

# UIT-T

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

# Y.2741

(01/2011)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA  
INFORMACIÓN, ASPECTOS DEL PROTOCOLO  
INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Seguridad

---

## **Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación**

Recomendación UIT-T Y.2741

RECOMENDACIONES UIT-T DE LA SERIE Y  
**INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET  
Y REDES DE LA PRÓXIMA GENERACIÓN**

**INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN**

Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899

**ASPECTOS DEL PROTOCOLO INTERNET**

Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999

**REDES DE LA PRÓXIMA GENERACIÓN**

Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
Redes futuras	Y.3000–Y.3099

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

## Recomendación UIT-T Y.2741

### Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación

#### Resumen

En la Recomendación UIT-T Y.2741 se especifica la arquitectura general de seguridad para las transacciones comerciales y bancarias móviles en el contexto de las NGN. Se describen los principales participantes, su función, y las hipótesis operativas de los sistemas comerciales y bancarios móviles. También se presentan ejemplos de aplicación de modelos de sistemas comerciales y bancarios móviles.

#### Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T Y.2741	2011-01-28	13

#### Palabras clave

Banca móvil, comercio móvil, pago móvil, pagos a distancia, pagos móviles, seguridad.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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 Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), 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 1 de la AMNT.

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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## 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 en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2011

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	1
3.1    Términos definidos en otros documentos.....	1
3.2    Términos definidos en esta Recomendación .....	1
4 Abreviaturas y acrónimos .....	2
5 Convenios .....	2
6 Funciones, riesgos, participantes y posibilidades de pago móvil en las NGN .....	2
6.1    Funciones dentro de los sistemas de comercio móvil y de banca móvil .....	2
6.2    Riesgos en el MPS y niveles de seguridad del MPS .....	3
6.3    Participantes y arquitectura del sistema de comercio móvil y de banca móvil.....	3
6.4    Ejemplos de utilización del sistema de pagos móviles.....	5
7 Transición desde los sistemas de pago por testigo .....	15
Apéndice I – Ingreso de un instrumento de pago en el sistema.....	16
Apéndice II – Modelos de aplicación del sistema de banca móvil y de comercio móvil .....	18
II.1    Sistema sin aplicación de cliente.....	19
II.2    Sistema con aplicación de cliente.....	19
Bibliografía .....	21



## Recomendación UIT-T Y.2741

### Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación

#### 1 Alcance

En esta Recomendación se define la arquitectura de seguridad para las transacciones financieras móviles a distancia en las NGN. Se excluyen todas las demás transacciones financieras, así como aquéllas que utilizan testigos monetarios y no monetarios para transferir valores.

Al organizar una amplia gama de servicios mediante funciones de gestión y personalización flexibles, las NGN pueden ofrecer un cómodo acceso a los servicios del sistema de pago móvil (MPS).

#### 2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T Y.2740] Recomendación UIT-T Y.2740 (2011), *Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación (NGN)*.

#### 3 Definiciones

##### 3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

**3.1.1 red de la próxima generación (NGN)** [b-UIT-T Y.2001]: Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios.

##### 3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

**3.2.1 aplicación:** aplicación especial de banca móvil o comercio móvil telecargada en el dispositivo móvil del cliente (usuario).

**3.2.2 cuenta bancaria:** cuenta de fondos electrónica perteneciente a una persona física o moral en un banco u otro tipo de institución financiera autorizada por la autoridad monetaria nacional (por ejemplo, banco central), que puede emplearse para el pago de bienes y servicios.

**3.2.3 cliente:** persona física o moral que firmado un acuerdo contractual que rige la utilización de servicios de telecomunicaciones y del sistema de comercio móvil.

**3.2.4 transacción financiera:** evento o condición prevista en los términos del contrato establecido entre un comprador y un vendedor a fin de ofrecer un bien a cambio de un pago.

**3.2.5 entorno intersistemas:** conjunto de normas o sistema que permite la interacción de diversos sistemas de banca móvil y de comercio móvil.

**3.2.6 dispositivo móvil:** dispositivo electrónico utilizado para establecer telecomunicaciones a través de una red NGN inalámbrica.

**3.2.7 transacción financiera móvil:** transacción financiera iniciada y/o autorizada mediante un dispositivo móvil.

**3.2.8 sistema de pago móvil (MPS):** sistemas de banda móvil y/o de comercio móvil

**3.2.9 testigo monetario:** artefacto electrónico o físico utilizado para realizar un pago, representado por las unidades monetarias nacionales, y que las utiliza, que no obstante no está almacenado ni directamente ligado a una cuenta bancaria.

Como ejemplo de testigo monetario electrónico se puede citar el efectivo electrónico almacenado en una cartera electrónica independiente, sin correspondencia en la cuenta bancaria. Los testigos monetarios físicos son, por ejemplo, las monedas, los billetes, los cheques de viaje, etc.

**3.2.10 testigo no monetario:** artefacto electrónico o físico utilizado para realizar un pago, pero que no utiliza las unidades monetarias nacionales. Como ejemplo de testigos no monetarios electrónicos pueden citarse los "minutos" no utilizados o los "mensajes SMS" restantes en la cuenta del abonado a la NGN, que los operadores permiten que se transfieran de una cuenta de abonado a otra.

**3.2.11 identificador de pago (ID de pago):** parámetro de petición necesario que identifica explícitamente al receptor del pago. El identificador mercante (ID mercante) y el ID MPS (identificador unívoco de un sistema de pago móvil) han de estar presentes en la aplicación del entorno intersistemas.

## 4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las abreviaturas y acrónimos siguientes:

DB Base de datos (*database*)

ID Identificación (*identification*)

IS Sistema informático (*information system*)

MPS Sistema de pago móvil (*mobile payment system*)

NGN Red de la próxima generación (*next generation network*)

## 5 Convenios

Ninguno.

## 6 Funciones, riesgos, participantes y posibilidades de pago móvil en las NGN

### 6.1 Funciones dentro de los sistemas de comercio móvil y de banca móvil

Las funciones básicas de los participantes en el MPS y sus responsabilidades son:

- El cliente es un abonado móvil que posee un instrumento de pago para efectuar pagos.



