Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1171

(02/2009)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad – Seguridad de la identidad en las redes

Amenazas y requisitos para la protección de la información que permite identificar a una persona en las aplicaciones que utilizan la identificación basada en marcadores

Recomendación UIT-T X.1171

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	**X.1170–X.1179**
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

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

Recomendación UIT-T X.1171

Amenazas y requisitos para la protección de la información que permite identificar a una persona en las aplicaciones que utilizan la identificación basada en marcadores

Resumen

La implantación generalizada de marcadores de identificación (incluidos los marcadores de identificación por radiofrecuencias (RFID) puede causar inquietud ante posibles vulneraciones de la intimidad aprovechando las posibilidades que ofrece la tecnología RFID para recopilar (y procesar) datos de manera automática, con la posibilidad de revelar dichos datos al público (de manera deliberada o accidental).

En el caso de las aplicaciones que recurren a la identificación por medio de marcadores y se basan en un marcador de identificación personalizado para las aplicaciones de gestión personalizadas después de su venta, las aplicaciones de atención de la salud, etc., la cuestión de la protección de la intimidad se está convirtiendo en un problema cada vez más grave. En esta Recomendación se describen diversas infracciones de la información que permite identificar a la persona (IIP) a partir de aplicaciones que recurren a la identificación por medio de marcadores, así como los requisitos para proteger la IIP. Además, en esta Recomendación se facilita una estructura básica de protección de la IIP a partir de las características de la política de IIP.

Orígenes

La Recomendación UIT-T X.1171 fue aprobada el 20 de febrero de 2009 por la Comisión de Estudio 17 (2009-2012) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

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 X.1171[1]

Amenazas y requisitos para la protección de la información que permite identificar a una persona en las aplicaciones que utilizan la identificación basada en marcadores

1 Alcance

Esta Recomendación abarca los siguientes objetivos, así como amenazas y requisitos, en lo que respecta a la protección de la información que permite identificar a una persona (PII) en las aplicaciones que utilizan la identificación basada en marcadores:

– para describir las amenazas contra la PII en entornos empresa-cliente de aplicaciones que utilizan identificación basada en marcadores;

– para identificar los requisitos de protección de la PII en un entorno empresa-cliente de aplicaciones que utilizan identificación basada en marcadores.

Los siguientes objetivos quedan al margen de la presente Recomendación:

– analizar las amenazas generales que pesan sobre la seguridad y los requisitos de las aplicaciones que utilizan identificación basada en marcadores;

– analizar las amenazas y requisitos relacionados con la PII que sobrevienen entre un marcador de identificación (ID) y un terminal ID;

– analizar las amenazas y requisitos relacionados con la PII que dependen de la marcación ID y del método de lectura que se consideren, por ejemplo, marcador de identificación por radiofrecuencia (RFID) y terminal ID;

– definir y diseñar los formatos de mensajes y el mecanismo de protección PII, basándose en el perfil de política PII de usuario de una aplicación que utilice identificación basada en marcadores.

NOTA 1– Habrá que trabajar más para definir dichos formatos, que pueden no quedar restringidos únicamente a la protección PII en el marco de la identificación basada en marcadores, y que requieren acaso un enfoque más general (privacidad).

En la presente Recomendación, el usuario de un marcador ID cuenta con la capacidad de controlar el propio marcador ID, por lo cual se supone que dicho usuario es responsable del comportamiento de dicho ID.

NOTA 2 – En ciertos casos, el usuario del marcador ID carece de toda capacidad de control del marcador, lo que ocurre, por ejemplo, cuando un particular adquiere un producto marcado y el fabricante exige que el marcador ID permanezca activo con propósitos de garantía. En este caso, cabe la posibilidad de que el usuario del marcador ID sólo sea un particular que transporta y utiliza el producto marcado. De ahí, que la presente Recomendación no pueda aplicarse para resolver ese problema en el caso mencionado. Este escenario plantea problemas de legislación y política (véase [b-OECD]), por lo cual el tema puede ser abordado en otra Recomendación.

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

---

[1] Puede ocurrir que la presente Recomendación no resulte aplicable en Alemania debido a la legislación del país.

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 una Recomendación.

[UIT-T X.1121] Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

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

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

3.1.2 servidor de aplicación [UIT-T X.1121]: Entidad que se conecta a una red abierta para la comunicación de datos con terminales móviles.

3.1.3 proveedor de servicio de aplicación (ASP) [UIT-T X.1121]: Entidad (persona o grupo) que suministra servicios de aplicación a usuarios móviles a través de un servidor de aplicación.

3.1.4 autenticación [b-UIT-T X.811]: Confirmación de la identidad declarada de una entidad.

NOTA – El término "identidad" se utiliza aquí, en la inteligencia de que en el contexto de telecomunicaciones se trata de un identificador o conjunto de identificadores digno de confianza, lo que quiere decir que se considera fiable en una determinada situación para representar a un elemento de red, equipo de terminal de red o usuario, una vez terminado el correspondiente proceso de validación. Tal como el término se utiliza en esta Recomendación, no se puede concluir que los identificadores dignos de confianza representen la validación positiva de una persona.

3.1.5 identificador [b-UIT-T F.771]: Serie de cifras, caracteres y símbolos o cualquier otra forma de datos, utilizados para identificar una entidad real. Un identificador se utiliza para representar una relación entre la entidad real y su información/atributos en computador. Esta relación no permite que los usuarios accedan a través de sus terminales ID a la información/atributos de la entidad almacenados en computador.

3.1.6 marcador ID [b-UIT-T F.771]: Pequeño objeto físico que almacena una reducida cantidad de información, cantidad que constituye un identificador o incluye un identificador con otros datos de aplicación adicionales, tales como nombre, título, precio y dirección.

3.1.7 terminal ID [b-UIT-T F.771]: Dispositivo que cuenta con una capacidad de captura de datos de marcadores ID y con otra capacidad, por ejemplo de comunicación o de presentación de información multimedios. La capacidad de captura de datos puede incluir una función que permita obtener el identificador a partir de identificadores ID, incluso sin capacidad de comunicación, por ejemplo, códigos de barra y códigos de barra 2D. Entre los equipos que utilizan técnicas de captura de datos cabe citar las que consisten en la utilización de cámaras digitales, dispositivos de barrido óptico, transpondedores RF, IrDA, línea alámbrica galvanizada, etc.

3.1.8 red móvil [UIT-T X.1121]: Red que proporciona puntos de acceso de red inalámbrica a terminales móviles.

