |
| Serie Z | Lenguajes de programación |