- La aplicación de cliente es el software especial telecargado en el dispositivo móvil de cliente (teléfono, tarjeta SIM, comunicador, etc.) y diseñado para realizar operaciones de pago móvil seguras.
- El instrumento de pago es un instrumento financiero utilizado para efectuar pagos a cambio de bienes y servicios.
- El operador NGN facilita la red de comunicación móvil para la interacción a distancia del cliente con el MPS, el encaminamiento de los datos y la transferencia.
- El distribuidor de aplicaciones de cliente es un participante que pone las aplicaciones a disposición de los clientes.
- El proveedor de seguridad es un participante que asegura la transferencia de los datos a través de los canales de comunicación.
- El operador MPS (proveedor de servicio, pasarela de pago) es un participante que garantiza la interacción dentro del MPS y ofrece servicios de pago al usuario extremo.
- El emisor es una institución financiera que emite instrumentos de pago.
- El proveedor de autenticación de cliente valida las operaciones de cliente.
- El aval es una institución financiera que mantiene relaciones mercantiles y recibe todas las transacciones financieras del comerciante.
- El sistema de pago es una organización que garantiza las transacciones de pago interbancarias.

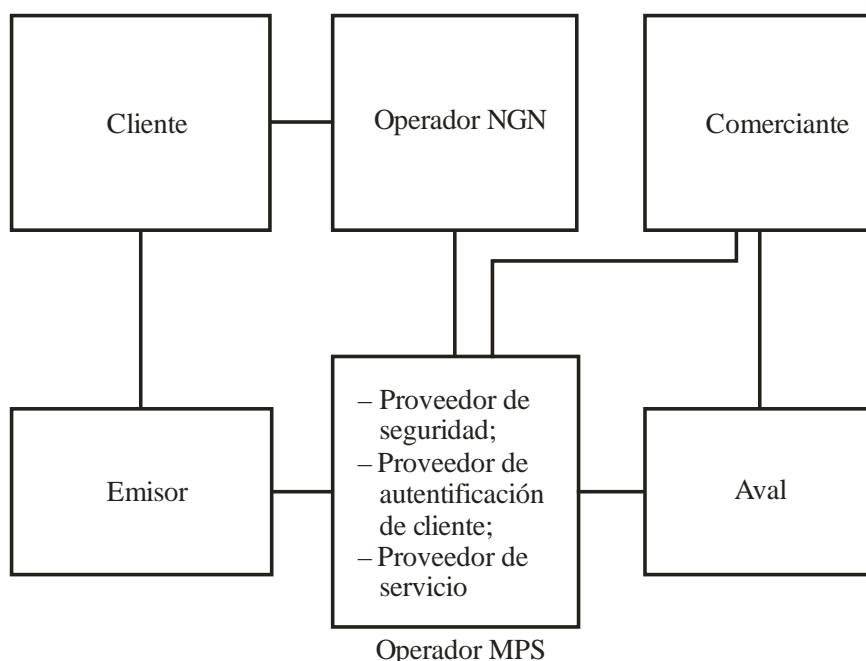
## **6.2 Riesgos en el MPS y niveles de seguridad del MPS**

En esta cláusula se describen de manera no exhaustiva los riesgos de seguridad informática básicos que se pueden correr al realizar pagos móviles a distancia:

- Riesgo de peligro para la confidencialidad – un tercero no autorizado accede a información confidencial.
- Riesgo de peligro para la integridad – distorsión de la información durante su transferencia o procesamiento.
- Riesgo de falsificación de documentos electrónicos – una parte no autorizada genera un documento.
- Riesgo de repudio – denegación de la autoría de un documento electrónico.
- Riesgo de destrucción de la información, voluntaria o involuntariamente.
- Riesgo de transacción – imposibilidad de finalizar una transacción (por ejemplo, a causa de la inestabilidad de la comunicación móvil).
- Dependiendo de los mecanismos de seguridad en función de los riesgos aplicados, hay sistemas con cuatro niveles de seguridad [UIT-T Y.2740].

## **6.3 Participantes y arquitectura del sistema de comercio móvil y de banca móvil**

La arquitectura del MPS ha de ajustarse al sistema de interrelaciones entre organizaciones financieras, jurídicas y comerciales existente y permitir a sus participantes efectuar transacciones de pago móvil con el grado de seguridad necesario en función del nivel de riesgo estimado. La arquitectura propuesta ha de soportar los esquemas y especificaciones ya utilizados por los participantes del sistema para efectuar las transacciones de pago.



ITU-T Y.2741(11)\_F01

**Figura 1 – Participantes y arquitectura del sistema de comercio móvil y de banca móvil**

**Cuadro 1 – Participantes en el sistema de pago móvil**

Participante	Descripción, fin (meta, objetivo, interés)	Función
Cliente	<p>Persona física o moral que ha concluido un acuerdo contractual para la utilización de servicios de telecomunicaciones y del sistema de comercio móvil.</p> <p>Posee un dispositivo móvil y un instrumento de pago.</p> <p>Principal fin: incrementar el número de servicios, tener la posibilidad de realizar transacciones financieras a distancia seguras, ampliar el alcance de los instrumentos de pago.</p>	Cliente
Operador NGN	<p>Institución que ofrece al cliente servicios de comunicaciones digitales.</p> <p>Principal fin: incrementar el número de clientes, ampliar la gama de servicios disponibles; aumentar el tráfico.</p>	Operador NGN
Operador MPS	<p>Institución que garantiza la interacción segura de las estructuras financieras, el cliente y el operador NGN dentro del sistema de pagos móviles.</p> <p>Principal fin: crear una amplia red de comercio móvil; incrementar el número de participantes y de transacciones a distancia; garantizar la máxima seguridad de las operaciones.</p>	Proveedor de seguridad; proveedor de servicio; proveedor de autenticación de cliente
Emisor	<p>Institución financiera y jurídica que emite y facilita instrumentos de pago.</p> <p>Principal fin: incrementar el número de instrumentos de pago emitidos, incrementar el número de clientes.</p>	Emisor

**Cuadro 1 – Participantes en el sistema de pago móvil**

<b>Participante</b>	<b>Descripción, fin (meta, objetivo, interés)</b>	<b>Función</b>
Aval	Institución financiera y jurídica que acepta pagos a cambio de productos o servicios en nombre de un comerciante. Principal fin: incrementar el número de transacciones de los comerciantes a que sirve.	Aval
Comerciante	Empresa que ofrece bienes o servicios y recibe pagos del cliente. Principal fin: promover sus bienes y servicios, incrementar el número de clientes, aumentar las posibles maneras de pago de los bienes y servicios.	Comerciante

Los participantes pueden combinar las funciones, en función de la arquitectura utilizada.

A fin de alcanzar el nivel de seguridad requerido que se describe en [UIT-T Y.2740] es posible que se hayan de añadir las funciones de aplicación de cliente, distribuidor de aplicaciones de cliente o ambas. La aplicación de cliente se telecarga en su dispositivo móvil. El distribuidor puede ser el operador NGN, un operador de pago móvil o un tercero.

