UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Q.1531

(06/2000)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN

Red inteligente

Requisitos de seguridad en telecomunicaciones personales universales para el conjunto de servicios 1

Recomendación UIT-T Q.1531

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
FUNCIONES Y FLUJOS DE INFORMACIÓN PARA SERVICIOS DE LA RDSI	Q.60–Q.99
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.° 4 Y N.° 5	Q.120–Q.249
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 6	Q.250–Q.309
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R1	Q.310–Q.399
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R2	Q.400–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 7	Q.700–Q.799
INTERFAZ Q3	Q.800–Q.849
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.° 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	**Q.1200–Q.1699**
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000	Q.1700–Q.1799
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2999

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

Recomendación UIT-T Q.1531

Requisitos de seguridad en telecomunicaciones personales universales para el conjunto de servicios 1

Resumen

Esta Recomendación especifica los requisitos de seguridad UPT para las comunicaciones usuario a red y entre redes aplicables al conjunto de servicios 1 de UPT definido en la Recomendación F.851 [1]. Esta Recomendación cubre todos los aspectos de la seguridad para las UPT que utilizan acceso DTMF y accesos de usuario basados en DSS1 fuera de banda.

Orígenes

La Recomendación UIT-T Q.1531, preparada por la Comisión de Estudio 11 (1997-2000) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la CMNT el 15 de junio de 2000.

Palabras clave

UPT, seguridad.

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 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 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

Recomendación Q.1531

Requisitos de seguridad en telecomunicaciones personales universales para el conjunto de servicios 1

1 Alcance

Esta Recomendación UIT-T especifica los requisitos de seguridad UPT para las comunicaciones usuario a red y entre redes aplicables al conjunto de servicios 1 definido en la Recomendación F.851 [1]. Por regla general, hay dos métodos de acceso del usuario a la UPT. Uno es el acceso de usuario basado en la multifrecuencia bitono (DTMF) dentro de banda, y el otro es un acceso de usuario fuera de banda tal como la señalización basada en DSS1. Los requisitos dependen de la utilización de estos métodos. La presente Recomendación trata todos los aspectos de seguridad de la UPT que utiliza el acceso DTMF y los accesos de usuario basados en la DSS1 fuera de banda.

2 Referencias

La siguiente Recomendación 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.

[1] Recomendación UIT-T F.851 (1995), *Telecomunicación personal universal – Descripción del servicio (conjunto de servicios 1).*

3 Definiciones de términos

3.1 Términos definidos en la Recomendación F.851 [1]

Los siguientes términos se definen en la Recomendación F.851 [1].

– autenticación;

– identificación;

– movilidad personal;

– telecomunicación personal universal (UPT);

– perfil de servicio UPT;

– gestión del perfil de servicio UPT;

– proveedor del servicio UPT;

– abonado UPT;

– usuario UPT.

3.2 Términos no definidos en la Recomendación F.851 [1]

En esta Recomendación se definen los términos siguientes.

3.2.1 autorización: Propiedad por la cual se establecen y entran en vigor los derechos de acceso a los recursos.

3.2.2 confidencialidad: Propiedad por la cual la información relativa a una entidad o parte no se encuentra disponible o es revelada a individuos, entidades o procesos no autorizados.

3.2.3 integridad: Propiedad por la cual el contenido de información de un objeto es protegido contra su modificación de un modo no autorizado.

3.2.4 privacidad: Provisión de capacidades para proteger a los usuarios contra los inconvenientes de su libertad de acción.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

CS-1 Conjunto de capacidades 1 (*capability set 1*)

CS-2 Conjunto de capacidades 2 (*capability set 2*)

DSS1 Sistema de señalización digital de abonado N.º 1 (*digital subscriber signalling No. 1*)

DTMF Multifrecuencia bitono (*dual tone multiple frequency*)

IC-card Tarjeta de circuito integrado (*integrated circuit-card*)

MAC Código de autenticación de mensaje (*message authentication code*)

OCPIN PIN de llamada saliente (*outgoing call PIN*)

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

PIN Número de identificación personal (*personal identification number*)

PINX Central de red integrada privada (*private integrated network exchange*)

PUI Identidad personal de usuario (*personal user identity*)

RDSI Red digital de servicios integrados

RGT Red de gestión de telecomunicaciones

RI Red inteligente

RMTP Red móvil terrestre pública

SAPIN PIN de respuesta segura (*secure answering PIN*)

SCP Punto de control de servicio (*service control point*)

SDP Punto de datos de servicio (*service data point*)

SS7 Sistema de señalización N.º 7 (*signalling system No. 7*)

UPT Telecomunicaciones personales universales (*universal personal telecommunication*)

5 Introducción

La libertad otorgada a los usuarios UPT de moverse libremente de un terminal a otro acarrea también que puedan hacerse tentativas de utilización fraudulenta de sus abonos desde cualquier terminal. Los abonados UPT están por tanto más expuestos al uso fraudulento de sus abonos que los abonados ordinarios. Es necesario que el servicio UPT proporcione mecanismos de seguridad suficientes, de

modo que el nivel de riesgo a que estén expuestos los abonados UPT no se presente prohibitivo en comparación con los abonados ordinarios.

Los mecanismos de seguridad proporcionados por el servicio UPT, con independencia de la fortaleza de su protección, no deben, sin embargo, aparecer al usuario UPT como una complicación adicional en absoluto, sino que deben formar parte de los procedimiento UPT generales.

La seguridad en un contexto UPT se refiere a los aspectos de:

a) fraude;

b) confidencialidad;

c) disponibilidad del servicio;

d) esquema de protección.

5.1 Fraude

Fraude es el uso indebido de facilidades UPT por usuarios no autorizados, en particular el uso facturable del servicio UPT, cuya factura se carga a la cuenta del usuario UPT legítimo. Como consecuencia, se requiere por ejemplo:

a) la autenticación de usuarios y abonados;

b) los detalles de las llamadas;

c) la auditoria (análisis retrospectivo).

5.2 Confidencialidad

La confidencialidad consiste en que la información concerniente al usuario UPT y al abonado UPT no sea revelada a quien no tenga autorización legal para examinarla. Esta información comprende:

a) el contenido de la comunicación;

b) los detalles de la facturación;

c) los detalles de las llamadas;

d) los detalles del registro.

5.3 Disponibilidad del servicio

La capacidad de los usuarios UPT de recibir los servicios UPT en el momento que lo desean puede verse limitada por:

a) la fiabilidad del servicio;

b) la denegación del servicio.

5.4 Esquema de protección

Las especificaciones UPT deben definir los mecanismos de seguridad apropiados para proteger frente a cualquier peligro contra la seguridad a:

a) los usuarios UPT;

b) los operadores de red con capacidad UPT y los proveedores de servicios;

c) el servicio UPT,

debido a las circunstancias en que se espera que se preste el servicio UPT. UPT será un sistema abierto con acceso de ámbito mundial y con la posibilidad de que el fraude sea mínimo.