3.1.9 terminal móvil [UIT-T X.1121]: Entidad que cuenta con una función de acceso a una red inalámbrica y conecta a una red móvil de comunicación de datos con servidores de aplicaciones u otros terminales móviles.

3.1.10 usuario móvil [UIT-T X.1121]: Entidad (persona) que utiliza y explota un terminal móvil para recibir diferentes servicios de proveedores de servicios de aplicaciones.

3.1.11 información de identificación personal (PII) [b-UIT-T Y.2720]: Información perteneciente a una persona física, que posibilita su identificación (incluida la información que puede identificar a una persona cuando se combina con otra información, incluso si tal información no identifica claramente a la persona).

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 aplicaciones que utilizan identificación basada en marcadores: Aplicaciones que entrañan al menos los siguientes elementos: identificador, terminal ID, marcador ID y una o varias redes. En esta aplicación, el identificador se almacena en un marcador ID y la información asociada con el identificador se proporciona en el lado de la red.

NOTA – El identificador se almacena en un marcador ID (o dentro de un marcador ID, dependiendo del tipo de marcador ID que se considere) y un terminal ID lee o escribe el identificador a partir de/al marcador ID mediante un dispositivo de barrido óptico (únicamente lectura) o una cámara (únicamente lectura) o asociación de datos en infrarrojo (lectura/escritura), una técnica de radiofrecuencia (lectura/escritura) u otros métodos similares.

3.2.2 empresa-consumidor (B2C): Una relación de negocios entre empresas y consumidores, en virtud de la cual los proveedores de servicio proporcionan servicios valiosos y útiles a los consumidores y los consumidores los utilizan.

3.2.3 perfil de política PII por defecto: Un conjunto formateado de reglas y políticas de protección PII de una aplicación que utiliza identificación basada en marcadores.

3.2.4 identificación (ID): Procedimiento que sirve para identificar específicamente un objeto en una clase de objetos de gran magnitud mediante la lectura de identificadores de marcadores ID.

3.2.5 usuario de marcador ID: Persona que adquiere y transporta o utiliza un objeto habilitado mediante un marcador ID.

3.2.6 usuario de terminal ID: Persona que utiliza y explota un terminal ID. Un ejemplo típico de este tipo de usuario podría ser un usuario móvil provisto de un terminal ID.

3.2.7 marcador ID personalizado: Marcador ID que contiene un identificador que habilita la posible identificación de una persona, en lugar de un objeto anónimo.

3.2.8 servicio de protección PII (PPS): Servicio de seguridad que proporciona protección PII para usuarios de marcadores ID y/o terminales ID de aplicaciones que utilizan identificación basada en marcadores. El PPS gestiona (esto es, crea/actualiza/suprime/aplica) (marcador ID y/o terminal ID) un perfil de política PII de usuario en una red en la cual se encuentra funcionando una aplicación que utiliza identificación basada en marcadores.

3.2.9 perfil de política PII: Conjunto formateado de reglas y políticas de protección PII.

3.2.10 perfil de política PII definido por el usuario: Conjunto formateado de reglas y políticas de protección PII definido por el usuario (marcador ID y/o marcador ID).

4 Abreviaturas y acrónimos

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

ASP Proveedor de servicio de aplicación (*application service provider*)

B2C Business-to-Customer

ID Identificación (*identification*)

IrDA Asociación de datos en infrarrojo (*infrared data association*)

OCDE Organización de Cooperación y Desarrollo Económico (*Organization for Economic Cooperation and Development*)

PII Información de identificación personal (*personally identifiable information*)

PPS Servicio de protección de la PII (*PII protection service*)

RF Radiofrecuencia (*radio frequency*)

RFID Identificación mediante radiofrecuencias (*radio frequency identification*)

SCM Gestión de cadena de suministro (*supply chain management*)

5 Convenciones

Ninguna.

6 Panorama

El despliegue generalizado de marcadores de identificación (incluidos los marcadores RFID) puede ser objeto de preocupación, dada la capacidad de la tecnología RFID para recoger (y procesar) automáticamente datos y a la vista de la posibilidad de difusión pública de dichos datos (de manera deliberada o accidental).

Tratándose de aplicaciones que utilizan identificación basada en marcadores y que dependen de un marcador de identificación personalizado en el marco de los servicios de gestión postventa personalizados, los servicios relacionados con la atención de salud, etc., la cuestión que supone la privacidad se está convirtiendo en un problema cada vez más grave.

En el mundo académico y la industria la mayoría de los esfuerzos desplegados para establecer mecanismos de protección PII se han centrado en protocolos de autenticación entre el marcador ID y el terminal ID. Hay que señalar, sin embargo, que los resultados de estos esfuerzos no pueden llevarse a la práctica en un entorno real, especialmente cuando se trata de aplicaciones que utilizan identificación basada en marcadores, entorno en el que la información significativa del identificador se encuentra en el servidor situado dentro del dominio de la red. Por consiguiente, resulta esencial establecer el mecanismo de protección PII idóneo en el entorno de aplicaciones que utilizan identificación basada en marcadores. Es posible que un mecanismo de protección PII basado en perfiles sólo constituya una de las muchas posibles soluciones para dicho entorno.

En la presente Recomendación se describe la violación de la PII en el entorno de aplicaciones que utilizan identificación basada en marcadores, los requisitos de protección PII y la estructura básica de la protección PII basada en el perfil de política PII definido por el usuario.

7 Aplicaciones de empresa-consumidor que utilizan identificación basada en marcadores

A los propósitos de esta cláusula, una aplicación que utiliza identificación basada en marcadores es una aplicación de identificación ampliada y más general que se utiliza para comunicar con una serie de redes, interredes y sistemas de aplicación distribuida globalmente. Dicho de otro modo, se trata de una aplicación global basada en redes que es activada por un marcador ID (incluida la RFID).

Las aplicaciones que utilizan identificación basada en marcadores se han adoptado ya en grado considerable en sectores tales como la gestión de la cadena de suministro (SCM) y la gestión de almacén de diferentes industrias, así como para tomar medidas contra la falsificación en la cadena de suministro de medicamentos. Las aplicaciones que utilizan identificación basada en marcadores se han extendido actualmente para cubrir el campo de aplicaciones del usuario de extremo (por ejemplo, entrega del contenido de la información sobre productos activada por un marcador ID,

gestión postventa del objeto físico de que se trate, estadísticas de pacientes, control de tarifas, etc.), y aplicaciones industriales.