Cuando se utilizan tarjetas de sistemas de pago internacionales como instrumentos de pago, la función del sistema de pago es íntegra.

## **6.4 Ejemplos de utilización del sistema de pagos móviles**

### **6.4.1 Ejemplos de utilización básica**

#### **6.4.1.1 Ingreso del cliente en el MPS**

*Fin:* Abonar al cliente al servicio del MSP.

#### *Funciones básicas: metas y objetivos*

Cliente: tener la oportunidad de utilizar los servicios MPS.

Operador MPS: ingresar un nuevo cliente en el MPS.

#### *Garantías máximas*

Se registra el consentimiento del cliente a los términos y condiciones de utilización del MPS.

El cliente queda registrado en el sistema informático del operador MPS.

El cliente recibe un código de activación.

#### *Garantías mínimas*

Se deniega al cliente el ingreso indicándosele la causa.

El operador MPS guarda registro de la cancelación del ingreso del cliente.

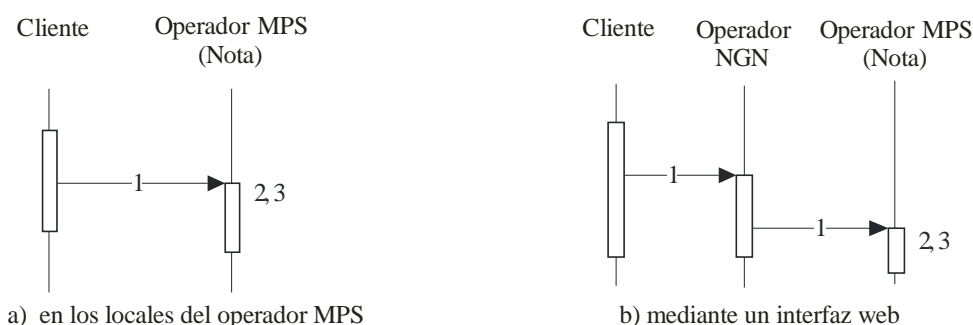
#### *Datos iniciales*

No hay un perfil activo del cliente en el MPS: el cliente no ha ingresado en el MPS o su perfil fue eliminado anteriormente.

#### *Fases básicas*

- 1) El cliente inicia el ingreso:
  - a) en los locales del operador MPS;
  - b) mediante una interfaz web: se autoriza al cliente en el sitio web del operador y se envía la solicitud de ingreso

- 2) El MPS autentifica al cliente.
- 3) El IS del operador MPS crea el perfil de datos del cliente en la base de datos.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F02

**Figura 2 – Ingreso del cliente en el MPS**

### *Fases alternativas*

#### **3. a. El cliente ya ha ingresado en el MPS (posee un perfil activo):**

El IS del operador MPS informa al cliente de que ya había ingresado en el servicio.

#### **3. b. El cliente tiene una cuenta en el MPS, pero está bloqueada:**

El IS del operador MPS activa la cuenta del cliente.

#### **3. c. El IS del operador MSP deniega el registro:**

- a) El IS del operador del MPS registra un intento de conexión al servicio por parte del cliente.
- b) El IS del operador MPS informa al cliente de la denegación de conexión al servicio y especifica los motivos.

### **6.4.1.2 Ingreso del instrumento de pago que se utilizará en el MPS**

El cliente ha de registrar su instrumento de pago. A lo largo del proceso se cumplirán las siguientes condiciones:

- el cliente deberá confirmar la autoridad de utilización del instrumento de pago que registra;
- en el proceso de registro del instrumento de pago, en la base de datos del operador MPS habrá de figurar un número mínimo de parámetros necesarios para que el cliente realice una transacción de pago a distancia;
- los parámetros del instrumento de pago estarán almacenados en el lado del operador MPS con un grado de seguridad tal que se excluya el acceso no autorizado y resulte imposible realizar transacciones financieras no autorizadas por el cliente.

En el Apéndice I se describe el medio de conexión a un instrumento de pago.

### **6.4.1.3 Realización de operaciones financieras por parte del cliente en su zona de residencia con su propio sistema de pago**

**Fin:** ofrecer al cliente la posibilidad de utilizar los servicios financieros del MPS.

#### **Funciones básicas: metas y objetivos**

Cliente: utilizar los servicios que ofrece a distancia el comerciante.

Operador móvil: transmitir el mensaje por los canales de comunicación.

Operador MPS: permitir al cliente realizar pagos a cambio de bienes y servicios utilizando el MPS.

Comerciante: ofrecer a distancia servicios al cliente.

Emisor: autorizar la operación de pago del cliente e iniciarla.

Aval: transferir la autorización de la operación al comerciante.

### **Garantías máximas**

El cliente paga por el servicio del comerciante.

El comerciante ofrece el servicio.

### **Garantías mínimas**

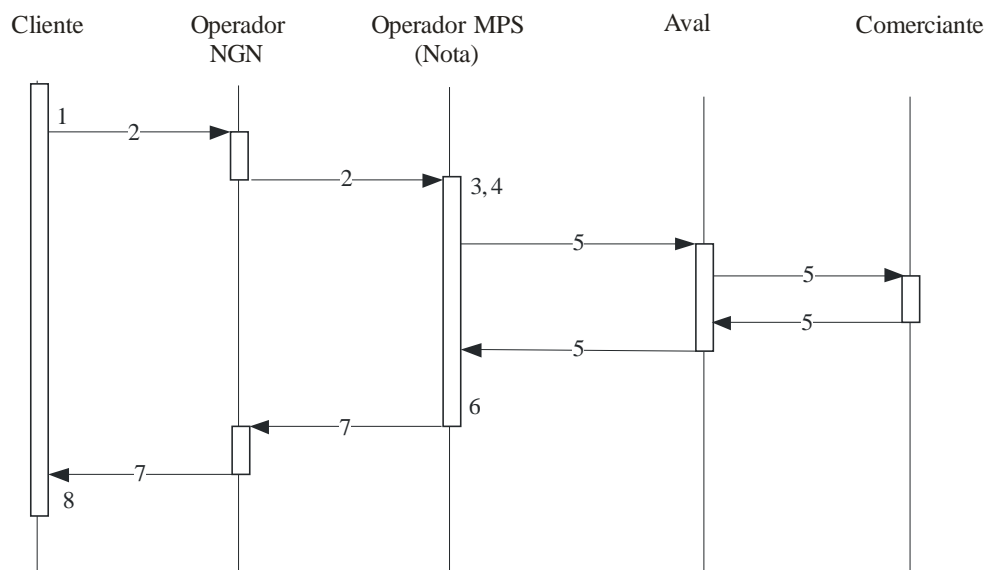
Se impide al cliente que pague por los bienes y servicios del operador MPS.