6 Descripción general

6.1 Objetivos generales para la seguridad

Se aplican los siguientes objetivos generales a la seguridad de la UPT:

a) el usuario UPT puede utilizar el servicio UPT con un riesgo mínimo de que se viole su privacidad o de que se produzcan facturaciones erróneas debidas a la utilización fraudulenta;

b) la seguridad proporcionada a un usuario UPT cuando utiliza servicios UPT debe ser comparable a la seguridad que proporcionan las redes fijas y móviles contemporáneas cuando utilizan los mismos servicios;

c) la seguridad proporcionada a un operador de red o proveedor de servicio UPT debe ser como mínimo comparable a la seguridad proporcionada por las redes fijas y móviles contemporáneas y debe proteger los intereses empresariales de dichos proveedores u operadores;

d) los aspectos legales, reglamentarios y comerciales de la seguridad proporcionada por el servicio UPT deben contemplar la disponibilidad a nivel mundial;

e) la seguridad que ha de proporcionar el servicio UPT debe normalizarse adecuadamente para proveer una interoperabilidad e itinerancia internacionales seguras.

6.2 Requisitos generales de seguridad

La introducción del servicio UPT y las poderosas capacidades de comunicación que éste permite requieren que se disponga de distintos mecanismos de seguridad para proteger a los usuarios afectados. Los niveles de seguridad ofrecidos por estos mecanismos dependen de varios factores:

a) los mecanismos de seguridad concretos que pueden elegirse;

b) la elección de terminales UPT y dispositivos UPT;

c) la utilización real de los procedimientos UPT;

d) la elección de los procedimientos de acceso y autenticación.

Se señala que los mecanismos de seguridad aparecen como partes integrantes de determinados procedimientos UPT. En general, es deseable que todos los mecanismos de seguridad sustentados por el servicio UPT sean sencillos de utilizar y aparezcan como parte de los procedimientos generales UPT.

Es conveniente que los proveedores del servicio UPT sustenten una gama de niveles de seguridad que se ofrecerían a los usuarios UPT para que eligieran en el momento del abono.

El nivel de seguridad ofrecido al usuario UPT depende considerablemente de la elección del grado de autenticación.

7 Peligros que amenazan la seguridad de la UPT

Debido a la naturaleza flexible del servicio UPT, los abonados UPT están muy expuestos al uso fraudulento de sus abonos. Los usuarios UPT pueden, en principio, utilizar cualquier terminal en el mundo para realizar o recibir llamadas que será facturadas a su cuenta. De igual modo, una persona malintencionada puede utilizar incorrectamente la cuenta de los abonados UPT desde cualquier terminal en el mundo. Es prudente que en el servicio UPT se protejan específicamente:

a) las facturas de los abonados;

b) la responsabilidad del usuario con sus abonados;

c) los datos personales de los usuarios;

d) la integridad de la red;

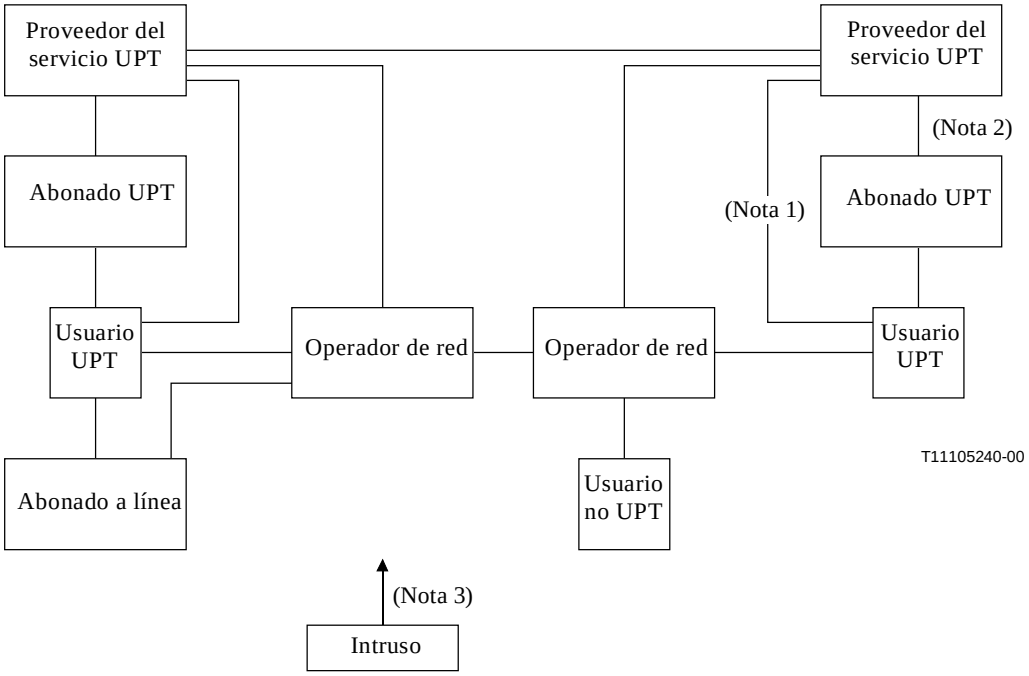
e) los flujos de ingresos de los operadores de la red;

f) la reputación de los operadores de la red;

contra los ataques fraudulentos o malintencionados por parte de cualquier persona.

Hay una gran variedad de relaciones entre las diferentes partes de la UPT. Todas las relaciones han de ser controladas mediante acuerdos adecuados que tengan en cuenta las diferentes situaciones legales vigentes en los diversos países.

En la figura 1 se presenta un diagrama representativo de las relaciones entre las partes involucradas en la UPT. El intruso no ha sido situado específicamente dentro del diagrama ya que la relación depende exclusivamente del tipo de intrusión perpetrada.



NOTA 1 – Por ejemplo, acceso y gestión del perfil de servicio.
NOTA 2 – Por ejemplo, tarificación y gestión del perfil de servicio.
NOTA 3 – Un intruso puede atacar cualquier parte y cualquier enlace entre partes.

Figura 1/Q.1531 – Modelo de partes UPT y sus relaciones

7.1 Peligros asociados con las características de la UPT

Los principales peligros a que se ve sometido el servicio UPT se enumeran a continuación.

Suplantación (impostura) como usuario UPT

Un intruso puede utilizar los datos de autenticación obtenidos por escucha indiscreta para efectuar llamadas con un número UPT, de modo que el abonado UPT de este número habría de pagar la tarificación generada por estas llamadas del intruso.

Un intruso puede utilizar información obtenida por escucha indiscreta para registrar llamadas entrantes en algún otro número UPT. Como consecuencia, el usuario UPT perderá sus llamadas entrantes, que pueden ser reenviadas por el intruso, y el abonado UPT corresponsal puede tener que pagar las facturas de estas llamadas (por ejemplo, en la tarificación dividida).

Suplantación (impostura) como proveedor del servicio UPT

Si un tercero tiene éxito en suplantar la identidad de un proveedor del servicio UPT, la seguridad del usuario UPT se ve comprometida por algunos peligros graves.

Lectura o modificación no autorizada de los datos del abono por el usuario/abonado

Un usuario/abonado puede leer o modificar los datos del abono en el perfil del servicio sin estar autorizado para ello por el proveedor del servicio en el acuerdo con su abonado (y posiblemente proveedor de servicio) debido a la escasa protección del perfil de servicio.

Inexactitud de los datos de facturación

Un peligro que amenaza a la facturación es la posible incorrección de los datos de la cuenta de facturación, tanto para el abonado como para el proveedor del servicio UPT y el operador de red, que tarifican uno a otro por el uso del servicio y la red.