Las aplicaciones de empresa-consumidor que utilizan identificación basada en marcadores pueden ser de tres tipos:

a) Cuando el usuario de un terminal ID se considera el cliente: por ejemplo, tratándose del servicio de entrega del contenido de la información, el cliente recupera la información utilizando su terminal ID. En este tipo de servicio la mayoría de los proveedores de servicio que suministran la aplicación considerada pueden partir del supuesto de que el terminal ID posee una capacidad de telecomunicación móvil y una capacidad de presentación de la información multimedios. En la figura 1 puede verse un modelo básico de este tipo de aplicaciones, que utilizan identificación basada en marcadores. El modelo consiste en dos operaciones de red básicas, a saber: la resolución ID y recuperación de contenidos. La resolución ID es el procedimiento consistente en traducir o convertir un identificador en una dirección [b-UIT-T Y.2213]. El terminal móvil equipado con un terminal ID transforma, en primer lugar, un identificador recibido del marcador ID a través del servicio de directorio y acto seguido realiza una recuperación del contenido.

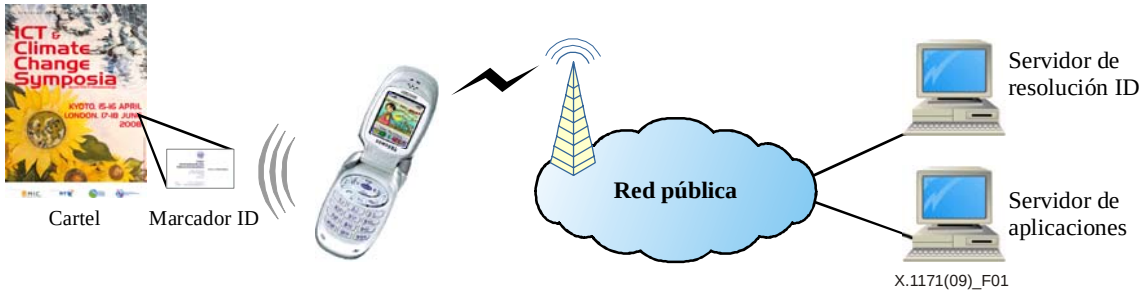

Figura 1 – Modelo básico de una aplicación de empresa-consumidor que utiliza identificación basada en marcadores

b) Cuando el usuario provisto de un marcador ID se considera el cliente: Un ejemplo típico de esta aplicación de empresa-consumidor que utiliza identificación basada en marcadores tiene que ver con el control y/o autenticación del acceso; así por ejemplo, control de entrada, pasaporte, licencia y servicio de gestión postventa. En esta clase de modelo de aplicación los terminales ID son del tipo terminal fijo y/o terminal móvil, y puede suceder que el cliente no necesite contar con su propio terminal ID.

c) Cuando el cliente es tanto el usuario de un marcador ID como el usuario de un terminal ID: En el servicio de recuperación de información sobre productos (tipo básico de aplicación empresa-consumidor que utiliza identificación basada en marcadores) el cliente se convierte, asimismo, en un usuario de marcador tras adquirir el producto marcado después de haber explorado el contenido de la información sobre el producto utilizando su terminal móvil. En este contexto, cabe considerar también el caso de un servicio de atención de salud activado por la tarjeta de un paciente que es habilitada por un marcador ID. En el marco de esta aplicación actúa un gran número de clientes: el paciente, el médico, la enfermera, etc., en calidad de usuarios de marcador ID. El usuario de marcador ID puede consultar sus propios datos de paciente leyendo su tarjeta de paciente habilitada por un marcador ID a través del terminal móvil dotado de un terminal ID.

Dado que muchas aplicaciones que utilizan identificación basada en marcadores se amplían para convertirlas en aplicaciones de empresa-consumidor, preocupa en grado considerable a los consumidores que la utilización de marcadores ID genera fugas en su PII. En la presente Recomendación nos centramos esencialmente en el modelo de aplicaciones empresa-consumidor que utilizan identificación basada en marcadores.

8 Modelo de referencia para aplicaciones empresa-consumidor que utilizan identificación basada en marcadores

En la figura 2 puede verse un modelo de referencia de este tipo de aplicación que utiliza identificación basada en marcadores.

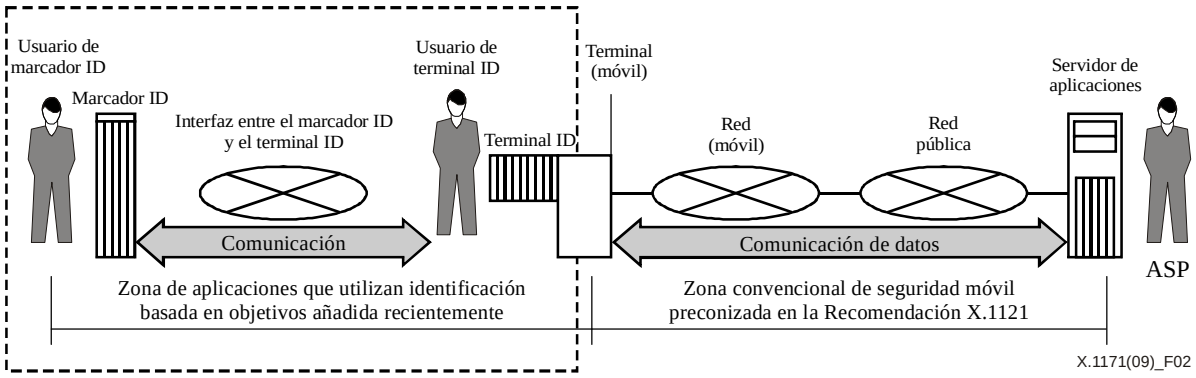

Figura 2 – Modelo de referencia de aplicaciones empresa-consumidor que utilizan identificación basada en marcadores

El modelo de referencia es un modelo ampliado de la comunicación móvil de datos de extremo a extremo descrita en [UIT-T X.1121]. Entre las entidades que se han añadido recientemente, cabe citar el marcador ID, el usuario de marcador ID, la interfaz entre el marcador ID y el terminal ID, y el terminal ID. En el modelo precitado el terminal (móvil) puede consistir en un terminal inalámbrico estacionario, así como en un terminal inalámbrico móvil, y considerarse como un terminal ID.

9 Violación de la PII en aplicaciones empresa-consumidor que utilizan identificación basada en marcadores

En el entorno de las aplicaciones que utilizan identificación basada en marcadores las principales violaciones de la PII tienen lugar cuando la titularidad de un producto o un documento provisto de un marcador ID se transfiere a un particular.