### **Datos iniciales**

El cliente se registra en el MPS e ingresa en el sistema su instrumento de pago.

### **Fases básicas**

- 1) Utilizando su dispositivo móvil, el cliente genera una petición que contiene los parámetros de la operación financiera y del instrumento de pago.
- 2) La petición se transmite a través de los canales del operador NGN.
- 3) El operador MPS recibe la petición.
- 4) El cliente queda autenticado.
- 5) Se realiza la operación financiera (ingreso/pago) solicitada utilizando los detalles del instrumento de pago del cliente.
- 6) Se envía al cliente el resultado de la operación.
- 7) La respuesta se transmite por los canales del operador NGN.
- 8) El cliente recibe el resultado de la operación financiera.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F03

**Figura 3 – Realización de operaciones financieras por parte del cliente**

### Fases alternativas

6. *No se autentifica al cliente*

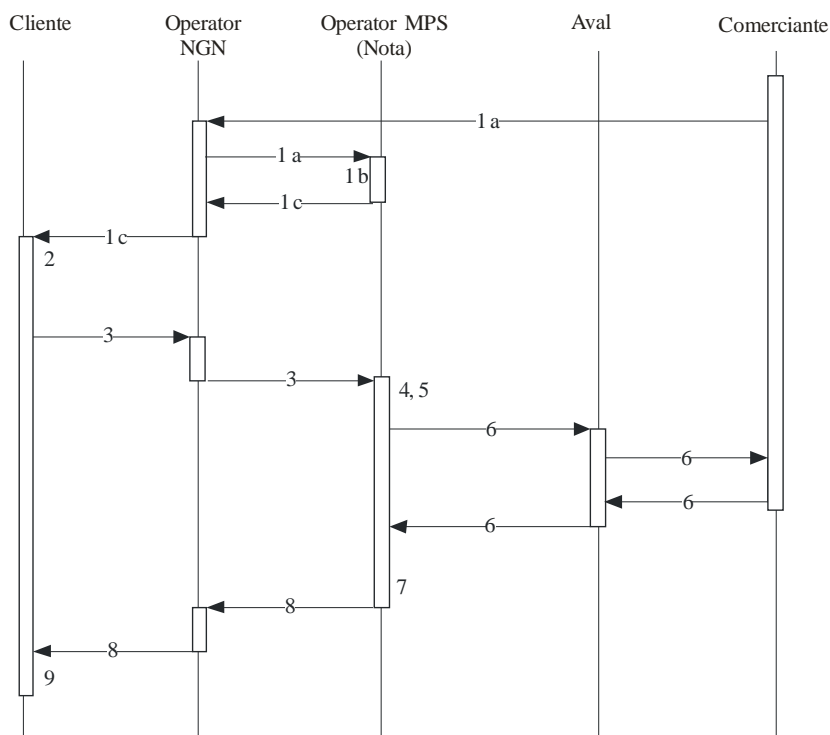
7. *No es posible realizar la operación financiera:*

- a) Se anula la transacción.
- b) Se devuelve al cliente el resultado del procesamiento de la operación.

### Caso alternativo: el comerciante inicia el pago

#### Fases básicas

- 1)
  - a) El comerciante genera una oferta de pago y la envía al operador MPS;
  - b) el operador MPS determina al cliente y la manera de entregar la oferta de pago al cliente;
  - c) se envía al cliente la petición a través de los canales del operador NGN.
- 2) El cliente recibe la petición en su dispositivo móvil y genera la respuesta que contiene los parámetros de la operación financiera y del instrumento de pago.
- 3) La petición se transmite por los canales del operador NGN.
- 4) El operador MPS recibe la respuesta del cliente.
- 5) Se autentifica al cliente.
- 6) Se realiza la operación financiera (ingreso/pago) solicitada utilizando los detalles del instrumento de pago del cliente.
- 7) Se envía al cliente el resultado de la operación.
- 8) La respuesta se transmite por los canales del operador NGN.
- 9) El cliente recibe el resultado de la operación financiera.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F04

**Figura 4 – Realización de pagos iniciados por el comerciante**

#### 6.4.1.4 Desconexión del instrumento de pago del MPS

**Fin:** permitir al cliente eliminar datos relativos al instrumento de pago del MPS.

**Funciones básicas: metas y objetivos**

Cliente: desconectar el instrumento de pago del MPS.

Operador móvil: transmitir el mensaje a través de los canales de comunicación.

Operador MPS: permitir al cliente desconectar el instrumento de pago.

**Garantías máximas**

El cliente desconecta el instrumento de pago del MPS.

**Garantías mínimas**

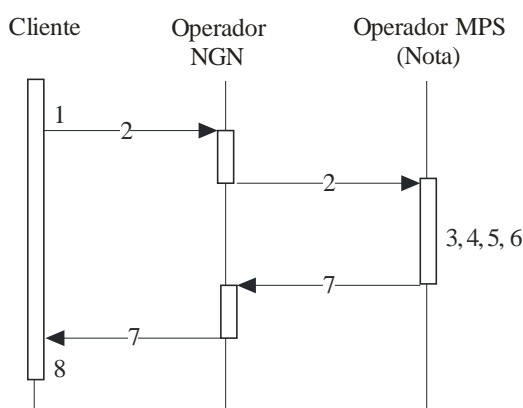
El cliente no puede desconectar el instrumento de pago.

**Datos iniciales**

El cliente ingresa en el MPS y tiene un instrumento de pago conectado.

**Fases básicas**

- 1) Utilizando su dispositivo móvil, el cliente genera la petición de desconexión de un determinado instrumento de pago.
- 2) La petición se transmite a través de los canales del operador NGN.
- 3) El operador MPS recibe la petición.
- 4) El MPS autentifica al cliente.
- 5) El instrumento de pago se elimina de la base de datos del IS.
- 6) El resultado de la desconexión del instrumento de pago se envía al cliente.
- 7) La respuesta se transmite a través de los canales del operador NGN.
- 8) El cliente recibe el resultado de la operación.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F05

**Figura 5 – Desconexión del instrumento de pago del MPS**

### Fases alternativas

#### 7. Se deniega la desconexión del instrumento de pago del MPS

- a) el IS del operador MPS informa al cliente de la imposibilidad de desconectar el instrumento de pago.

#### 6.4.1.5 Desconexión del cliente del MPS

**Fin:** desconectar al cliente de los servicios MPS.

#### Funciones básicas: metas y objetivos

Cliente: abandonar los servicios MPS.