Escucha indiscreta de la identidad del usuario, información de autenticación y datos de registro

Los datos de registro, la identidad del usuario y los datos de autenticación pueden ser obtenidos por escucha indiscreta durante el registro, por ejemplo utilizando un terminal simulado, información de radiación electromagnética, grabación de las señales en la línea, etc. Como consecuencia, se pueden generar muchos otros peligros.

Registro no autorizado

Registro de un número personal arbitrario en un acceso de terminal elegido, sin que el abonado a línea se de cuenta. El abonado a línea puede recibir llamadas entrantes perturbadoras/no deseadas. El usuario UPT puede tener que pagar por la llamada en el caso de que se aplique el sistema de tarificación dividida.

Utilización no autorizada del dispositivo de acceso UPT

Si el dispositivo contiene información de autenticación, ésta puede ser robada y utilizada por un simulador. De modo similar, el acceso temporal al dispositivo puede permitir la extracción de la información de autenticación.

Los peligros asociados con las características opcionales UPT específicas y los mecanismos de protección de terceros se enumeran a continuación.

Peligros asociados con el registro de llamadas salientes (incluido el registro de todas las llamadas y el registro vinculado activado a distancia o no)

Algunas personas pueden suscribir un abono, utilizarlo intensamente y evitar el pago de la factura. La repercusión de esta práctica se hace mayor por la posibilidad de efectuar varios registros de llamadas salientes al mismo tiempo.

La impostura (suplantación de identidad) como usuario UPT para el registro de llamadas salientes, registro de todas las llamadas y registro vinculado entrañará un riesgo económico grande en el caso de que el intruso adquiera datos de autenticación válidos.

Un usuario registrado puede no tener capacidad para supervisar el terminal (o terminales) registrado(s), por lo que un intruso puede efectuar llamadas sin pagar la factura. (véase también el elemento "Suplantación (impostura) como usuario UPT).

Un registro en un teléfono RDSI implica un registro en todos los terminales conectados al mismo bus-S de RDSI. El usuario UPT está puesto en peligro por la posibilidad que existe de que no se de cuenta de registros efectuados en más de un terminal (colocado posiblemente en otras piezas del domicilio).

Peligros asociados con "parte llamada especificó respuesta segura de llamadas entrantes"

Si un tercero tiene éxito en la suplantación como proveedor de servicio UPT, puede necesitar que la autenticación se efectúe simplemente haciendo una llamada telefónica al usuario UPT. El código de autenticación resultante puede ser registrado y reutilizado posteriormente para un registro ilegal o llamada saliente, etc., si se utiliza solamente la autenticación débil.

Peligros asociados con la toma de llamada

Cualquier usuario no válido puede tomar la llamada a menos que se efectúe la autenticación del usuario.

Peligros asociados con el registro de múltiples direcciones de terminal

En caso de registro de múltiples direcciones de terminal, el peligro de utilización incorrecta (con intención de no pagar la factura) y el peligro de impostura habrán aumentado los riesgos y el nivel de los mismos.

Peligros asociados con la puesta a cero de los registros

Este servicio se destina a proteger a terceros contra registros UPT no deseados. Sin embargo, puede también ocasionar la denegación de servicio para los usuarios UPT. Esto puede ser especialmente enojoso si se reinicia el registro sin que el usuario UPT se aperciba de ello.

7.2 Peligros asociados con las comunicaciones entre redes

Para el intercambio de datos relativos a la explotación, mantenimiento y tarificación entre proveedores del servicio UPT y operadores de redes capaces de UPT, se han de definir algunos procedimientos relativos a las comunicaciones entre redes específicas del servicio UPT.

Los peligros relacionados con las comunicaciones entre redes del servicio UPT se enumeran a continuación:

Suplantación (impostura) como entidades UPT

Un intruso puede simular una entidad UPT (por ejemplo, SCP, SDP) para la dirección o recepción ilegal de llamadas a través de una red capaz de UPT.

Modificación, borrado y reproducción de datos de señalización UPT

Un intruso puede cambiar la información de señalización con el fin de perturbar el servicio o manipular la información de tarificación.

Escucha indiscreta de datos de señalización UPT

Un intruso puede supervisar los datos de señalización para conseguir información referente, por ejemplo, a la posición de un usuario, o información interna de los proveedores del servicio UPT correspondientes.

Suplantación como originador, repudio, modificación, borrado y reproducción de ficheros y mensajes

Un intruso puede iniciar una de las acciones anteriores en beneficio propio, especialmente con el objetivo de manipular los datos de tarificación.

Escucha indiscreta de ficheros y mensajes

Un intruso puede supervisar ficheros y mensajes, por ejemplo para conseguir información acerca de la ubicación de un usuario o para revelar información de bases de datos confidencial de los proveedores del servicio UPT.

Privacidad de los datos en un entorno competitivo

Las comunicaciones interredes pueden también invocar aspectos de la seguridad en relación con la naturaleza competitiva de los datos del abonado al servicio.

7.3 Situaciones no intencionadas

Los peligros relativos a situaciones no intencionadas se enumeran a continuación.

Conexión de red a bases de datos erróneas

Se produce una situación de peligro no intencionada cuando el SCP no se conecta al SDP correcto. En tal caso, puede ser revelada información de otras personas. Por ejemplo, un usuario UPT ha sido autenticado por "su" SDP, pero la siguiente nueva tentativa de conexión con este SDP produce, debido a un error, una conexión con otro SDP.

8 Requisitos relativos a la seguridad del sistema

En esta cláusula se describen los requisitos de seguridad del sistema. Estos requisitos se aplican a una o más de las partes involucradas en el servicio UPT.

Los requisitos del sistema sobre la seguridad UPT se agrupan en las siguientes categorías:

a) requisitos relativos al servicio;

b) requisitos relativos al acceso;

c) requisitos de funcionamiento de la red;

d) requisitos de gestión de seguridad.

8.1 Requisitos del servicio

Los siguientes requisitos sobre seguridad relativos al servicio se aplican al servicio UPT:

a) las prestaciones de seguridad previstas para la protección de los usuarios UPT deben ser cómodas para el usuario y fáciles de utilizar. Deben ser, en la mayor medida posible, transparentes a los usuarios, y deben requerir la menor interacción posible entre el usuario y la red;

b) las características de seguridad previstas para la protección de los usuarios UPT no deben aumentar de manera significativa los tiempos de establecimientos de la llamada;

c) las características de seguridad no deben reducir el nivel de la seguridad en condiciones de itinerancia;

d) las característica de seguridad proporcionadas por el servicio UPT deben operar en distintos entornos de UPT, y no deben ser limitadas por ninguna capa física o método de acceso;

e) la privacidad de los usuarios no UPT no debe verse afectada por la utilización de equipos o servicios UPT.

8.2 Requisitos del acceso

Los siguientes requisitos sobre seguridad relativos al servicios se aplican al servicio UPT:

a) deberá ser muy difícil para los intrusos simular al usuario o abonado UPT;

b) deberá ser muy difícil para los intrusos simular a un proveedor de servicio/operador de red UPT en comunicación con un usuario UPT, o en comunicación con otros proveedor de servicio UPT;

c) deberá ser muy difícil para los intrusos acceder, leer o modificar la información del abono del usuario UPT que se encuentra almacenada o es transmitida;

d) el proveedor del servicio UPT dispondrá de mecanismos para comprobar la corrección y autenticidad de las transacciones llevadas a cabo con usuarios UPT;

e) deberá ser muy difícil para un intruso acceder o implantar instrucciones falsas en la estructura de señalización de la red capaz de UPT, así como en las funciones de control relacionadas.

