Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2740

(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.2740

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.2740

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

Resumen

Durante los últimos años han aparecido numerosos sistemas de pago a distancia por redes móviles. Son todos diferentes, pero a menudo carecen de seguridad. Por otra parte, las redes de comunicaciones, incluidas las móviles, están cambiando considerablemente debido a la transición hacia las redes de la próxima generación (NGN).

En la Recomendación UIT-T Y.2740 se pormenorizan planteamientos para el desarrollo de la seguridad sistémica del comercio móvil y la banca móvil en las redes de la próxima generación (NGN). Se describen requisitos de seguridad para los sistemas de comercio móvil y banca móvil para los cuatro niveles de seguridad especificados. Se indican sumariamente los riesgos de seguridad probables para los sistemas de comercio móvil y banca móvil, y se especifican los medios de reducir estos riesgos.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T Y.2740	2011-01-28	13

Palabras clave

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

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 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/.

ÍNDICE

Recomendación UIT-T Y.2740

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

1 Alcance

En esta Recomendación se describen riesgos de seguridad asociados a las transacciones financieras móviles a distancia soportadas por los servicios de aplicación de las redes de la próxima generación (NGN) y las medidas de supresión y mitigación del riesgo con cuatro niveles de seguridad. En la presente Recomendación se especifican asimismo los requisitos mínimos para la protección de la privacidad de los datos personales en el marco de las transacciones financieras móviles a distancia.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de Recomendación.

[UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.

[UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en las redes de la próxima generación*.

[UIT-T Y.2741] Recomendación UIT-T Y.2741 (2011), *Arquitectura de transacciones financieras móviles seguras en las redes de la próxima generación.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otras Recomendaciones:

3.1.1 control de acceso [UIT-T X.800]: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.1.2 aplicación [UIT-T Y.2741]: Aplicación especial de banca móvil o comercio móvil telecargada en el aparato móvil de un cliente (usuario).

3.1.3 autenticación [UIT-T X.800]: Véanse "autenticación de origen de los datos" y "autenticación de entidad par".

NOTA – En la presente Recomendación, el término "autenticación" no se utiliza en relación con la integridad de los datos; en su lugar se utiliza el término "integridad de los datos".

3.1.4 disponibilidad [UIT-T X.800]: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.1.5 cliente [UIT-T Y.2741]: Persona física o moral que ha concluido un acuerdo contractual para la utilización de servicios de telecomunicaciones y del sistema de comercio móvil.

3.1.6 confidencialidad [UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.7 integridad de los datos [UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.8 autenticación del origen de los datos [UIT-T X.800]: Confirmación de que la fuente de los datos recibidos es la alegada.

3.1.9 sistema de pago móvil [UIT-T Y.2741]: Sistemas de banca móvil y/o de comercio móvil.

3.1.10 red de 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.

3.1.11 privacidad [UIT-T X.800]: Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada.

NOTA – Como este término se relaciona con el derecho de las personas, no puede ser muy preciso y su uso debe evitarse, salvo como un motivo para exigir seguridad.

3.1.12 repudio [UIT-T X.800]: Negación de una de las entidades implicadas en una comunicación de haber participado en toda la comunicación o en parte de ella.

3.1.13 dimensión de seguridad [UIT-T X.805]: Conjunto de medidas de seguridad que responden a un determinado aspecto de la seguridad de red.

3.1.14 capa de seguridad [UIT-T X.805]: Jerarquía de equipos de red y agrupaciones de dispositivos.

3.1.15 planos de seguridad [UIT-T X.805]: Determinada actividad de red protegida por dimensiones de seguridad.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se utiliza el siguiente término:

3.2.1 nivel de seguridad: Especificación de seguridad del sistema que define la eficacia de la protección contra riesgos.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan los siguientes acrónimo y abreviaturas:

GSM Sistema Mundial de Comunicaciones Móviles (*Global System for Mobile Communications*)

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

MSISDN Número RDSI internacional de estación móvil (*mobile station international ISDN number*)

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

PA-DSS Norma de seguridad de datos para aplicaciones de pago (*payment application data security standard*)

PCI DSS Norma de seguridad de datos para el sector de las tarjetas de pago (*payment card industry data security standard*)

5 Convenciones

Ninguna.