Operador MPS: hacer que los servicios sean inaccesibles para el cliente.

#### Garantías máximas

Se registra la cancelación del cliente de los servicios MPS.

Los servicios MPS son inaccesibles para el cliente.

#### Garantías mínimas

Se deniega al cliente la desconexión de los servicios; se especifica el motivo.

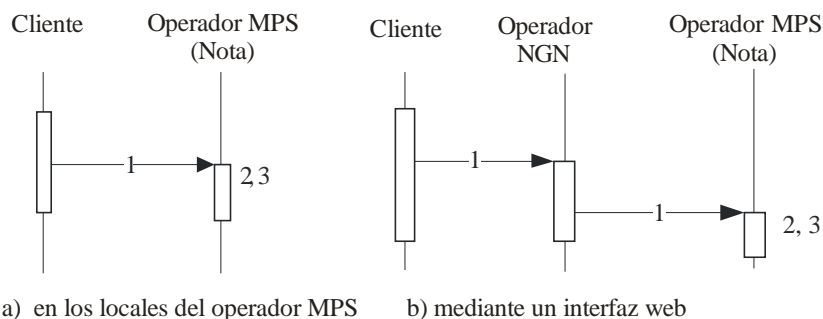
El cliente cancela la desconexión de los servicios MPS.

#### Datos iniciales

El cliente ha ingresado en el MPS.

#### Fases básicas

- 1) El cliente inicia la desconexión de los servicios:
  - en los locales del operador MPS;
  - mediante la interfaz web: el cliente queda autorizado por el sitio web del operador MPS y solicita la desconexión del servicio.
- 2) Se autentifica al cliente en el MPS.
- 3) El IS del operador MPS introduce los cambios relativos al estado del cliente en la base de datos (se bloquea el perfil).
- 4) El cliente no puede utilizar los servicios MPS sin volver a ingresar en el sistema.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F06

**Figura 6 – Desconexión del cliente del MPS**



## Fases alternativas

### 1. *Se utiliza en el MPS una aplicación de pago*

- El cliente inicia la desconexión del MPS en la aplicación.

### 3. *El cliente no puede desconectarse de los servicios MPS*

- El IS del operador MPS informa al cliente de que no se puede desconectar el servicio en ese momento.

## 6.4.2 Utilización con una aplicación de pago

### 6.4.2.1 Recepción de la aplicación de pago

**Fin:** ofrecer al cliente la posibilidad de utilizar la aplicación en el MPS.

#### **Funciones básicas: metas y objetivos**

Cliente: recibir la aplicación de pago que se utilizará en el dispositivo móvil.

Distribuidor de aplicaciones de cliente: ofrecer la aplicación al cliente.

#### **Garantías máximas**

El cliente recibe la aplicación.

#### **Garantías mínimas**

Se deniega la aplicación al cliente.

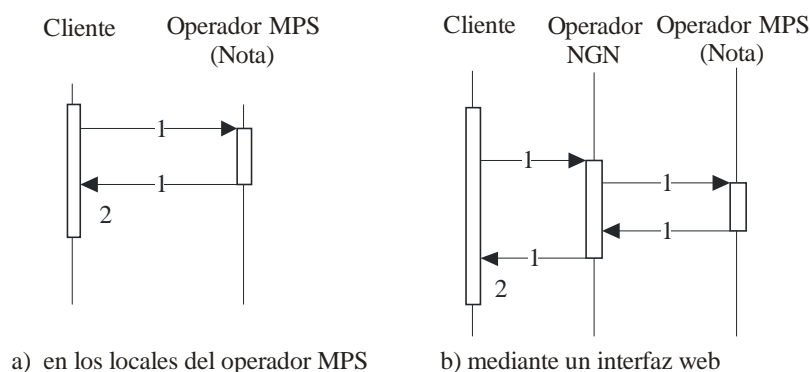
El cliente no puede utilizar la aplicación recibida a causa de determinadas características técnicas del dispositivo móvil.

#### **Datos iniciales**

El cliente ingresa en el MPS y posee la capacidad técnica de utilizar la aplicación.

#### **Fases básicas**

- 1) El cliente recibe la aplicación del distribuidor de aplicaciones de cliente:
  - en los locales del distribuidor de aplicaciones de cliente;
  - mediante la interfaz web (en el sitio web del distribuidor de aplicaciones de cliente).
- 2) El cliente puede utilizar la aplicación en el dispositivo móvil.



NOTA – Distribuidor de aplicaciones de cliente.

ITU-T Y.2741(11)\_F07

**Figura 7 – Recepción de la aplicación de pago**

### ***Fases alternativas***

#### ***1. a. El cliente recibe la versión actualizada de la aplicación***

El cliente ya ha recibido la aplicación antes.

#### ***1. b. El cliente no recibe la aplicación***

El cliente pide ayuda al servicio técnico del distribuidor de aplicaciones de cliente.

### **6.4.2.2 Activación de la aplicación de pago**

***Fin:*** activar la aplicación de pago del cliente.

#### ***Funciones básicas: metas y objetivos***

Cliente: poder utilizar los servicios MPS mediante la aplicación.

Operador MPS: validar la utilización de una determinada aplicación de pago en el MPS por parte de un determinado cliente.

Operador móvil: transmitir el mensaje a través de los canales de comunicación.

#### ***Garantías máximas***

El cliente activa la aplicación.

Se cargan las claves del cliente en la aplicación.

Se introducen las claves del cliente en la base de datos del IS del operador MPS.

#### ***Garantías mínimas***

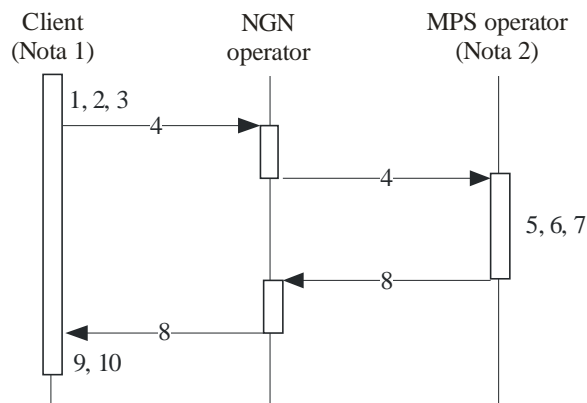
Se deniega al cliente la activación de la aplicación; se especifica la causa de la denegación.

#### ***Datos iniciales***

El cliente ha ingresado en el MPS, dispone del código de activación y de la aplicación en el dispositivo móvil.