En el entorno de las aplicaciones que utilizan identificación basada en marcadores existen varios métodos de identificación con almacenamiento/lectura; por ejemplo, la utilización de códigos de barras (bidimensionales) y dispositivos de lectura óptica (o cámaras), marcadores y lectores pasivos RFID de campo próximo y marcadores y lectores pasivos RFID de campo distante. En la presente cláusula se describen únicamente las fugas genéricas PII en un entorno de aplicaciones empresa-consumidor que utilizan identificación basada en marcadores. Desde un punto de vista más concreto, hay que señalar que la presente Recomendación no abarca las siguientes amenazas:

– Amenazas generales contra la seguridad en las aplicaciones que utilizan identificación basada en marcadores: esta cláusula se centra únicamente en amenazas relacionadas con la PII en las aplicaciones que utilizan identificación basada en marcadores.

– Amenazas que afectan específicamente a los diferentes métodos de identificación con almacenamiento/lectura: así, por ejemplo, tratándose de un marcador RFID, un atacante puede localizar la ubicación del usuario del producto marcado para su identificación por radiofrecuencia recurriendo al identificador del marcador RFID. En el apéndice I se explica detalladamente dicha localización en el entorno RFID.

– Amenazas registradas entre un marcador ID y un marcador ID: Esta cláusula se centra únicamente en las amenazas contra la PII que se producen en el lado de red.

9.1 Fugas de información asociadas con el identificador

Un atacante puede leer la información contenida en un marcador ID sin el conocimiento del usuario del marcador ID del producto marcado. En primer lugar, el atacante lee un identificador a partir del marcador ID transportado por el usuario. Posteriormente, el atacante resuelve el identificador y busca el lugar donde se encuentra la información interrogando al servicio de directorio. Por último, el atacante solicita la información asociada con el marcador ID. Además, si la información guarda relación con la PII: información sobre tarjetas de crédito, historiales médicos, etc., la violación de la PII contenida en el marcador ID del usuario puede ser más grave. En la figura 3 se indica la violación de la PII que se comete aprovechando fugas de información. En este caso, el atacante puede recoger cierta información dinámica (hora y lugar en que se registró la adquisición del producto marcado, seguimiento de la información del producto, etc.), así como información estática: nombre y descripción del producto, etc.

Cabe la posibilidad de impedir este tipo de violación de la PII, eliminando el marcador ID o desactivando su funcionalidad. Ahora bien, resulta esencial preservar el marcador ID o su funcionalidad en muchas aplicaciones que utilizan identificación basada en marcadores, tales como el servicio de gestión postventa personalizado y el servicio relacionado con la atención de salud.

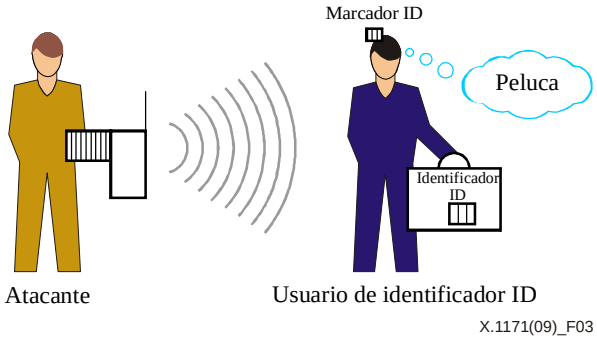

Figura 3 – Violación PII mediante fugas de información

9.2 Fuga de datos de antecedentes

El atacante puede extraer datos significativos del usuario tales como los relacionados con sus preferencias, hábitos, esferas de interés, etc. de los datos de antecedentes asociados con el marcador ID. Además, el atacante puede utilizar dichos datos con propósitos ilegales o comerciales sin consentimiento del usuario. En estos casos de violación, por el usuario se entiende el usuario del terminal ID. El usuario del terminal ID lee el identificador de los productos o documentos marcados utilizando su terminal ID y obtiene información del servidor de aplicaciones en aplicaciones que utilizan identificación basada en marcadores. En ese momento, los diferentes datos contextuales del fichero de registro cronológico (fecha de alquiler de una película DVD, fecha y lugar de la compra de dicho objeto, el lugar donde se leyó el cartel de la película, etc.) pueden ser recogidos por la red de aplicaciones que utilizan identificación basada en marcadores. Hay que señalar que estos datos pueden vincularse con el usuario (véase la figura 4).

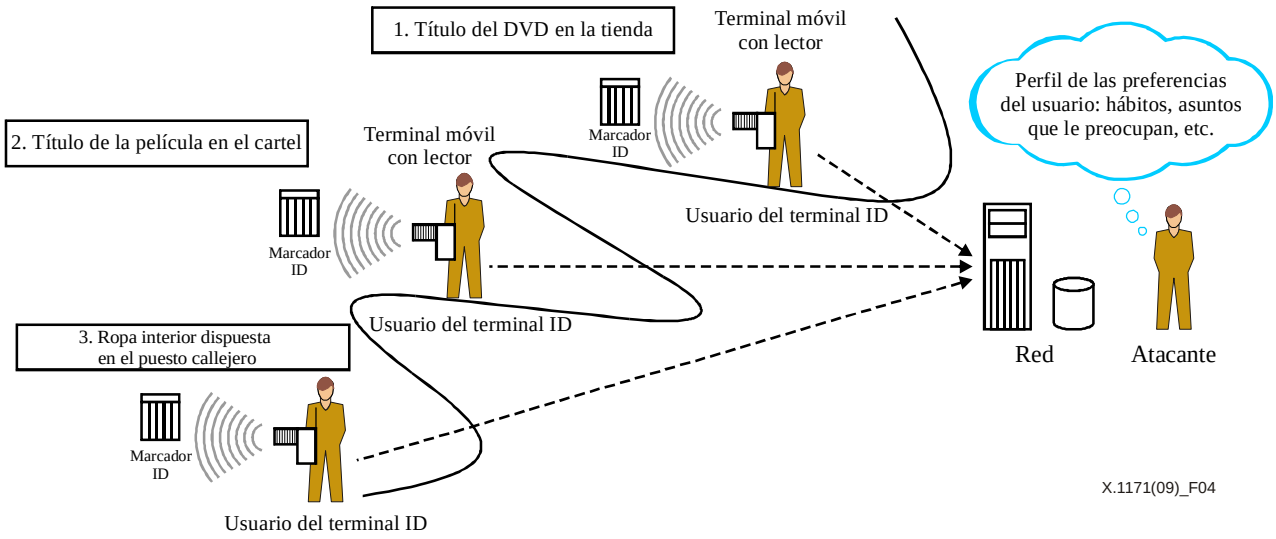

Figura 4 – Violación de la PII mediante el acopio de datos cronológicos

9.3 Relación entre las violaciones de la PII y el modelo de referencia

En el cuadro 1 se resumen las relaciones existentes entre las violaciones PII y las entidades descritas en el modelo indicado en la figura 2. En el cuadro las células marcadas con una "X" significan que una violación PII en la fila que se considera guardan relación con una entidad o relación entre entidades consignadas en la correspondiente columna.