6 Consideraciones de seguridad para los sistemas de banca móvil y comercio móvil en las redes de la próxima generación

La seguridad del sistema de pago móvil (MPS, *mobile payment system*) en la red de la próxima generación (NGN) se basa en la arquitectura MPS y la función de los participantes en el MPS especificada en [UIT-T Y.2741], *Arquitectura de transacciones financieras móviles seguras en las redes de la próxima generación*, así como en el análisis de riesgo de los participantes en el MPS descrito a continuación.

6.1 Principales riesgos de las transacciones financieras móviles a distancia

En este apartado no se consideran los factores que condicionan los nuevos riesgos industriales que, a nivel mundial, afrontan los participantes cuando implantan el MPS: riesgos del sistema, estratégicos, del país y soberanos, del mercado, del interés, de liquidez, jurídicos, de reputación, etc. En este apartado se consideran únicamente los riesgos que afectan a la información y que puedan aparecer justamente cuando se produzcan los pagos móviles a distancia y haya que adoptar decisiones en materia de seguridad a fin de minimizar los riesgos, a saber:

- el riesgo de pérdida de confidencialidad que entraña el acceso no autorizado a información confidencial;
- el riesgo de violación de la integridad de datos consistente en distorsionar la información cuando se transfieren o procesan los datos;
- el riesgo de falsificación de documentos electrónicos (riesgo para la autenticidad) consistente en la generación de documentos electrónicos por participantes no autorizados;
- el riesgo de repudio que entraña la negación de la autoría de un documento electrónico;
- el riesgo de destrucción de la información, ya sea voluntariamente o por negligencia;
- el riesgo transaccional que entraña la imposibilidad de terminar o completar una transacción (por ejemplo, debido a la mala calidad de la transmisión).

6.2 Objetivos de seguridad

Para mejorar la seguridad de los pagos móviles y reducir al mínimo los riesgos de los participantes, la solución adoptada debe conseguir los siguientes objetivos:

- reducir la posibilidad de interceptación de la información personal o financiera en el momento de la transacción;
- reducir la posibilidad de recuperar información personal o financiera de las bases de datos;
- reducir la posibilidad de sustituir o distorsionar la información de carácter personal o financiero en el momento de la transacción;
- reducir la posibilidad de que utilicen esta solución personas no autorizadas y personas que intenten suplantar una identidad mediante la implementación de una autenticación única;
- reducir la posibilidad de que en la solución se utilice información "robada";

- crear las condiciones necesarias para que sea imposible que el iniciador de una transacción o un participante en la misma, niegue sus acciones tras haberlas realizado;
- garantizar la conformidad con los derechos y deberes legales de todos los participantes en las interoperaciones;
- garantizar la compleción de las transacciones.

6.3 Niveles de seguridad y medios de soportarlos

En la presente Recomendación se describen cuatro niveles de seguridad del MPS basados en el análisis de riesgo de los participantes en el MPS.

El nivel de seguridad del sistema se define por el conjunto de implantaciones de la dimensión de seguridad (véase el cuadro 1). Por consiguiente, el cuarto nivel de seguridad (el más elevado) debe tener las implantaciones más fuertes de dimensiones de seguridad. No obstante, los requisitos de ciertas dimensiones de seguridad están unificados para todos los niveles de seguridad.

Las partes que utilizan el MPS deben conocer el nivel de seguridad del sistema y los riesgos del sistema.

El nivel de seguridad aceptable para cierto riesgo de cualquier componente del sistema viene determinado por la parte que asume dicho riesgo.

Las partes pueden, además, mitigar los riesgos de utilizar MPS mediante medidas operacionales que pueden consistir en limitar la frecuencia o el valor monetario de las transacciones, la disponibilidad del servicio a los usuarios más leales, etc.

El cliente se identifica ante el sistema mediante el identificador público de la red NGN (por ejemplo, el MSISDN para redes GSM).

6.3.1 Implantación de las dimensiones de seguridad para todos los niveles de seguridad

La seguridad del sistema se confía a cada uno de los participantes de éste y se consigue gracias a las facilidades físicas y administrativas de garantía de seguridad en la transferencia, procesamiento y almacenamiento de los datos. Los participantes del sistema velarán por la aplicación de las normas de garantía de seguridad de la información del sector (por ejemplo, [b-PCI DSS] y [b-PA-DSS], etc.).

A continuación se indican ocho dimensiones de seguridad [UIT-T X.805] que definen los niveles de seguridad del MPS. Es obligatorio que todos los participantes del sistema implanten las dimensiones de seguridad correspondiente a la información implicada en el intercambio de datos.

1) Control de acceso: el acceso a cada componente del MPS debe concederse sólo conforme a lo estipulado por el personal del sistema o en función del nivel de acceso del usuario final. Este requisito es válido para todos los sistemas de seguridad.

2) Autenticación: la autenticidad de la identificación reclamada por las entidades que participan debe estar garantizada. Éste es uno de los factores clave para mitigar el riesgo de negación de autoría. Dada la amplitud de las posibilidades de implantación organizativa y técnica, cada nivel de seguridad define unos requisitos mínimos para el mecanismo de autenticación.

   Los tres factores de autenticación del cliente (usuario) son los siguientes:

   – el cliente utiliza cierta información que nadie más puede conocer, por ejemplo la contraseña de acceso (algo que sabe);
   – el cliente posee algo que sólo está a su alcance y que ejecuta ciertas acciones de modo exclusivo, por ejemplo generando una firma electrónica o un código de autenticación de mensaje (algo que tiene);
   – el cliente utiliza sus datos biométricos (algo que es).

3) No repudio: ofrece un medio de evitar que un individuo o entidad niegue haber ejecutado una acción concreta (por ejemplo el envío, transferencia o recepción de un mensaje). Para poder llevarlo a cabo, se registrarán, obligatoriamente, todas las acciones, tanto del personal como de los usuarios finales del sistema. Los registros históricos de eventos deben estar construidos a prueba de cambios y anotar todas las acciones de los usuarios. La conformidad con los requisitos se consigue por medios y mecanismos de autenticación aceptados en contratos mutuos públicos o privados. Este requisito es válido para todos los niveles de seguridad.

4) Confidencialidad de los datos: los datos utilizados en el sistema están protegidos frente a la revelación y alteración no autorizadas. Los requisitos de la confidencialidad vienen definidos por la criticidad de los datos del sistema. Cada nivel de seguridad especifica ciertos medios de garantizar la confidencialidad e impone restricciones sobre el nivel de criticidad de los datos del sistema.

5) Seguridad de la comunicación: la entrega garantizada de la secuencia de mensajes en ambas direcciones (con origen y destino en el destinatario) comprende la compleción de una transacción (utilizando los protocolos que garantizan la compleción de una transacción), y la protección de la información contra la revelación no autorizada en el momento de la transferencia por los canales de comunicación. Este requisito es válido para todos los niveles de seguridad.

6) Integridad de los datos: la corrección, precisión e integridad de los datos se consigue gracias a su protección contra la modificación, supresión, creación y reproducción no autorizadas, y gracias asimismo a la denuncia de actividades no autorizadas. La compleción lógica de una transacción está garantizada si se satisfacen ciertas condiciones, y esto se implementa a nivel de aplicación. Cada nivel de seguridad define ciertos mecanismos de garantía de la integridad. La garantía de la integridad puede conseguirse por medio de la confidencialidad de los datos y el control de acceso.

7) Disponibilidad: garantiza la conservación del acceso autorizado a los datos y servicios del MPS. Este requisito es válido para todos los niveles de seguridad y el proveedor de servicios debe cumplirlo lo mejor posible.

8) La privacidad garantiza la seguridad de la información implicada en el intercambio de datos y almacenada por los participantes del sistema. La solución debe utilizar el mínimo número de datos indispensable para que el sistema funcione. Los participantes del sistema deberán tomar medidas contra la adquisición o transferencia no autorizadas de datos. El sistema asegurará la conformidad con las normas del sector financiero.

Las dimensiones de seguridad implantadas en pie de igualdad en todos los niveles de seguridad son las siguientes:

– control de acceso;
– no repudio;
– seguridad de la comunicación;
– disponibilidad.

Las siguientes dimensiones de seguridad tienen una implantación peculiar en cada uno de los niveles de seguridad:

– autenticación;
– confidencialidad de los datos;
– integridad de los datos;
– privacidad.

6.3.2 Nivel de seguridad 1

El MPS puede confiar en la autenticación del cliente suministrada por el operador de la NGN.

La confidencialidad e integridad de los datos están garantizadas por el entorno de transferencia de datos (seguridad de las comunicaciones), y por el mecanismo de almacenamiento de datos y las facilidades del control de acceso del sistema durante su almacenamiento y procesamiento.

La privacidad viene garantizada por la ausencia de datos vulnerables en los mensajes que se transfieren, así como por la implementación de los mecanismos necesarios de almacenamiento de datos y de las facilidades de control de acceso del sistema. Los componentes del sistema no deben ofrecer posibilidades latentes de adquisición ni transferencia de datos sin autorización.

6.3.3 Nivel de seguridad 2

Cuando se utilizan los servicios del sistema, la autenticación puede ser monofactorial, por lo que puede implementarse sin tener que aplicar protocolos criptográficos.

Para la autenticación se utiliza una contraseña de uso único. Esta contraseña se genera por medio de varios dispositivos (testigo monofactorial de generación de contraseña de uso único, testigo monofactorial criptográfico, etc.).

La confidencialidad, integridad y privacidad de los datos se garantiza de un modo similar al del nivel 1.

6.3.4 Nivel de seguridad 3

Para el acceso a los servicios del sistema debe utilizarse la autenticación de cliente multifactorial.

El sistema deberá utilizar más de un factor de autenticación para autenticar el cliente.

La confidencialidad, integridad y privacidad de los datos en la transferencia de los mensajes debe venir garantizada además por la encriptación del mensaje y por la utilización de protocolos de transferencia de datos que garanticen la seguridad de que los datos son transferidos por los participantes en la interoperación (incluida la verificación de la integridad de los datos). Durante el almacenamiento y procesamiento de los datos, su confidencialidad, integridad y privacidad están garantizadas además por mecanismos de encriptación y enmascaramiento junto con una distribución de acceso bien definida, de conformidad con los privilegios y permisos.

Para cumplir los requisitos de seguridad en este nivel, el sistema utilizará aplicaciones informáticas especiales telecargadas en los aparatos móviles de los clientes. Estas aplicaciones implementarán autenticación dictatorial y realizarán la encriptación y desencriptación de los datos transferidos.

Cada autenticación exigirá la introducción de la contraseña u otros datos de activación de la clave de autenticación, borrándose la copia desencriptada de la clave de autenticación después de cada autenticación (testigo criptográfico multifactorial por software).

Todos los participantes en la interoperación MPS deberán utilizar facilidades de seguridad que garanticen la inmunidad del sistema. En las soluciones de nivel 3, la seguridad de los datos transferidos por los canales de comunicaciones deberá garantizarse por medio de criptografía fuerte. La fuerza de un método criptográfico depende de la clave criptográfica utilizada. El tamaño eficaz de la clave deberá satisfacer las recomendaciones de tamaño mínimo de la clave que garantice su fuerza relativa.

6.3.5 Nivel de seguridad 4

Éste es el nivel más alto de garantía de seguridad del sistema. Para satisfacer los requisitos de seguridad a este nivel, el sistema debe utilizar módulos de hardware instalados en los aparatos móviles de los clientes. Estos modelos de seguridad por hardware ejecutarán la autenticación bifactorial y garantizarán tanto la encriptación como la desencriptación de los datos transferidos. Cada autenticación requerirá la entrada de la contraseña u otros datos de activación de la clave de

autenticación, borrándose la copia desencriptada de la clave de autenticación después de cada autenticación (testigo criptográfico multifactorial por hardware). Algoritmos criptográfico simétricos y asimétricos se aplican a la encriptación del mensaje.

La implantación de otras dimensiones de seguridad corresponderá totalmente al nivel 3.