#### ***Fases básicas***

- 1) El cliente selecciona "Activación" en el menú de la aplicación.
- 2) El cliente presenta el código de activación, recibido durante el procedimiento de ingreso, a la aplicación.
- 3) La aplicación genera y envía una petición al MPS.
- 4) La petición se transmite a través de los canales del operador NGN.
- 5) El operador MPS recibe la petición. Se verifica el código de activación.
- 6) Se generan las claves del cliente y se almacenan en la base de datos del IS del proveedor MPS.
- 7) Se envían al cliente las claves y el resultado de la activación.
- 8) La respuesta se transmite a través de los canales del operador NGN.
- 9) La aplicación de cliente recibe el mensaje, almacena las claves de cliente y se muestra al cliente el resultado de la activación.
- 10) El cliente recibe acceso a los servicios MPS en la aplicación.



NOTA 1 – Cliente, instrumento de pago, aplicación de pago.

NOTA 2 – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_F08

**Figura 8 – Activación de la aplicación de pago**

### *Fases alternativas*

#### **5. Error en la activación del código de validación:**

- a) El IS del operador MPS informa al cliente de que ha introducido un código de activación incorrecto.
- b) Se bloquea la cuenta del cliente si se excede el límite de intentos de introducción del código de activación.

### **6.4.3 Posibles interacciones entre sistemas**

En esta Recomendación se tratan cuestiones de orden general y se presentan ejemplos básicos de interacción.

#### **6.4.3.1 Realización de transacciones financieras cuando el cliente está en itinerancia**

**Fin:** hacer que el cliente pueda utilizar el servicio MPS habilitado cuando se encuentre fuera de la zona de cobertura de su operador (zona de residencia).

#### **Funciones básicas: metas y objetivos**

Cliente: tener la posibilidad de pagar a cambio de servicios utilizando el MPS cuando esté fuera de su zona de residencia.

Operador móvil: transmitir el mensaje a través de los canales de comunicación.

Operador MPS: permitir al cliente pagar a cambio de bienes y servicios utilizando el MPS.

Comerciante: prestar servicios a distancia al cliente.

Emisor: autorizar e iniciar la operación de pago del cliente.

Aval: transferir la autorización de la operación al comerciante.

#### **Garantías máximas**

El cliente paga por el servicio que le presta el comerciante.

El comerciante presta el servicio.

### ***Garantías mínimas***

Se deniega al cliente la posibilidad de pagar por los bienes y servicios del operador MPS.

### ***Datos iniciales***

El cliente ha ingresado en el MPS. El cliente está en una zona de itinerancia (fuera de la zona de residencia) y dispone de un instrumento de pago conectado.

### ***Fases básicas***

Las fases básicas son semejantes a las descritas para la transacción financiera dentro de la zona de residencia. La transmisión de la petición del cliente y el resultado de la transacción entre la zona de itinerancia y la zona de residencia se realiza siguiendo las normas de la itinerancia, que no entran en el alcance de la presente Recomendación.

#### **6.4.3.2 Realización de operaciones financieras por parte del cliente en otro MPS**

**Fin:** permitir al cliente utilizar los servicios de un MPS diferente en el que no ha ingresado.

#### ***Funciones básicas: metas y objetivo:***

Cliente: obtener la posibilidad de pagar los servicios prestados por un comerciante ubicado en la zona de cobertura de un MPS diferente.

Operador móvil: transmitir el mensaje a través de los canales de comunicación.

Operador MPS: permitir al cliente pagar a cambio de bienes y servicios utilizando otro MPS.

Comerciante: prestar servicios a distancia al cliente.

Emisor: autorizar e iniciar la operación de pago del cliente.

Aval: transferir la autorización de la operación al comerciante.

### ***Garantías máximas***

El cliente paga por los servicios del comerciante.

El comerciante presta el servicio.

### ***Garantías mínimas***

Se deniega al cliente la posibilidad de pagar a cambio de los bienes y servicios del operador MPS.

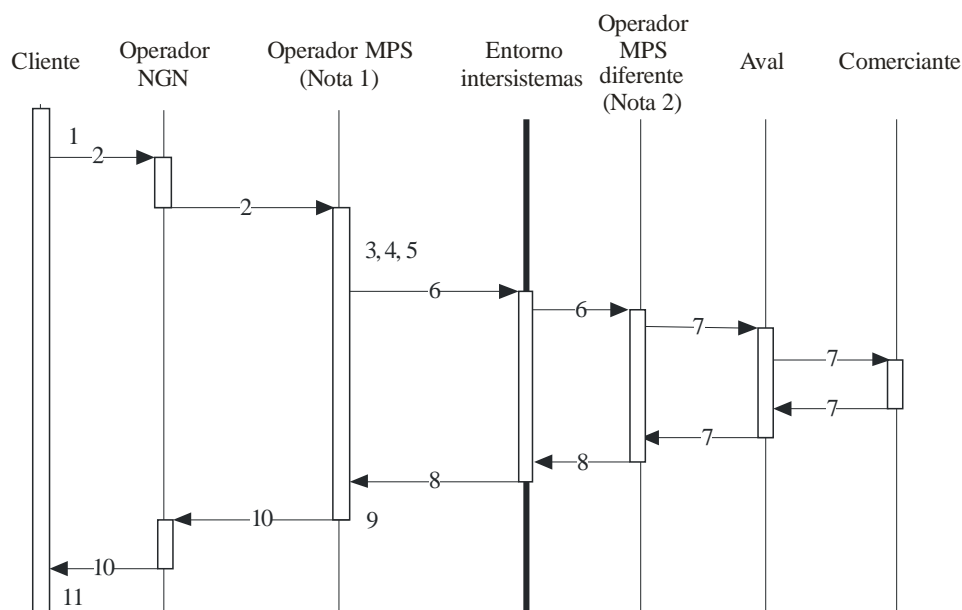
### ***Datos iniciales***

El cliente ha ingresado en el MPS, dispone de un instrumento de pago conectado y conoce los detalles del comerciante necesarios para efectuar la transacción de pago.

### ***Fases básicas***

- 1) El cliente genera una petición a través de su teléfono móvil. Esta petición contiene los parámetros de la transacción financiera (ID de pago) y los parámetros del instrumento de pago.
- 2) Se transmite la petición a través de los canales de comunicación del operador.
- 3) El operador MPS recibe la petición.
- 4) Se autentifica al cliente.
- 5) El operador MPS queda identificado por el ID de pago.
- 6) Se transmite la petición al destinatario (el operador de un MPS diferente) a través de los canales seguros entre sistemas.
- 7) Se realiza la transacción financiera solicitada utilizando los detalles del instrumento de pago del cliente.