8.3 Requisitos de funcionamiento de la red

Los siguientes requisitos sobre seguridad relativos al funcionamiento de la red se aplican al servicio UPT:

a) se debe normalizar adecuadamente la seguridad que ha de proporcionar el servicio UPT, de modo que se proporcionen una itinerancia e interoperabilidad seguras en el ámbito internacional. Sin embargo, dentro del mecanismo de seguridad de la UPT, deberá permitirse la máxima independencia entre las partes implicadas en el funcionamiento UPT, así como la máxima libertad de todos las partes para implantar sus propias políticas y mecanismos de seguridad;

b) los mecanismos de seguridad de UPT deben requerir el mínimo posible de conexiones de señalización de larga distancia en tiempo real (para evitar, por ejemplo, el establecimiento de conexiones de señalización internacional en cada proceso de actualización de posición o en cada llamada durante la itinerancia).

8.4 Requisitos relativos a la gestión de la seguridad

Los siguientes requisitos relativos a la gestión de la seguridad se aplican al servicio UPT:

a) las claves y dispositivos de seguridad distribuidos a los usuarios UPT deben poderse gestionar y actualizar fácilmente y de modo seguro;

b) la gestión de las claves de seguridad dentro de los proveedores del servicio UPT y entre ellos debe ser segura;

c) el proveedor del servicio UPT debe disponer de mecanismos seguros para registrar eventos asociados con los usuarios o abonados UPT;

d) deberá ser muy difícil para los intrusos simular a un proveedor del servicio UPT en comunicación con operadores de redes capaces de UPT, y viceversa;

e) los mecanismos de seguridad proporcionados por el servicio UPT deben disponer de medios para la gestión de versión, y deben ser fáciles de actualizar durante la vida útil de la UPT.

9 Características de seguridad de la UPT

En la UPT, como en todos los sistemas existentes en la práctica que son accesibles al público en general, han de estar presentes, y cooperar entre sí, muchas prestaciones de seguridad diferentes para dar el nivel requerido de seguridad global.

Los servicios de seguridad se pueden distinguir por alguna de las siguientes propiedades:

Preventivo: intenta hacer imposibles los peligros.

Informativo: proporciona la gestión del sistema o la información de usuario acerca de la seguridad.

Limitativo: introduce restricciones en el sistema para limitar las consecuencias de las posibles brechas en la seguridad.

Restaurador: efectúa un retorno rápido, seguro y ordenado al funcionamiento normal después de que se han solventado los problemas de seguridad.

Disuasorio: tiene la propiedad de que los usuarios restringen ellos mismos los posibles usos incorrectos al tener conocimiento de la existencia de esta característica de seguridad.

Todas estas propiedades son necesarias y constituyen elementos valiosos de la arquitectura de la seguridad UPT global.

Se pueden identificar las siguientes características para UPT:

a) confidencialidad;

b) autenticación;

c) integridad;

d) autorización y control de acceso;

e) privacidad y anonimato;

f) disponibilidad del servicio;

g) limitación de eventos;

h) informe de eventos.

9.1 Características del servicio UPT que aportan seguridad

Estas características no siempre suficientes por sí solas para contrarrestar un peligro concreto, pero contribuyen sin embargo (en unión de otras medidas de seguridad) a alcanzar el nivel de seguridad requerido.

Limitación del importe de la factura

La limitación de la factura, o crédito, es el único camino efectivo de limitar las consecuencias de una utilización extensiva, y posiblemente no autorizada, por el usuario, o el uso fraudulento por intrusos impostores. El límite de la facturación acumulada debe ser fijado por el proveedor del servicio en cooperación con el abonado. Para que el control sea efectivo, debe efectuarse en conexión con la autenticación para cada llamada saliente (la cual puede ampliarse al control de las llamadas entrantes dependiendo de la política de seguridad y de tarificación del operador). Cuando se rebase este límite, el proveedor del servicio no permitirá más llamadas que incrementen las cargas. El usuario debe ser avisado de esta situación inmediatamente antes de que se alcance dicho límite y de las tentativas de llamadas efectuadas después de alcanzarse el límite.

Para una protección extra, el proveedor del servicio puede restringir la continuación de llamadas salientes, el registro de llamadas salientes o el registro de llamadas salientes distante.

Facturación detallada

Las facturas detalladas juegan un papel importante frente a algunos peligros que de otro modo no serían tan fácilmente descubiertos o evitados. Un inconveniente de este método estriba por supuesto en que la detección de los problemas se retrasa hasta la recepción de la factura, y que su solución depende de un examen a fondo de la misma. El hecho de que se conozca que se está aplicando la facturación pormenorizada tendrá un efecto disuasorio, que puede retener a algunas personas en el uso indebido o incorrecto del servicio.

Puede ser necesario que haya que prestar especial atención a la protección de la privacidad.

Supervisión de actividades

La supervisión de actividades es la supervisión en tiempo real de las actividades y eventos asociados con la factura del usuario o con el propio servicio UPT, incluidas alguna o todas de las siguientes: tentativas de autenticación, actividades de llamada, indicaciones de tarificación. El esquema de una actividad de usuario puede indicar que su cuenta esta sufriendo algún abuso. La supervisión de actividades es la única actuación rápida de protección contra el uso fraudulento de que dispone el

proveedor del servicio UPT (e indirectamente, sus abonados y usuarios). Resulta necesaria especialmente cuando se utiliza la autenticación débil.

Avisos

Los avisos dados desempeñan una función importante en la seguridad del servicio. Deben ser diseñados cuidadosamente para informar a los usuarios y a terceros sobre los diferentes estados de sus conexión o relación con el operador/proveedor del servicio.

Puede ser necesario que haya que prestar especial atención a la protección de la privacidad.

Bloqueo del registro

El bloqueo del registro puede ser un medio para un tercero de evitar permanentemente registros UPT. Si el bloqueo UPT es el estado original por defecto de todos los abonados a línea y solamente un desbloqueo activo por parte del abonado a línea permite el registro UPT, entonces se puede conseguir una protección substancial de terceros. Este sistema puede constituir la práctica normal en los registros a distancia. El desbloqueo puede efectuarse de dos maneras: mediante el consentimiento escrito del abonado a línea que permita, bien efectuar registros de números UPT específicos o de todos los registros UPT, o bien por procedimientos en línea. El consentimiento puede esta sujeto a condiciones diferente según las condiciones ofrecidas por el proveedor del servicio UPT a este respecto. El tercero deberá poder retirarse de sus acuerdos anteriores.

Los registros locales, donde el registro de un terminal de línea específico se efectúa desde el mismo terminal, deben ser excluidos de este requisito.

Puesta a cero del registro

La reiniciación del registro es una parte esencial del servicio UPT. Sin embargo, esta puesta a cero del registro no aporta una protección completa contra los problemas derivados de los registros no deseados, ya que no se puede espera en general que los terceros estén familiarizados con los procedimientos de reiniciación.