Cuadro 1 – Correlación entre los niveles de seguridad e implantación de dimensiones de seguridad

<table>
<tr><th rowspan="2">Dimensión de seguridad</th><th colspan="4">Nivel de seguridad</th></tr>
<tr><th>Nivel 1</th><th>Nivel 2</th><th>Nivel 3</th><th>Nivel 4</th></tr>
<tr><td>Control de acceso</td><td colspan="4">El acceso a cada componente del sistema sólo se otorgará a personal de sistema autorizado. La activación de aplicaciones especiales telecargadas a terminales móviles sólo debe permitirse a los clientes autorizados.</td></tr>
<tr><td>Autenticación</td><td>La autenticación en el sistema está garantizada por el entorno de transferencia de datos de la NGN.</td><td>Autenticación monofactorial para utilizar los servicios del sistema.</td><td>Autenticación multifactorial para utilizar los servicios del sistema.</td><td>Conexión presencial a los servicios utilizando datos personales con identificación obligatoria.
Autenticación multifactorial al utilizar los servicios del sistema.
Uso obligatorio de módulo criptográfico por hardware.</td></tr>
<tr><td>No repudio</td><td colspan="4">La imposibilidad de que un participante en una transacción o el iniciador de ésta niegue su acción una vez completada, viene garantizada por contratos legales explícitos e implícitos, por una declaración legal o por un contrato de reciprocidad y por mecanismos de autenticación aceptados. Los históricos de eventos estarán construidos a prueba de cambios y registrarán todas las acciones de los usuarios.</td></tr>
<tr><td>Confidencialidad de los datos</td><td colspan="2" rowspan="2">Durante las transferencias de datos, su confidencialidad está garantizada por el entorno de la transferencia (seguridad de las comunicaciones), y por el mecanismo de almacenamiento de los datos junto con los medios de control del acceso al sistema – en el almacenamiento de los datos y en su procesamiento.</td><td rowspan="3">Durante la transferencia de datos, la confidencialidad está garantizada por la encriptación adicional del mensaje y por los protocolos de transferencia de datos que garantizan la seguridad de los datos transferidos por los participantes en la interoperación (incluida la verificación de la integridad). Durante el almacenamiento y procesamiento de los datos, su confidencialidad, integridad y privacidad están garantizadas por mecanismos adicionales de encriptación y enmascaramiento, junto con una distribución de accesos bien definida con arreglo a privilegios y permisos.</td><td rowspan="3">Implementación de los requisitos del nivel 3 con la utilización obligatoria de facilidades criptográficas y de seguridad de datos realizadas mediante hardware en el lado del cliente (módulo criptográfico por hardware).</td></tr>
<tr><td>Integridad de los datos</td></tr>
<tr><td>Privacidad</td><td colspan="2">La privacidad está garantizada por la ausencia de datos vulnerables en los mensajes que se transfieren, así como por la implementación de los oportunos mecanismos de almacenamiento de datos y las facilidades de control de acceso al sistema.
Los componentes del sistema no deben ofrecer posibilidades latentes de que se adquieran o transfieran datos sin autorización.</td></tr>
<tr><td>Seguridad de la comunicación</td><td colspan="4">La entrega de un mensaje a su destinatario está garantizada, como también lo está la seguridad frente a la revelación no autorizada en el momento de la transferencia por los canales de comunicación. La garantizan los proveedores de comunicaciones de la red NGN.</td></tr>
<tr><td>Disponibilidad</td><td colspan="4">Garantiza que no haya denegación de accesos autorizados a los servicios y datos del sistema. La disponibilidad está asegurada por los proveedores de comunicaciones de la red NGN, así como por los proveedores de servicios.</td></tr>
</table>

Bibliografía

[b-UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *General overview of NGN*.

[b-PA-DSS] Payment Card Industry (PCI), *Payment Application Data Security Standard. Requirements and Security Assessment Procedures*, Versión 2.0, octubre de 2010.

[b-PCI DSS] Payment Card Industry (PCI), *Data Security Standard. Requirements and Security Assessment Procedures*, Versión 2.0, octubre de 2010.

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
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2011