- 8) Se envía al MPS propio del cliente el resultado de la transacción.
- 9) El MPS genera una respuesta para el cliente.
- 10) Se transmite la respuesta a través de los canales de comunicación del operador.
- 11) El cliente recibe el resultado de la transacción.



NOTA 1 – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

NOTA 2 – Proveedor de seguridad, proveedor de servicio.

ITU-T Y.2741(11)\_F09

**Figura 9 – Realización de operaciones financieras por parte del cliente en otro MPS**

### *Fases alternativas*

4. *No se autentifica al cliente.*
5. *No se puede identificar al MPS.*
7. *No se puede realizar la operación financiera:*
  - a) Se ejecuta la anulación de la transacción;
  - b) Se devuelve al cliente el resultado de la operación.

## **7 Transición desde los sistemas de pago por testigo**

Algunos operadores han introducido servicios que permiten la transferencia de testigos monetarios y no monetarios en calidad de pago a cambio de bienes y servicios dentro de los sistemas de facturación de los operadores NGN (y, en ocasiones, entre ellos).

Aunque estos servicios suelen considerarse convenientes para el desarrollo de las economías inmaduras, donde gran parte de la población carece de identidad bancaria, a la larga, estos servicios pueden influir negativamente en los sistemas fiscal y monetario de esas economías.

Los países en desarrollo tienen muchos problemas de delincuencia relacionada con el dinero en efectivo. El desarrollo de sistemas de banca electrónica en esos países reduce la cantidad de efectivo en circulación, reduciéndose a su vez ese tipo de delincuencia.

Por consiguiente, los operadores NGN que ofrecen servicios de pago por testigo han de elaborar planes de transición desde esos sistemas a los que utilizan las transacciones financieras para el intercambio de valor.

## Apéndice I

### Ingreso de un instrumento de pago en el sistema

(Este apéndice no forma parte integrante de la presente Recomendación.)

**Fin:** ofrecer al cliente la posibilidad de utilizar su instrumento de pago en el MPS.

#### **Funciones básicas: metas y objetivos**

Cliente: tener la oportunidad de utilizar el MPS con un instrumento de pago;

Operador móvil: transmitir el mensaje a través de los canales de comunicación;

Operador MPS: aprovechar la utilización de una aplicación de pago dada en el MPS por parte de un cliente dado;

Proveedor de autenticación de cliente: autenticar al cliente y su instrumento de pago.

#### **Garantías máximas**

El cliente recibe la oportunidad de utilizar el MPS para utilizar el instrumento de pago.

#### **Garantías mínimas**

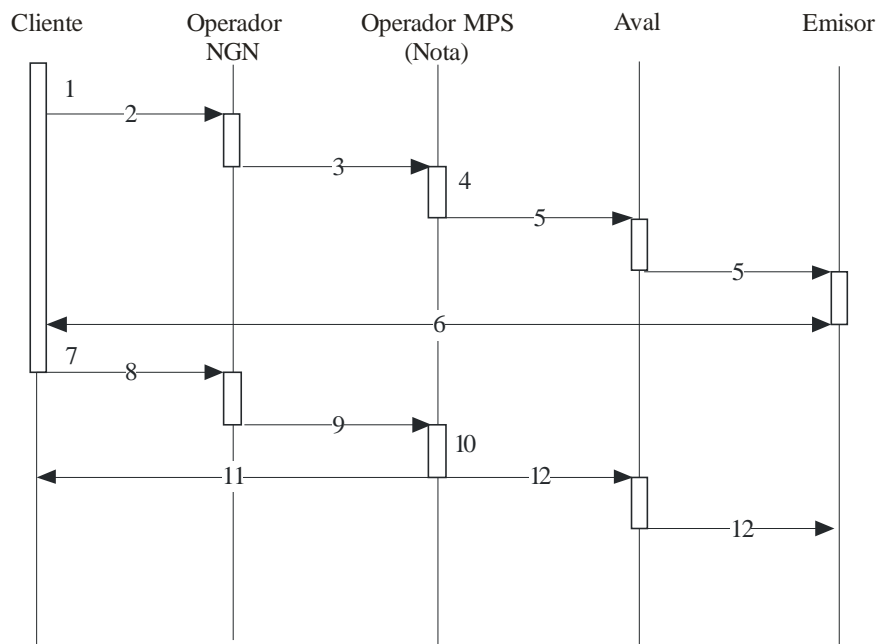
Se deniega al cliente la posibilidad de utilizar el instrumento de pago en cuestión.

#### **Datos iniciales**

El cliente ha ingresado en el MPS y dispone de un instrumento de pago

#### **Fases básicas**

- 1) Utilizando su dispositivo móvil, el cliente transmite los parámetros del instrumento de pago al operador MPS.
- 2) Se transmite la petición a través de los canales del operador MPS.
- 3) El operador MPS recibe la petición.
- 4) El IS del operador MPS genera una cuantía aleatoria.
- 5) El operador MPS envía al sistema del aval una petición para reservar esta cuantía en el instrumento de pago en cuestión. El aval envía una petición de autorización al emisor del instrumento de pago. El cliente contactará al emisor y conocerá la cuantía a fin de confirmar que es el propietario legítimo del instrumento de pago.
- 6) El emisor del instrumento de pago autentifica al cliente utilizando sus medios habituales de autenticación.
- 7) Tras la autenticación, el emisor informa al cliente del valor de la cuantía reservada.
- 8) El cliente transmite el valor al operador MPS a través de la aplicación de cliente.
- 9) Se transmite la petición a través de los canales del operador MPS.
- 10) Una vez recibido el valor de la cuantía reservada al cliente, el operador MPS la compara con la cuantía previamente generada.
- 11) Si ambas cuantías coinciden, el operador MPS almacena de manera segura la información del instrumento de pago para su posterior utilización y notifica el resultado de la operación al cliente.
- 12) Al mismo tiempo, se envía al emisor (a través del aval) una petición para cancelar la reserva del instrumento de pago.



NOTA – Proveedor de seguridad, proveedor de autenticación de cliente, proveedor de servicio.

ITU-T Y.2741(11)\_FI.1

**Figura I.1 – Ingreso de un instrumento de pago en el MPS**

**Fases alternativas**

**10. El valor de la cuantía previamente reservada no coincide con la introducida por el cliente**

El cliente recibe una notificación de error. Cuando el número de intentos fallidos es superior a tres, el sistema MPS bloquea el perfil del cliente móvil. Se cancela la reserva.