Acuerdos contractuales

Los acuerdos contractuales relativos a temas de seguridad deben incluirse en las condiciones del abono. Las partes, relativas a la seguridad, de las condiciones que el abonado ha de acordar y firmar debidamente pueden ser:

a) seguir las reglas (declaradas por el proveedor del servicio UPT y anexadas al contrato de abono) relativas al tratamiento seguro de la PUI y el PIN para la autenticación débil, y las reglas correspondientes en relación con el uso de dispositivos UPT;

b) informar inmediatamente al proveedor del servicio sobre las pérdidas de PIN o dispositivo, o de otras condiciones que puedan conducir al fraude o uso incorrecto del servicio;

c) respetar las restricciones en el uso del servicio que puedan imponerse con respecto a la protección de un tercero;

d) aceptar las limitaciones del servicio derivadas de los niveles acordados de control del crédito/limitación de facturación;

e) aceptar las limitaciones del servicio que el proveedor del mismo puede juzgar necesario introducir más tarde para proteger el servicio UPT contra el fraude y la utilización incorrecta;

f) aceptar la responsabilidad civil derivada del posible fraude o uso incorrecto de la factura del abonado cuando éste o sus usuarios hayan quebrantado gravemente las reglas;

g) imponer las instrucciones y restricciones correspondientes a sus usuarios (si son distintos del abonado).

9.2 Características de seguridad del acceso de usuario

Muchos peligros pueden evitarse por la aplicación de las prestaciones ya definidas en el concepto de servicio UPT. Estas prestaciones se describen en UIT-T F.851 [1] como oferta de servicio UPT general. Los servicios de seguridad específicos requeridos para evitar la mayor parte de los peligros se enumeran aquí.

Las prestaciones de seguridad que se han identificado como necesarias para enfrentarse a los peligros de la UPT son las siguientes:

Autenticación del usuario UPT/abonados UPT

Los peligros relacionados con la suplantación de identidad hacia el proveedor del servicio UPT son los que se han identificado como más importantes, y la autenticación del usuario UPT (y del abonado UPT) es la principal característica de seguridad del servicio UPT. Por este motivo se recomienda una autenticación fuerte que utilice un dispositivo UPT avanzado y dotado de inteligencia (por ejemplo, un dispositivo del tipo DTMF o un dispositivo de tarjeta IC). La autenticación débil no es una solución suficiente en sí misma, y sólo se puede aceptar cuando vaya acompañada de otras característica de seguridad y de limitaciones del servicio.

Control de acceso al dispositivo de acceso UPT

Para controlar el acceso a información sensible en el dispositivo de acceso UPT se requieren dos características:

a) la autenticación de usuario/propietario hacia el dispositivo;

b) la protección física fuerte, por ejemplo, utilizando una tarjeta IC del tipo de microprocesador.

Sistema de control de acceso a la información del perfil de servicio

Los usuarios, abonados y personal del proveedor del servicio tendrán acceso a diferentes partes del perfil del servicio. Para controlar el acceso a las bases de datos de perfiles de servicio es preciso disponer de un sistema de control de acceso. Parte de este control de acceso será, por supuesto, la autenticación del usuario/abonado UPT. La autenticación del personal y el control de acceso en el entorno del local del proveedor del servicio debe disponer de una solución dedicada para este entorno de soporte físico y soporte lógico.

Gestión segura del proceso de abono

Se ha de disponer en primer lugar de procedimientos seguros y rigurosos para la administración de los abonos y de toda la información y dispositivos secretos, así como de sistema de control de acceso adecuados para los abonos.

El abono puede ser tratado (parcialmente) vía medios de telecomunicación si existen medidas de seguridad adecuadas (autenticación, control de acceso). Muy probablemente, la suscripción será manual (con presencia personal o por correo), adoptándose las medidas de seguridad correspondientes para este caso.

Este servicio debe ser diseñado para que proteja contra peligros tales como:

a) la modificación no autorizada de los datos del abono por el usuario o el abonado;

b) la cancelación no autorizada del abono;

c) la denegación del servicio por el mal funcionamiento del dispositivo;

d) la entrega incorrecta de dispositivos UPT.

Las prestaciones (características) de seguridad necesarias para alcanzar el nivel deseado de gestión de la seguridad pueden variar substancialmente dependiendo de los diferentes entornos de los proveedores del servicio, y su estudio cae fuera del alcance de esta Recomendación.

9.3 Características de seguridad para las comunicaciones entre redes

En las comunicaciones entre redes se han de considerar los siguientes requisitos de seguridad:

a) seguridad de los diálogos;

b) seguridad de las transferencias de ficheros.

Los requisitos de seguridad descritos aquí, no sólo se pueden aplicar al servicio UPT, sino también a la protección de otras comunicaciones interredes RI. Por razones de eficacia, todos los servicios de RI deberán utilizar normalmente, y siempre que sea posible, funciones de seguridad.

Por consiguiente, deberá considerarse la asignación de características de seguridad dentro de la estructura OSI. Se identifican los siguientes requisitos:

a) las funciones de seguridad deben ser independientes en la mayor medida posible de la red subyacente;

b) los protocolos de seguridad deberán ser independientes en la mayor medida posible de los protocolos de la capa de aplicación.

Las características de seguridad definidas en esta subcláusula se distribuyen entre dos entidades RI. Los enlaces de red forman parte del SS7.

Las características de seguridad mencionadas en los puntos siguientes se muestran a título de ejemplo. Las características y mecanismos de seguridad necesarios deben ser examinados en conexión con el desarrollo de una arquitectura de seguridad de RI general.

9.3.1 Diálogo seguro

Los diálogos seguros deben estar constituidos por un procedimiento de autenticación mutua, un servicio de confidencialidad y un servicio de integridad de los datos en el enlace de comunicación. Los mecanismos de seguridad proporcionados pueden ser:

a) la autenticación mutua;

b) la criptación del enlace;

c) la integridad de los datos del enlace;

d) la gestión de claves para soportar este diálogo seguro.

9.3.2 Transferencia segura de ficheros

Los ficheros deben protegerse mediante dos prestaciones de seguridad: integridad de los datos del fichero y confidencialidad del fichero. Los mecanismos de seguridad proporcionados pueden ser:

a) firma digital o MAC para la integridad de los datos del fichero;

b) criptación del fichero;

c) gestión de claves para soportar esta transferencia segura.

La verificación/protección de la integridad y la criptación/descriptación son funciones locales en las entidades comunicantes respectivas.

9.4 Limitación de la seguridad

Esta subcláusula identifica los peligros que pueden ser evitados por las características de seguridad pertinentes. Algunos de estos peligros se pueden considerar de importancia menor, bien porque la probabilidad de que ocurran es baja, o bien porque sus consecuencias sólo son de poca importancia, y a menudo por ambos motivos. En el caso de otros peligros, no se ha identificado un método realizable (justificado por el coste) de protección contra ellos.

9.4.1 Acceso de usuario basado en la multifrecuencia bitono (DTMF)

Los peligros no cubiertos incluyen todos los afectados por la escucha indiscreta o la manipulación activa de las líneas utilizadas para los registros UPT. Los peligros asociados a la escucha indiscreta implican un grado de vulnerabilidad elevado, especialmente si se registran los datos (por ejemplo, PUI, PIN) de autenticación. Existe, sin embargo, una diferencia substancial en cuanto al riesgo si se aplica la autenticación débil en lugar de la autenticación fuerte recomendada. Esto es especialmente cierto si el registro se transporta por el aire, como un acceso RMTP, o si atraviesa algún equipo que tiene facilidades de registro inherentes, como algunas PINX. Esto constituye un motivo para limitar el servicio de UPT cuando se utiliza la autenticación débil.

La protección contra registros molestos realizados a terminales de terceros de manera inconsciente y no intencionada no aporta una solución definitiva en el caso del acceso de un usuario basado en DTMF, debido a que no se puede disponer en general de la puesta a cero de los registros. Las indicaciones, tonos de marcar, etc., recomendados no son suficientes. Las condiciones de bloqueo por defecto y el acuerdo activo a través de acuerdos previos al registro o en línea son posibles, pero pueden no resultar suficientes.

9.4.2 Acceso de usuario basado en DSS1 fuera de banda

Puesto que se dispone de dos métodos de autenticación en los accesos DSS1, solamente quedan sin proteger los peligros relativos a la manipulación de línea activa y a la escucha indiscreta de los datos personales.

La manipulación activa de la línea relacionada con el registro molesto puede ser parcialmente protegida por prestaciones de gestión de seguridad tales como el reinicio del registro, la limitación de la facturación y la limitación del servicio.

La escucha indiscreta de los códigos de autenticación no tiene ninguna repercusión cuando se utiliza la autenticación fuerte.

10 Mecanismos de seguridad del servicio UPT

10.1 Mecanismos de control del acceso

Los mecanismos de control del acceso se utilizarán en los tres campos siguientes:

a) acceso al servicio basado en la identidad del usuario o abonado;

b) acceso al perfil de servicio y otros datos de gestión por usuarios, abonados, personas autorizadas de los proveedores del servicio, y por consultas procedentes de entidades de red de domicilio o visitadas;

c) acceso a los datos en el dispositivo de acceso UPT.

10.1.1 Control de acceso a los servicios

El control de acceso al servicio UPT o a determinadas funciones de servicio puede contemplarse como un proceso combinado de la identificación y la autenticación de las partes involucradas

Los mecanismos de control de acceso a los servicios deberán utilizar las siguientes listas de autenticación:

Listas blancas

Las listas blancas son listas de control de acceso o listas de capacidades que especifican los servicios que pueden utilizar los usuarios y abonados UPT individuales. Estas listas pueden constituirse como parte de los datos de perfil de servicio correspondientes.

Listas negras

Las listas negras especifican aquellas identidades que no deberán ser aceptadas como autorizadas para acceder al servicio UPT debido, por ejemplo, a que el usuario UPT ha rebasado el límite de crédito. Las listas negras deberán actualizarse con la mayor frecuencia posible. Se prepararán en la entidad de autenticación (por ejemplo, SCP, SDP).

Listas grises

El proveedor UPT puede definir listas grises, y además, para aquellas identidades con las que deben adoptarse medidas adicionales, por ejemplo, cuando deba activarse una supervisión de actividades detallada.

Para la autenticación débil, una PUI es bloqueada si el acceso es denegado temporalmente cuando se producen también demasiadas tentativas de autenticación consecutivas equivocadas. El bloqueo deberá realizarse en la entidad autenticante. Debe proveerse un procedimiento de desbloqueo, puesto que se puede bloquear maliciosamente la PUI de algún usuario. Sin embargo, el usuario con la PUI bloqueada sufre grandes complicaciones.

En el caso de la autenticación fuerte, no debe bloquearse una identidad, ya que la autenticación puede ser considerada suficientemente segura. La clave de usuario debe cambiarse si se revelan tanto la clave como el algoritmo.

10.1.2 Control de acceso a los datos del perfil de servicio

El acceso a los datos del perfil de servicio debe quedar restringido a los siguientes sujetos y con distintos derechos:

a) usuario UPT;

b) abonado UPT;

c) proveedor del servicio UPT.

La información almacenada en los datos del perfil de servicio puede dividirse, desde el punto de vista del usuario UPT, en información fija e información variable. La información fija es típicamente fijada en el momento del abono y solo puede ser modificada por el proveedor del servicio UPT, probablemente a petición del abonado UPT. La información variable puede ser modificada por el usuario UPT o su abonado UPT, bien explícitamente mediante el uso de las funciones de gestión del perfil de servicio o bien implícitamente utilizando funciones de movilidad personal.

El proveedor del servicio UPT es responsable de que sólo puedan acceder a los datos las personas autorizadas. La especificación de los mecanismos pertinentes es responsabilidad del proveedor del servicio UPT y cae fuera al alcance de esta Recomendación. El acceso de señalización (por ejemplo, mediante SS7) deberá protegerse aplicando la autenticación de las entidades de red y las listas de autorización que contienen los proveedores del servicio con contratos de itinerancia, de conformidad con el contrato entre los proveedores del servicio.

10.1.3 Control de acceso a los datos en el dispositivo UPT

El mecanismo de control de acceso utilizará una protección física fuerte contra la lectura.

El mecanismo de control de acceso para la utilización del dispositivo UPT puede ser soportado por una verificación del titular del dispositivo.

10.2 Mecanismos de autenticación del usuario

10.2.1 Grados de autenticación

El grado de autenticación (fuerte o débil) depende del método de autenticación empleado. El grado de autenticación utilizado debe ser suficiente para reducir los riesgos de seguridad anticipados.

Por lo general, la autenticación debe también ser suficientemente fuerte para garantizar un nivel de seguridad conveniente cuando los servicios UPT son accedidos a través de redes soporte de UPT visitadas por usuarios UPT. El procedimiento de autenticación que ha de adoptarse puede ser negociado entre el proveedor del servicio UPT y las redes visitadas. Los usuarios UPT y los proveedores del servicio UPT tienen la posibilidad de sustentar varios mecanismos de autenticación para satisfacer el grado requerido de autenticación.

La autenticación UPT puede clasificarse en varios tipos, que comprenden los siguientes:

Unidireccional con un PIN fijo

En este caso, el procedimiento de autenticación se completa cuando el usuario UPT envía el PIN correcto.

Unidireccional con códigos de autenticación variables

En este caso, el procedimiento de autenticación utiliza también la transmisión unidireccional, pero con un código de autenticación variable.

Bidireccional con códigos de autenticación variables

En este caso, el procedimiento de autenticación emplea la transmisión bidireccional en un modo de "puesta a prueba-respuesta".

10.2.2 Tipos de dispositivo UPT

Si la autenticación de la identidad del usuario UPT se realiza mediante un dispositivo UPT, el nivel de protección depende del modo en que el dispositivo está realizado. Puede haber dispositivos UPT de diferentes realizaciones dependiendo de las redes, terminales y servicios utilizados, los cuales imponen diferentes restricciones en los mecanismos de seguridad que pueden proporcionarse en un modo sencillo y cómodo para el usuario. Por este motivo, puede ser necesario disponer de diferentes procedimientos de autenticación para las diferentes realizaciones de los dispositivos UPT. Las realizaciones pueden ser:

Ningún dispositivo UPT

En este caso, puede ser necesario introducir manualmente la PUI para identificación, y puede haber necesidad también de limitar el procedimiento de autenticación al uso de un código PIN solamente.

Dispositivo UPT de tarjeta magnética de identificación

Este tipo de dispositivo UPT requiere un terminal equipado con un lector de tarjeta magnética de identificación y una interfaz de señalización para comunicar con la red.

Dispositivo UPT unidireccional del tipo tonos (por ejemplo, DTMF)

Este dispositivo puede, bien simular sencillamente la secuencia de tonos que sería generada por el usuario UPT que utiliza un PIN para la autenticación, o bien contener la inteligencia para aportar procedimientos de autenticación análogos a los que se pueden conseguir con una tarjeta inteligente que utiliza una autenticación unidireccional (el dispositivo UPT transmite solamente datos). La inteligencia debe tener la capacidad de almacenar y generar información de sincronización. En caso de que se utilice clave de autenticación, debe disponer también de la capacidad de almacenar la clave de autenticación y de generar el código de autenticación.

Dispositivo UPT del tipo módem

Este dispositivo tendría funciones similares al dispositivo de tipo tonos, pero dispondría de la señalización acústica física dentro de banda de un módem normalizado. Idealmente, los procedimientos de autenticación deben, en este caso, ser los mismos que los de una tarjeta inteligente que utiliza autenticación unidireccional o bidireccional (es decir, el dispositivo UPT transmite y recibe datos). La inteligencia debe tener la capacidad de almacenar y generar información de

sincronización. En caso de que se utilice clave de autenticación, debe disponer también de la capacidad de almacenar la clave de autenticación y de generar el código de autenticación.

Dispositivo UPT del tipo tarjeta inteligente

Se pude utilizar un procedimiento de autenticación unidireccional o bidireccional. La autenticación del proveedor del servicio UPT puede combinarse con la autenticación de la identidad del abonado (autenticación mutua). Una tarjeta inteligente debe tener la capacidad de almacenar la clave de autenticación y de generar el código de autenticación.

10.2.3 Señalización de usuario

10.2.3.1 Acceso de usuario basado en DTMF (conforme con CS-1 de RI)

Limitación

Para el conjunto de servicios 1 de UPT, el servicio UPT será suministrado por las redes existentes. Debido a las limitaciones de esta red y de su terminal conectado, la autenticación solamente se puede realizar según unos modos determinados.

Las opciones de mecanismos de autenticación son limitadas; el intercambio de información se efectúa solamente en un sentido y la señalización se limita a los tonos DTMF.

La señalización unidireccional permite a los usuarios UPT autenticarse ellos mismo a la red. No permite a los usuarios UPT autenticar la red. Su uso restringe también los mecanismos disponibles para realizar la autenticación.

Selección del tipo de autenticación

Puede haber dos tipos de autenticación para el acceso de usuario basado en DTMF. Uno es la autenticación unidireccional con un PIN fijo. El otro es la autenticación bidireccional con códigos de autenticación variables. Si el usuario UPT necesita un procedimiento de autenticación fuerte, entonces el último tipo es mejor que el primero.

Clave de autenticación

Una clave de autenticación es una identidad expedida a un usuario para su uso en un proceso de autenticación. Esta clave toma normalmente la forma de un número de dígitos o de bits especificado.

Una clave de autenticación es normalmente un valor largo almacenado en soporte físico y utilizado como entrada a una función criptográfica.

Características de la autenticación unidireccional con un PIN

a) esta autenticación pertenece al tipo de autenticación débil;

b) el UPTN no se debe cambiar, incluso si el proveedor del servicio puede reconocer que su PIN ha sido descubierto por usuarios no autorizados. El empleo de la PUI sería una de las soluciones;

c) el dispositivo debe tener una PUI secreta para comodidad del;

d) usuario UPT envía su PIN al proveedor del servicio;

e) la pareja de PUI y PIN se compara con los mismos valores almacenados en el proveedor del servicio;

f) si no se corresponden, fallaría entonces el acceso;

g) se necesitaría un contador de tentativas de autenticación infructuosas para proteger su PIN contra la utilización fraudulenta;

h) la PUI sería bloqueada cuando el contador alcanzase el valor máximo;

i) como puede producirse el bloqueo malicioso de la PUI de alguna persona, se necesitaría disponer de un PIN para desbloquearla. Aun así, el usuario con la PUI bloqueada sufrirá un gran trastorno.

Características de la autenticación unidireccional con códigos de autenticación variables

a) esta autenticación pertenece al tipo de autenticación fuerte;

b) la PUI secreta no se precisa necesariamente porque es en extremo difícil revelar el algoritmo y la clave de autenticación de alguna entidad. El empleo de la PUI puede ser facultativo;

c) el dispositivo envía un código de autenticación variable e información de sincronización entre el dispositivo y la red (por ejemplo, indicación de tiempo, número de serie).

NOTA – son también posibles varios códigos de autenticación variables.

d) el dispositivo y el proveedor del servicio tienen una clave de usuario y un algoritmo;

e) el proveedor del servicio calcula el código de autenticación variable utilizando una clave de usuario, un algoritmo y la información de sincronización proporcionada por el usuario;

f) la autenticación puede ser válida para durante un periodo de tiempo determinado;

g) el código de autenticación variable calculado se compara con el enviado por el usuario;

h) si no son iguales, la autenticación fracasa;

i) no puede haber ningún contador para las tentativas fallidas y su valor máximo. Por consiguiente, el número de tentativas fracasadas no está limitado;

j) el UPTN no debe ser bloqueado, incluso si la clave y el algoritmo fueran revelados;

k) la clave del usuario debe cambiarse cuando su clave y algoritmo hayan sido revelados;

l) el dispositivo requeriría que el usuario UPT fuera autenticado a este dispositivo para evitar que usuarios no autorizadas hagan un uso fraudulento del mismo. Podría efectuarse mediante, por ejemplo, un PIN local. El modo en que el usuario UPT se autentique él mismo al dispositivo es un tema de implementación. El PIN local se encuentra disponible solamente para la interfaz usuario UPT- dispositivo. Considerando la facilidad de utilización por parte del usuario, la introducción del PIN en el dispositivo puede ser una función opcional;

m) el dispositivo utilizaría un protocolo normalizado para comunicar datos de autenticación y de instrucciones con el proveedor del servicio UPT local (por ejemplo, a través de un canal vocal).

Autenticación débil adicional para llamadas salientes después del registro de llamada salientes

a) esta autenticación se utiliza facultativamente para cada llamada en el caso en que el registro de llamadas salientes está activo, de manera adicional a la autenticación normal en el momento del registro;

b) en el momento del abono, se asignará a cada usuario un OCPIN especial. Si el usuario está autorizado para utilizar la autenticación débil, el valor del OCPIN deberá ser distinto del valor del PIN;

c) el usuario envía su OCPIN cada vez que desea establecer una llamada desde el terminal en el que está registrado. El OCPIN puede ser almacenado en el dispositivo para facilidad de utilización por el usuario.

d) el valor del OCPIN es comprobado por la red, y si su valor es correcto se autoriza al usuario a proseguir.

Autenticación débil adicional para "parte llamada especificó respuesta segura de llamadas UPT entrantes"

a) esta autenticación se utiliza para "parte llamada especificó respuesta segura de llamadas entrantes" en caso de acceso DTMF si el usuario no está autorizado a utilizar su dispositivo UPT. El proveedor del servicio puede facultativamente dar al usuario la posibilidad de utilizar solamente la autenticación fuerte, o la autenticación fuerte junto con esta característica;

b) en el momento del abono, cada usuario puede obtener un SAPIN. Si el usuario está autorizado a emplear la autenticación débil, el valor del SAPIN deberá ser distinto del valor del PIN;

c) se pide al usuario que se autentique él mismo cada vez que recibe una llamada en el terminal en el que está registrado;

d) el usuario envía su SAPIN. El SAPIN puede almacenarse en el dispositivo para facilidad de utilización por el usuario;

e) la red comprueba el valor del SAPIN, y si es el valor correcto se completa la llamada.

10.2.3.2 Acceso de usuario basado en DSS1 fuera de banda

Limitación

En el servicio UPT basado en CS-2 de RI o posteriores, estará disponible el empleo del acceso de usuario fuera de banda, tal como la señalización basada en DSS1. Por consiguiente, la limitación concerniente a redes y terminales disminuiría. Por lo que se refiere al acceso de usuario basado en DSS1 fuera de banda, se pueden utilizar varios tipos de autenticación, como la autenticación unidireccional, la autenticación bidireccional en un modo "puesta a prueba-respuesta", la autenticación mutua, etc. Y se pueden implementar varios tipos de dispositivo UPT descritos en 10.2.2. Bajo tales circunstancias, debe aplicarse la autenticación fuerte que utiliza un dispositivo inteligente.

Selección del tipo de autenticación

La RDSI tiene la capacidad de ofrecer una señalización bidireccional fácil que brinda la oportunidad de utilizar mecanismos de autenticación bidireccional. Permite también la autenticación mutua, esto es, la capacidad de que los usuarios se autentiquen ellos mismos hacia el proveedor del servicio UPT y de que el proveedor del servicio UPT autentique a los usuarios.

Clave de autenticación

Una clave de autenticación es una identidad expedida a un usuario para su uso en un proceso de autenticación. Esta clave toma normalmente la forma de un número de dígitos o de bits especificado.

Una clave de autenticación es normalmente un valor largo y utilizado como entrada a una función criptográfica.

Características para la autenticación del tipo "puesta a prueba-respuesta"

a) esta autenticación pertenece a un tipo de autenticación fuerte

b) el proveedor del servicio envía un número aleatorio al dispositivo;

c) el dispositivo utiliza una clave de autenticación y el número aleatorio, y calcula el código de autenticación variable. Envía a continuación este código al proveedor del servicio;

d) el dispositivo y el proveedor del servicio tienen una clave de usuario y un algoritmo;

e) el proveedor del servicio calcula el código de autenticación variable mediante la clave de usuario y el algoritmo;

f) se compara el código de autenticación variable calculado con el enviado por el usuario;

g) si no son iguales, la autenticación falla;

h) puede no haber contador para las tentativas fallidas y su valor máximo;

i) el UPTN no se cambia, incluso si la clave es revelada. Se proporcionaría otra clave y otro algoritmo al usuario;

j) la autenticación del tipo "puesta a prueba-respuesta" debe utilizar un dispositivo con función inteligente;

k) el dispositivo requeriría que el usuario UPT fuera autenticado al dispositivo para evitar que usuarios no autorizadas hagan un uso fraudulento de éste. Podría efectuarse mediante, por ejemplo, un PIN local. El modo en que el usuario UPT se autentique él mismo al dispositivo es un tema de implementación. El PIN local se encuentra disponible solamente para la interfaz usuario UPT -dispositivo. Considerando la facilidad de utilización por parte del usuario, la introducción del PIN en el dispositivo puede ser una función opcional;

l) el dispositivo utilizaría un protocolo del modo "puesta a prueba-respuesta" normalizado vía señalización de canal D de RDSI.

10.3 Mecanismos de gestión de seguridad

Para detectar lo más pronto posibles las amenazas contra algunas partes comprometidas con el sistema UPT y adoptar las medidas adecuadas, el análisis retrospectivo de la seguridad y el tratamiento de eventos deberán soportar los mecanismos de seguridad mencionados anteriormente. El control de la tarificación es un medio de limitar los daños potenciales a un nivel aceptable. La gestión de la información proporciona al usuario la posibilidad de tener conocimiento de los eventos de seguridad pertinentes.

10.3.1 Análisis retrospectivo de la seguridad

El cometido del análisis retrospectivo de la seguridad (pista de auditoria) es detectar las amenazas reales contra el sistema UPT como, por ejemplo, el acceso no autorizado al sistema o a datos del usuario y el cambio no autorizado de los derechos de acceso.

El sistema puede contener componentes de auditoria que son capaces de registrar cronológicamente los siguientes eventos con los siguientes datos:

a) utilización del mecanismo de identificación y autenticación (fecha, hora, identidad del usuario, identidad de la línea llamante, identidad del distintivo de zona, número marcado, éxito o fracaso de la tentativa, número de actualizaciones de sincronización);

b) tentativa de acceso al perfil de servicio (fecha, hora, identidad del usuario, nombre del objeto, tipo de tentativa de acceso, éxito o fracaso de la tentativa);

c) acciones de los proveedores del servicio UPT y de los operadores de red (fecha, hora, identidad del usuario, tipo de acción, nombre del objeto al que se refiere la acción; ejemplos: la introducción, supresión o suspensión de usuarios, la introducción o supresión de medios de almacenamiento, el arranque o caída del sistema).

Los mecanismos para obtener, mantener y evaluar una pista de auditoria (análisis retrospectivo de la seguridad) caen fuera del ámbito de esta Recomendación. Ellos son específicos del sistema y pueden ser soportados por mecanismos de seguridad de la red de gestión de telecomunicaciones (RGT).

10.3.2 Acciones de tratamiento de eventos

De acuerdo con los resultados de la evaluación de datos de auditoria (en línea o fuera de línea), deberán emprenderse las acciones adecuadas para poner en vigor la política de seguridad. Estas acciones pueden ser:

a) alarma al administrador de seguridad;

b) bloqueo del acceso de usuario al sistema;

c) interrupción de las llamas (por ejemplo, en especial las llamadas internacionales excesivamente largas).

Los mecanismos de tratamiento de eventos caen fuera del ámbito de la presente Recomendación. Ellos son específicos del sistema y pueden ser soportados por mecanismos de seguridad RGT.

10.3.3 Control de la tarificación

La administración de la tarificación ha de considerar la seguridad muy cuidadosamente. Los datos personales y los datos de facturación deberán almacenarse, procesarse y transmitirse de modo que la privacidad del usuario y la integridad de los datos queden garantizadas.

El análisis de peligros ha señalado que muchos problemas y amenazas se refieren a la tarificación y la facturación. La autenticación, complementada por los mecanismos de control de acceso y los procedimientos de gestión, evita estos peligros o al menos disminuye la posibilidad de que ocurran. Sin embargo, sobre todo a efectos de aceptabilidad, puede ser necesario proteger a los usuarios contra facturas o cantidades inesperadas. Las limitaciones de la factura se recomiendan especialmente cuando se utiliza la autenticación débil.

10.3.4 Gestión de la información

Debe disponerse de una facilidad para informar a los usuarios UPT, los abonados UPT y a terceros acerca de las acciones que afectan a su privacidad y seguridad o a la tarificación. En la mayor medida posible, esta información debe ser dada en línea mediante avisos (vocales o de presentación visual) o mediante tonos de marcación especiales. Corresponde al proveedor del servicio especificar la información que ha de darse a las partes involucradas. El contenido de la información cae fuera del alcance de esta Recomendación.

Los proveedores del servicio UPT deberán tener cuidado de no dar mucha información. Los posibles intrusos no deben tener la posibilidad de hacer un uso indebido de tal información para sus ataques. Además, la información y los avisos se han de seleccionar cuidadosamente para que no afecte a la privacidad de los usuarios UPT y de terceros.

El usuario UPT deberá ser informado sobre los riesgos de las características UPT y los servicios suplementarios, así como de los medios para hacer estos riesgos mínimos.

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

Ginebra, 2001