Cuadro 1 – Relaciones entre violaciones PII y el modelo de referencia

Entidades y relaciones entre las entidades	**Violaciones**	
	Fuga de la información proporcionada por la aplicación o aplicaciones que utilizan identificación basada en objetivos	**Fuga de los datos cronológicos almacenados en el servidor o servidores de aplicación**
Relación entre el marcador ID y el usuario del terminal ID		X
Relación entre el terminal (móvil) y el servidor de aplicaciones	X	X
Relación entre el usuario del marcador ID y el servidor de aplicaciones	X	
Relación entre el marcador ID y el servidor de aplicaciones	X	
Servidor de aplicaciones	X	X

10 Requisitos de protección PII para aplicaciones empresa-consumidor que utilizan identificación basada en marcadores

Esta cláusula se centra básicamente en los requisitos técnicos relacionados con dos violaciones PII analizadas en la cláusula 9. En otras Recomendaciones se examinan directrices de carácter más general destinadas a los usuarios y vendedores de dispositivos RFID en lo que concierne a la protección PII en el contexto de la tecnología RFID. Los requisitos se basan parcialmente en los principios asentados en las directrices sobre privacidad de la OCDE [b-OCDE]. En el anexo A se

describen los principios de [b-OCDE] considerados en esta cláusula, y en el anexo B los demás principios de [b-OCDE]. Los siguientes requisitos se han extraído a partir de violaciones PII en aplicaciones empresa-consumidor que utilizan identificación basada en objetivos:

– control de la PII por parte del usuario del marcador ID y/o del usuario del terminal ID;
– autenticación del usuario del marcador ID y/o del usuario del terminal ID;
– control de acceso a la PII de un usuario de marcador ID en un servidor de aplicaciones;
– confidencialidad de la información asociada con un marcador ID;
– consentimiento en cuanto al acopio de PII;
– salvaguardias técnicas para los servidores de aplicación.

10.1 Control de la PII por parte del usuario del marcador ID y/o del usuario del terminal D

Es preciso que este usuario esté en condiciones de gestionar o actualizar la PII asociada con su marcador ID y/o terminal ID en la red. De este modo, el usuario del marcador ID puede determinar qué PII debe suprimirse o conservarse en la aplicación que utiliza identificación basada en marcadores. Además, el usuario puede determinar el límite de tiempo durante el cual se guardará su PII en la aplicación que utiliza identificación basada en marcadores.

10.2 Autenticación del usuario del marcador ID y/o del usuario del terminal ID

El servidor de una aplicación que utiliza identificación basada en marcadores debe proporcionar un procedimiento de autenticación para el usuario del marcador ID, y, en caso necesario, dicho servidor podría ofrecer un procedimiento de autenticación del usuario del terminal ID (tratándose de algunas aplicaciones que utilizan identificación basada en marcadores, no se exige que dichas aplicaciones autentifiquen al usuario).

10.3 Control de acceso a la PII del usuario del marcador ID en un servidor de aplicaciones

El acceso a la PII del usuario del marcador ID almacenada en un servidor de aplicación ha de ser seguro y estar limitado a los solicitantes de información autorizados, así como a la información pertinente que cada solicitante necesita.

10.4 Confidencialidad de la información asociada con un marcador ID

El servidor de una aplicación que utilice identificación basada en marcadores debe garantizar la confidencialidad de los datos para que los usuarios no autorizados no puedan leer la información relacionada con el marcador ID.

10.5 Consentimiento relativo al acopio de PII

El servidor de una aplicación que utilice identificación basada en marcadores debe proporcionar un procedimiento de consentimiento en lo que concierne a la recopilación de PII, incluidos los datos del fichero de registro cronológico que tienen que ver con el usuario del terminal ID. La aplicación que utiliza identificación basada en marcadores ofrece una solución técnica para que la PII sea exacta y esté tan actualizada como sea necesario para la identificación, además de limitarse a la información pertinente necesaria. Durante el proceso de consentimiento, la aplicación debe indicar el objetivo de la recopilación de PII. El usuario habrá de dar también su consentimiento si la PII previamente almacenada se va a utilizar para fines distintos de los inicialmente indicados.

10.6 Salvaguardias técnicas para los servidores de aplicación

La ASP de una aplicación que utiliza identificación basada en marcadores encargada de procesar la PII deberá adoptar medidas técnicas de seguridad para los servidores de aplicación, incluida la PII.

10.7 Relación entre los requisitos y las violaciones PII

En el cuadro 2 se indica resumidamente la relación existente entre los requisitos de protección PII y las violaciones PII. En el cuadro las células marcadas con una "X" indican que una infracción de la PII registrada en la correspondiente columna del cuadro guarda relación con el requisito de protección de la PII consignado en la fila correspondiente.

Cuadro 2 – Relación entre los requisitos y las violaciones PII

Requisitos	**Violaciones**	
	Fugas de información asociadas con el identificador	**Fugas de datos cronológicos**
Control de la PII por parte del usuario del marcador ID y/o del terminal ID	X	
Autenticación del usuario del marcador ID y/o del usuario del terminal ID	X	X
Control del acceso a la PII del usuario del marcador ID en un servidor de aplicaciones	X	
Confidencialidad de la información asociada al marcador ID	X	X
Consentimiento del acopio PII		X
Salvaguardias técnicas para los servidores de aplicación	X	X

Anexo A

Principios básicos de aplicación nacional[2]

(Este anexo forma parte integrante de la presente Recomendación)

- Principio de limitación de recogida: Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.
- Principio de calidad de los datos: Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.
- Principio de especificación del propósito: El propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.
- Principio de limitación de uso: No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el apartado anterior, excepto:
  - si se tiene el consentimiento del sujeto implicado; o
  - por imposición legal o de las autoridades.
- Principio de salvaguardia de la seguridad: Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.
- Principio de transparencia: Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.
- Principio de participación individual: Todo individuo tendrá derecho a:
  a) que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona;
  b) que se le comuniquen los datos relativos a su persona
     - en un tiempo razonable;
     - a un precio, si existiese, que no sea excesivo;
     - de forma razonable; y
     - de manera inteligible;
  c) que se le expliquen las razones por las que una petición suya según los subapartados a) y b) haya sido denegada, así como poder cuestionar tal denegación; y
  d) expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.
- Principio de responsabilidad: Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

---

[2] Estos principios se han extraído de la Parte II de las "Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales", OCDE, 1980.

Anexo B[3]

Principios básicos de aplicación internacional: restricciones en el libre flujo y la legitimidad

(Este anexo forma parte integrante de la presente Recomendación)

– Los Estados Miembros deberán considerar las implicaciones que el procesamiento nacional y la reexportación de datos personales puedan tener para otros países miembros.

– Los Estados Miembros deberán seguir todos los pasos razonables y apropiados para asegurar que el flujo transfronterizo de datos personales, incluido el tránsito a través de un país miembro, se realice de forma ininterrumpida y segura.

– Los Estados Miembros deberán abstenerse de restringir el intercambio transfronterizo de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial estas directrices o cuando la reexportación de tales datos burle la legislación nacional sobre privacidad. Un Estado Miembro también podrá imponer restricciones a ciertas categorías de datos personales sobre las que rijan normativas específicas, contenidas en su legislación nacional sobre privacidad, que por su naturaleza no tienen una protección equiparable en el país receptor.

– Los Estados Miembros deberán evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección.

---

[3] Estos principios se han extraído de la Parte III de las "Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales", OCDE, 1980.

Apéndice I

Localización por parte del identificador en los servicios RFID

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

El atacante puede localizar al usuario del marcador ID del producto marcado, recurriendo al identificador del marcador RFID. Este tipo de violación de la seguridad permite localizar o supervisar un determinado identificador de marcador utilizando un lector RFID invisible y malicioso. Como el atacante está en condiciones de utilizar el identificador del marcador como identificador personal, podría localizar fácilmente al usuario, tal como se indica en la figura I.1.

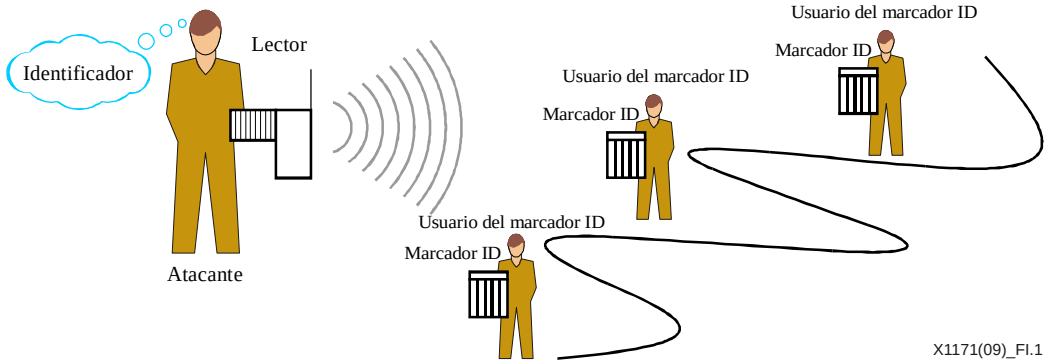

Figura I.1 – Amenaza contra la seguridad mediante la localización de una persona

Para proteger al identificador de la posibilidad de localización, cabe utilizar un método de autenticación entre el marcador RFID y el lector. El marcador RFID asigna al lector un identificador únicamente después de autenticar al lector. Dicho de otro modo, el atacante no puede obtener el identificador si no sigue el procedimiento de autenticación. Ahora bien, puede ocurrir que este método de autenticación no sea una solución realista, si el marcador RFID no posee la suficiente potencia de procesamiento para realizar operaciones complejas, tales como las que exige la computación criptográfica.

Otra solución podría venir representada por la técnica de recodificación del identificador, técnica que hace necesario recodificar periódicamente el identificador del marcador RFID con un seudoidentificador (o metaidentificador), lo que reduce la conectividad del identificador del marcador ID y del usuario del marcador ID. Hay que señalar, sin embargo, que este método de recodificación del identificador no resulta aplicable, cuando el marcador RFID no consta de una funcionalidad reescribible o si el marcador ID emplea un determinado formato de identificador (por ejemplo, el código EPC [b-EPCglobal]). Asimismo, la utilidad de esta técnica se circunscribe a los servicios que requieren una frecuente lectura del marcador RFID y puede introducir un elevado grado de complejidad en el lado del servidor.

Apéndice II

Servicio de protección PII (PPS) para aplicaciones que utilizan identificación basada en marcadores

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

II.1 Servicio de protección PII (PPS) para aplicaciones que utilizan identificación basada en marcadores

El PPS es un ejemplo de un servicio de protección PII basado en el perfil de política PII del usuario.

En la cláusula II.3 se describe un escenario general del PPS en el caso de una aplicación que utilice identificación basada en marcadores. Tratándose del PPS, el usuario del marcador ID o del terminal ID al que atiende una aplicación específica que utiliza identificación basada en marcadores establece sus políticas de protección PII para la aplicación de que se trate y comunica dichas políticas a un sistema fiable de un tercero (sistema PPS). A continuación, dicho sistema crea el perfil de política PII de usuario y lo envía a los servidores de aplicaciones (sistemas situados en el lado de servicio), momento en el cual los servidores de aplicaciones pueden controlar el acceso a la información PII asociada con el usuario del marcador ID y/o el usuario del terminal ID.

II.2 Entidades de servicio del PPS para aplicaciones que utilizan identificación basada en marcadores

El PPS consta de las siguientes tres entidades de servicio (véase la figura II.1):

– Sistema PPS: En tanto que entidad con la función de gestión para la política PII de usuario, dicho sistema crea el perfil de política PII definida por el usuario y destinado a la política PII de éste y proporciona el perfil de política PII al sistema o sistemas situados en el lado de servicio.

  NOTA – Cuando se trata de un sistema PPS centralizado que se encarga de un gran número de aplicaciones que utilizan identificación basada en marcadores, deberían proporcionarse las medidas apropiadas contra un único punto de fuga. Con todo y dependiendo en el caso en que se encuentre el usuario, podría haber únicamente un sistema PPS para una aplicación que utiliza identificación basada en marcadores.

– Sistema situado en el lado de servicio: Entidad que proporciona información relacionada con el identificador de un marcador ID, esto es, que puede considerarse como un servidor de aplicaciones en el contexto de una aplicación que utilice identificación basada en marcadores. Así pues, cabe la posibilidad de que existan muchos sistemas en el lado de servicio para una aplicación que utilice identificación basada en marcadores. Esta entidad proporciona una función de control de acceso que utiliza el perfil de política PII definida por el usuario o un perfil de política PII por defecto.

– Sistema en el lado de usuario: Entidad dotada de la función de acceso inalámbrico (o alámbrico) a la red, y de la función de captura de identificador, y que, si así se estima necesario, podría consistir en un terminal móvil dotado de un terminal ID. El usuario del marcador ID y/o el usuario del terminal ID pueden acceder al lado de servicio y a los sistemas PPS, recurriendo a dicho sistema en el lado del usuario. Utilizando un sistema de este tipo, el usuario controla su política de protección PII para una determinada aplicación que utilice identificación basada en marcadores.

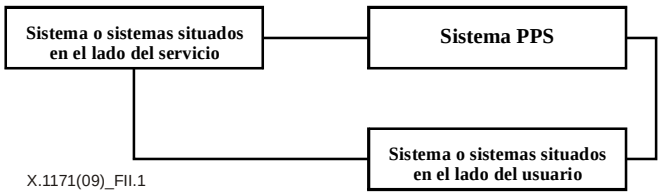

Figura II.1 – Entidades de servicio del PPS para aplicaciones que utilizan identificación basada en marcadores

II.3 Escenario general de servicio para el PPS

Este escenario se plantea por regla general cuando se trata de un procedimiento de personalización de marcadores, tal como la compra de productos marcados. La figura II.2 ilustra el flujo general PPS en una aplicación que utiliza identificación basada en marcadores.

Figura II.2 – Flujo general del PPS

0) Un consumidor lee el identificador del producto marcado utilizando su equipo terminal móvil dotado de un terminal ID.

1) El consumidor consume la información relacionada con el producto en la red del servicio de aplicación y ulteriormente adquiere el producto utilizando uno o más métodos de pago, momento en el cual, el consumidor se convierte en un usuario de marcador ID.

2) Acto seguido, la aplicación que utiliza identificación basada en marcadores solicita un perfil de política PII definido por el usuario al sistema PPS, que responde a la aplicación con el perfil PII definido por el usuario.

3) El sistema PPS recibe la política de protección PII del usuario para esta aplicación

4) Cualquier persona puede solicitar desde el sistema situado en el lado del servicio la información asociada con el marcador ID.

5) El solicitante puede consultar toda la información proporcionada por el sistema situado en el lado de servicio, siempre que el solicitante sea el usuario del marcador ID. En caso contrario, el solicitante obtiene información limitada o no puede acceder a información alguna.

NOTA – Habrá que seguir estudiando diferentes escenarios de utilización del PPS para aplicaciones que utilicen identificación basada en marcadores, escenarios gracias a los cuales puedan describirse las ventajas del PPS.

II.4 Funciones del PPS

Para atender a los requisitos de protección PII de aplicaciones que utilizan identificación basada en marcadores, el PPS deberá contar con las siguientes funciones:

– Gestión de perfil de política PII.

– Control de acceso.

– Registro.

– Transmisión del perfil de política PII.

– Renovación del perfil de política PII.

II.4.1 Gestión del perfil de política PII

La gestión del perfil de política PII es una función básica del PPS. El sistema PPS gestiona los dos siguientes tipos de perfil de política PII:

– Perfil de política PII por defecto: Este perfil permite a un conjunto formateado de reglas y políticas de protección PII de una aplicación que utiliza identificación basada en marcadores. Dichas reglas pueden basarse en prácticas de información equitativas, tales como las que se describen en las Directrices de la OCDE sobre la protección de la privacidad y el flujo transfronterizo de datos personales ([b-OCDE]).

– Perfil de política PII definida por los usuarios: Este perfil corresponde a un conjunto formateado de reglas y políticas de protección PII, que define el usuario de un marcador ID y/o un terminal ID.

El sistema PPS lleva a cabo el establecimiento y gestión del perfil de política PII definido por el usuario (o por defecto). Concretamente, el sistema PPS debe crear y gestionar el perfil de política PII por defecto, cuando se trata de una aplicación que utiliza identificación basada en objetivos, y el perfil PII que define el usuario basándose en la política de protección PII del usuario proporcionada por el procedimiento de registro. Así pues, el perfil de política PII puede enviarse al sistema o sistemas situados en el lado de servicio. Esencialmente, dicho perfil puede contener los siguientes elementos:

– Política de revelación de recursos de información (incluida la PII).

– Política de expiración de recursos de información.

– Política de acopio de eventos para el fichero de registro cronológico.

Acto seguido, el sistema situado en el lado de servicio controla el acceso a los recursos de información utilizando dicho perfil de política PII para cada solicitante de información.

II.4.2 Control de acceso

La función de control de acceso del sistema PPS se utiliza para autenticar la identidad del usuario o ASP y autorizar el acceso a los recursos de información del usuario, que consisten esencialmente en las políticas de protección PII del propietario.

NOTA – El término "identidad" se utiliza en la inteligencia de que en el contexto de las telecomunicaciones se trata de un conjunto de identificación digno de confianza, lo que, a su vez, quiere decir que se considera fiable a los efectos de una situación determinada y en lo que concierne a representar un elemento de red, equipo de terminal de red, o usuario, una vez concluido el correspondiente proceso de validación. Tal como el término se utiliza aquí, no cabe concluir que los identificadores dignos de confianza constituyan una validación positiva de una persona.

Por otra parte, la función de control de acceso del sistema situado en el lado del servicio es un componente esencial del PPS, ya que el sistema en el lado del servicio debe controlar el acceso a todos los recursos de información y proporcionar PII basada en el perfil de política PII definido por el usuario (o por defecto, en ausencia de un perfil de política PII definido por el usuario). Resulta necesario que el sistema en el lado de servicio pueda deducir si un solicitante tiene o no acceso a una determinada PII de usuario basada en el perfil de política PII definido por el propietario.

II.4.3 Registro

El sistema situado en el lado de servicio y el sistema situado en el lado de usuario cuentan con un procedimiento para el registro en el sistema PPS. En el marco del procedimiento de registro, la información de registro proporcionada por los sistemas en el lado de servicio y de usuario es la siguiente:

– Sistema en el lado de servicio: Información de identidad (que incluye información de autenticación, tal como una contraseña) y tipo de información (por ejemplo, información sobre precios, métodos de adquisición, etc.) proporcionada a un sistema en el lado de usuario por el servidor de aplicaciones que utiliza identificación basada en marcadores.

– Sistema en el lado de usuario: Información de identidad (que incluye información de autenticación, tal como una contraseña), las propias políticas de protección PII del usuario y el consentimiento del mismo en lo que concierne a la aplicación que utiliza identificación basada en marcadores).

El sistema PPS debe crear el perfil de política PII por defecto para el sistema en el lado de servicio y proporcionar el perfil de política PII por defecto al sistema en el lado de servicio (véase la figura II.3). El perfil de política PII por defecto puede establecerse mediante la funcionalidad de gestión del perfil PII.

Por otra parte, el sistema PPS debe crear el perfil de política PII definido por el usuario basándose en las políticas de protección PII del usuario. En la figura II.3 puede verse el procedimiento de registro del PPS.

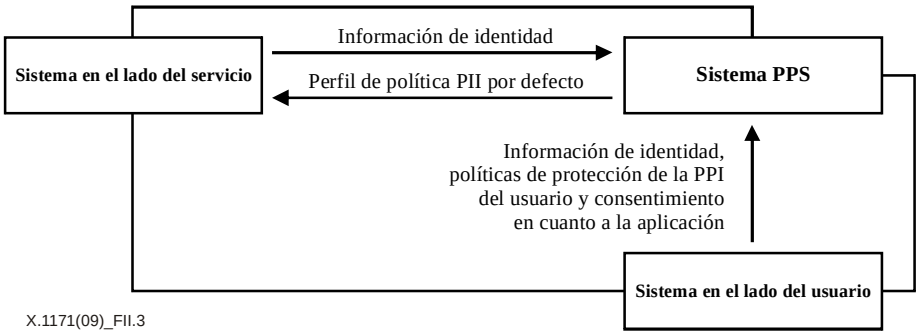

Figura II.3 – Procedimiento de registro

II.4.4 Transmisión del perfil de política PII

El procedimiento de transmisión del perfil de política PII queda activado por el sistema en el lado de servicio. La figura II.4 indica el procedimiento de transmisión del perfil PII.

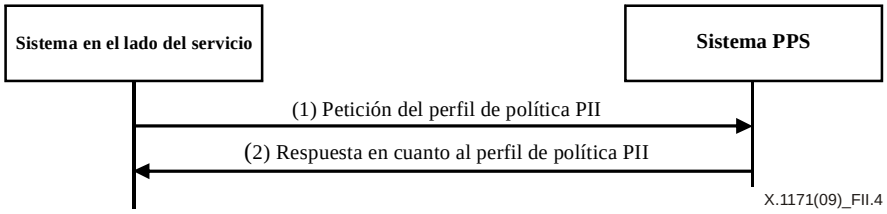

Figura II.4 – Procedimiento de transmisión del perfil de política PII

1) Solicitud del perfil de política PII: El sistema en el lado servicio solicita el perfil de política PII definido por el usuario, sirviéndose para ello de la identidad del usuario.

2) Respuesta en lo que concierne al perfil de política PII: El sistema PPS verifica el perfil de política PII definido por el usuario y envía dicho perfil.

NOTA – El término "identidad" se utiliza en la inteligencia de que en el contexto de las telecomunicaciones se trata de un conjunto de identificación digno de confianza, lo que, a su vez, quiere decir que se considera fiable a los efectos de una situación determinada y en lo que concierne a representar un elemento de red, equipo de terminal de red o usuario, una vez concluido el correspondiente proceso de validación. Tal como el término se utiliza aquí, no cabe concluir que los identificadores dignos de confianza constituyan una validación positiva de una persona.

II.4.5 Renovación del perfil de política PII

El procedimiento de renovación del perfil de política PII queda activado por el sistema PPS. Cuando el usuario modifica sus propias políticas de protección PII, el sistema PPS regenera el perfil de política PII definido por el usuario. Acto seguido, el sistema PPS envía el mensaje de renovación del perfil de política PII a todos los sistemas en el lado de servicio registrados en el sistema PPS. A continuación, cada sistema en el lado de servicio actualiza el perfil de política PPI definido por el usuario y envía el mensaje de respuesta en cuanto a la renovación del perfil de política PII. En la figura II.5 se indica el procedimiento de renovación del perfil de política PII.

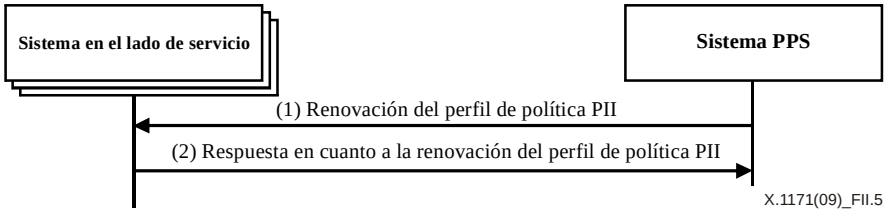

Figura II.5 – Procedimiento de renovación del perfil de política PII

1) Renovación del perfil de política PII: El sistema PPS envía el perfil actualizado de PII definido por el usuario a cada uno de los sistemas en el lado de servicio.

2) Respuesta en cuanto a la renovación del perfil de política PII: Cada uno de los sistemas en el lado de servicio envía el mensaje de respuesta de renovación al sistema PPS.

Bibliografía

[b-UIT-T F.771] Recomendación UIT-T F.771 (2008), *Descripción y requisitos del servicio para el acceso a la información sobre multimedios según la identificación basada en la etiqueta*.

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

[b-UIT-T X.811] Recomendación UIT-T X.811 (1995) | ISO/IEC 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

[b-UIT-T Y.2091] Recomendación UIT-T Y.2091 (2008), *Términos y definiciones para redes de próxima generación*.

[b-UIT-T Y.2213] Recomendación UIT-T Y.2213 (2008), *Requisitos y capacidades de servicio NGN para aspectos de red de aplicaciones y servicios basados en la identificación.*

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

[b-EPCglobal] EPCglobal standard (2008), EPCglobal Tag Data Standards Version 1.4. <http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OECD] OECD (1980), *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales* (OCDE, 2003). <http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8>

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, 2010