## Apéndice II

### Modelos de aplicación del sistema de banca móvil y de comercio móvil

(Este apéndice no forma parte integrante de la presente Recomendación)

En este apéndice se describen ejemplos de aplicación de sistemas de banda móvil y de comercio móvil básicos, que podrán variar en función del nivel de seguridad aplicado.

En este apéndice se utilizan los siguientes términos:

**Canal de transmisión de mensaje:** es un medio de transmitir la petición formulada por el cliente para realizar una operación financiera (transferencia de dinero), que requiere un acceso a distancia a los instrumentos de pago. Ejemplos de canales de transmisión de mensaje son los mensajes SMS, las peticiones USSD, comunicación de lotes (GPRS, EDGE, datos 3G, HSDPA etc.)

**Instrumento de pago:** es un conjunto de medidas jurídicas para efectuar un traspaso, monetario o no monetario, a fin de efectuar un pago. Ejemplos de instrumentos de pago son las cuentas bancarias, las cuentas de operador y las tarjetas bancarias.

**Operaciones disponibles:** es una lista de las operaciones disponibles en el sistema de un determinado nivel de seguridad.

**Restricciones:** son las limitaciones para utilizar el sistema que prevé el modelo de riesgo aceptado y están prescritas o reservadas con valor jurídico en los contratos.

**Teléfono predefinido:** es un número de teléfono previamente indicado por el cliente en un formato propio del proveedor de servicios.

**Teléfono ad hoc:** es un número de teléfono indicado directamente por el cliente a la hora de efectuar un pago.

**Cuenta predefinida:** es un número de cuenta previamente indicado por el cliente en un formato propio del proveedor de servicios.

**Cuenta ad hoc:** es un número de cuenta indicado directamente por el cliente a la hora de efectuar un pago.

**Pago predefinido:** es un pago efectuado de acuerdo con unos parámetros previamente facilitados, donde se puede seleccionar al receptor a partir de una lista definida por el proveedor de servicio MPS (por ejemplo, pago efectuado por una persona física a una persona moral a cambio de los servicios prestados).

**Pago ad hoc:** es un pago efectuado por el cliente a cambio de servicio no incluidos en la lista definida por el proveedor de servicio MPS, a condición de que técnicamente sea viable realizar el pago. Condición previa: es obligatorio que el proveedor de servicio tenga un canal de interfuncionamiento con el proveedor MPS o que el servicio sea prestado por otro proveedor MPS y el interfuncionamiento se lleva a cabo entre ambos proveedores.

**Pago automático:** es un pago periódico y automático iniciado por el proveedor de servicio MPS con el consentimiento previo del cliente.

**Pago automático con confirmación:** es un pago periódico y automático iniciado por el proveedor de servicio MPS con el consentimiento del cliente.

**Pago iniciado por el comerciante:** es un pago cuyos parámetros están definidos e introducidos por el comerciante. El cliente puede confirmar o rechazar el procesamiento del pago ofrecido.

**Servicio de información:** es una gama de servicios de información prestados por el proveedor de servicio MPS que no están asociados con la realización de operaciones financieras (por ejemplo, comunicación del balance de un instrumento de pago, comunicación de información de referencia).



## **Modelos de aplicación de sistemas de banca móvil y de comercio móvil**

A continuación se exponen algunos modelos de sistemas de banca móvil y de comercio móvil, que podrán variar en función del nivel de seguridad escogido. Cada modelo impone determinados requisitos en cuanto al instrumento de pago, las operaciones disponibles, las restricciones y la aplicación que utiliza el sistema.

### **II.1 Sistema sin aplicación de cliente**

Corresponde al Nivel 1 y el Nivel 2 del sistema de seguridad (véase [UIT-T Y.2740]).

**Canal de transmisión de mensaje:** mensajes SMS de texto simple, peticiones USSD.

**Instrumento de pago:** pagos a partir de cuentas bancarias y cuentas de operador predefinidas en el acuerdo de servicio.

**Operaciones disponibles:** sólo se efectúan pagos a receptores previamente definidos en el contrato. Al firmar el contrato se ha de especificar la lista de operaciones posibles:

- Pago para un teléfono predefinido
- Pago a una cuenta predefinida
- Realización de un pago predefinido
- Realización de pagos automáticos
- Realización de pagos automáticos con confirmación
- Servicios de información.

**Restricciones:** límites máximos de pago, que pueden incluir límites de cuantía por transacción, límites de transacción por 24 horas, restricción de las transacciones financieras disponibles, lo que implica la realización de pagos únicamente en concepto de servicios previamente acordado.

### **II.2 Sistema con aplicación de cliente**

Corresponde al Nivel 3 y el Nivel 4 del sistema de seguridad (véase [UIT-T Y.2740]).

**Canal de transmisión de mensaje:** mensajes SMS, comunicación de lotes (GPRS, EDGE, datos 3G, HSDPA, etc.). El canal de transmisión de mensaje y el mensaje transmitido han de encriptarse con un sistema criptográfico fuerte.

**Instrumento de pago:** pagos a partir de cuentas bancarias y de operador predefinidas en el acuerdo de servicio; pagos mediante tarjetas bancarias y tarjetas de sistemas de pago internacionales (los pagos incluyen la transmisión de datos muy importantes a través de los canales de comunicación)

**Operaciones disponibles:** conexión al sistema a distancia posible; amplia gama de pagos para diversos servicios conectados al sistema; posibilidad de incrementar considerablemente el número de operaciones realizadas en el MPS (introducción de nuevos pagos y servicios; conexión con nuevos comerciantes); el proveedor de servicio y el cliente pueden definir con flexibilidad la lista de pagos disponibles; distintos MPS pueden interfuncionar en la prestación de servicios. Es posible realizar las siguientes operaciones:

- Pago por un teléfono predefinido
- Pago a una cuenta predefinida
- Realización de pagos predefinidos
- Realización de pagos automáticos
- Realización de pagos automáticos con confirmación
- Servicios de información
- Pago por un teléfono ad hoc

- Pago a una cuenta ad hoc
- Pago ad hoc
- Pago iniciado por el comerciante.

**Restricciones:** las restricciones impuestas a los pagos están determinadas en los contratos establecidos entre los participantes en el sistema.

**Aplicación:** es obligatorio utilizar la aplicación para obtener la seguridad necesaria (encriptación de mensajes) y utilizar convenientemente el sistema.

## **Bibliografía**

[b-UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación*.





## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
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, comunicaciones de sistemas abiertos y seguridad
<b>Serie Y</b>	<b>Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación</b>
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación