

Unión Internacional de Telecomunicaciones

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.1275**

(12/2010)

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

Seguridad en el ciberespacio – Gestión de identidades

---

**Directrices en materia de protección de  
información de identificación personal  
en la aplicación de la tecnología RFID**

Recomendación UIT-T X.1275



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
<b>Gestión de identidades</b>	<b>X.1250–X.1279</b>
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

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

## Recomendación UIT-T X.1275

### Directrices en materia de protección de información de identificación personal en la aplicación de la tecnología RFID

#### Resumen

En la Recomendación UIT-T X.1275 se reconoce que, con la tecnología de identificación por radiofrecuencia (RFID) la información asociada específicamente al producto utilizado o transportado por las personas queda expuesta a abusos, aun cuando facilita en gran medida el acceso a dicha información y su distribución con fines beneficiosos. El abuso puede manifestarse en forma de rastreo para la localización de la persona o de alguna forma de intrusión malintencionada en su privacidad. Por este motivo, se proporcionan en esta Recomendación directrices relativas a los procedimientos de RFID utilizables para disfrutar de los beneficios de la RFID y, al mismo tiempo, tratar de proteger la información de identificación personal.>

#### Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T X.1275	2010-12-17	17

#### Palabras clave

Aplicación de la tecnología RFID, protección de información de identificación personal.

## PREFACIO

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

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

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

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

## NOTA

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

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

## PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2011

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

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	1
3.1    Términos definidos en otras Recomendaciones .....	1
3.2    Términos definidos en la presente Recomendación .....	2
4 Abreviaturas y acrónimos .....	2
5 Convenios .....	3
6 Principios de privacidad .....	3
7 Amenazas a la PII y violaciones de esa información en la RFID.....	3
7.1    Invisibilidad de la recopilación de datos .....	4
7.2    Elaboración de perfiles .....	4
7.3    Rastreo.....	4
8 Aplicaciones RFID .....	4
8.1    Gestión de la cadena de suministros.....	5
8.2    Transporte y logística .....	6
8.3    Aplicaciones médicas y de atención de la salud.....	8
8.4    Cibergobierno .....	9
8.5    Servicio de información .....	10
9 Directrices para la protección de la información de identificación personal.....	10
9.1    Políticas y procedimientos.....	11
9.2    Restricción en el registro de la PII .....	11
9.3    Información, consentimiento, derecho de acceso, rectificación, derecho de oposición.....	11
9.4    Restricciones a la obtención y vinculación de PII.....	13
9.5    Desactivación del marcador RFID una vez cumplido el objetivo.....	13
9.6    Información sobre los proveedores de servicio y los controladores de datos	14
9.7    Medidas de organización y técnicas para proteger la PII .....	14
9.8    Evaluación de las consecuencias del sistema RFID en la privacidad .....	15
9.9    Designación del responsable oficial de la protección de los datos.....	16
Apéndice I – Características y restricciones del marcador RFID .....	17
I.1    Clasificación y características de los marcadores RFID .....	17
I.2    Restricciones de los marcadores pasivos.....	18
Apéndice II – Medidas técnicas para proteger la PII en el sistema RFID .....	19
II.1    Marcador de desactivación con contraseña .....	19
II.2    Protección privada con tecnología física.....	19
II.3    Protección de la privacidad mediante una tecnología criptográfica.....	21
Bibliografía .....	23



## Recomendación UIT-T X.1275

### Directrices en materia de protección de información de identificación personal en la aplicación de la tecnología RFID

#### 1 Alcance

La presente Recomendación proporciona orientaciones a usuarios y proveedores de la identificación por radiofrecuencia (RFID) (incluidos fabricantes y proveedores de servicios RFID) en materia de protección de la información de identificación personal para la privacidad de las personas en el contexto de la tecnología RFID.

Estas directrices pueden aplicarse en los casos en que el sistema RFID se utiliza para invadir la privacidad individual, por ejemplo, cuando la información de identificación personal es registrada en un marcador RFID y posteriormente recopilada, o cuando la información sobre objetos recopilada a través de la RFID está vinculada a la información de identificación personal. No obstante, no se aplican a los casos en que la información del objeto es recopilada y utilizada sin ningún riesgo de divulgación de la información de identificación personal ni de invasión de la privacidad.

Las presentes directrices intentan proteger la información de identificación personal para la privacidad de personas que pudieran verse afectadas por un sistema RFID y fomentar un entorno seguro para la utilización de RFID. Estas directrices, cuya finalidad es proporcionar normas básicas para el proveedor de servicios RFID y orientación a proveedores de servicios, fabricantes y usuarios de RFID con respecto a la privacidad en RFID, están sujetas a la legislación local y nacional.

#### 2 Referencias

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

[ISO/IEC 18000] ISO/IEC 18000 (2004), *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz.*

[ISO/IEC 19762-3] ISO/IEC 19762-3 (2005), *Information technology – Automatic identification and data capture (AIDC) techniques-Harmonized vocabulary – Part 3: Radio frequency identification(RFID).*

#### 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 información de identificación personal (PII)** [UIT-T X.1171]: Información relativa a una persona viva que hace posible identificarla (incluida la información que permite identificar a una

persona, cuando se combina con otra información, incluso si la primera información no permite identificar claramente a dicha persona).

**3.1.2 sistema de identificación por radiofrecuencia (RFID)** [ISO/IEC 19762-3]: Sistema de identificación automático y sistema de captura de datos que comprende uno o más lectores/interrogadores y uno o más transpondedores en los que la transferencia de datos se efectúa mediante portadoras electromagnéticas inductivas o de radiación convenientemente moduladas.

**3.1.3 marcador de identificación por radiofrecuencia (RFID)** [ISO/IEC 19762-3]: Todo transpondedor además del mecanismo de almacenamiento de información insertado al objeto.

## 3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

**3.2.1 consentimiento:** Acuerdo de aceptación o de rechazo para que un controlador de datos recopile, transfiera, utilice, almacene, archive una determinada PII o tome una decisión con respecto a ella, que supone un acuerdo individual y limitado.

**3.2.2 controlador de datos:** Entidad que vincula la información del objeto registrada en el marcador RFID a la PII, que registra la PII en el marcador RFID o que recopila la PII registrada en el marcador RFID.

**3.2.3 sujeto a quien pertenecen los datos:** Entidad que puede ser identificada por uno o más elementos de los datos relativos a sus atributos físicos, fisiológicos, mentales, financieros, culturales o sociales.

**3.2.4 aceptación:** Consentimiento explícito de un particular para que un controlador de PII recopile, transfiera, utilice, almacene, archive una determinada PII o tome una decisión con respecto a ella, con una finalidad concreta.

**3.2.5 rechazo:** Ejercicio de opción de un particular, a través de una petición, de que no se recopilen, transfieran, utilicen, almacenen, archiven datos ni que se tome una decisión con respecto a ellos.

**3.2.6 datos personales:** Véase información de identificación personal. Sinónimo de información de identificación personal.

**3.2.7 fabricante de identificación por radiofrecuencia (RFID):** Entidad que fabrica y vende placas de circuitos integrados/marcadores RFID o que fabrica (incluidos procesamiento y almacenamiento) y vende objetos con marcadores RFID incorporados o insertados.

**3.2.8 proveedor de servicios de identificación por radiofrecuencia (RFID):** Entidad que ofrece un servicio basado en objetos con marcadores RFID incorporados o insertados.

**3.2.9 usuario:** Persona que compra un objeto con marcadores RFID incorporados o insertados o que utiliza el servicio basado en un objeto con marcadores RFID incorporados o insertados.

## 4 Abreviaturas y acrónimos

La presente Recomendación utiliza las siguientes abreviaturas y acrónimos:

AES	Norma de encriptación avanzada ( <i>advanced encryption standard</i> )
NFC	Comunicación de campo cercano ( <i>near field communication</i> )
PDA	Agenda digital ( <i>personal digital assistant</i> )
PIA	Evaluación de consecuencias para la privacidad ( <i>privacy impact assessment</i> )
PII	información de identificación personal ( <i>personally identifiable information</i> )
RFID	Identificación por radiofrecuencia ( <i>radio frequency identification</i> )

## 5 Convenios

Ninguno.

## 6 Principios de privacidad

Las directrices descritas en esta Recomendación se fundan en los principios de privacidad definidos en los siguientes Documentos: [b-Consejo de Europa], [b-CE1], [CE2], [b-OECD], [b-ACNUR] y en concreto los siguientes:

- Limitación impuesta a la recopilación: Deben imponerse límites a la recopilación de datos personales y todos los datos de ese tipo deben obtenerse por medios legales, justificados y, según el caso, con conocimiento o consentimiento del sujeto a quien pertenecen los datos.
- Calidad de los datos: Los datos personales deben guardar relación con los fines para los que van a ser utilizados y, en la medida necesaria para esos fines, deben ser exactos, completos y estar actualizados.
- Especificación de objetivos: Los objetivos que responden a la recopilación de datos personales deben indicarse a más tardar en el momento en que se efectúa dicha recopilación, y su utilización posterior debe limitarse al cumplimiento de esos fines, o de otros que no sean incompatibles con esos objetivos y que se especifiquen cada vez que se modifican los objetivos.
- Límites de utilización: Los datos personales no deben divulgarse, ponerse a disposición ni utilizarse con otros fines distintos a los indicados con arreglo a los objetivos definidos.
- Protección de la seguridad: Los datos personales deben estar protegidos con medidas de seguridad razonables contra peligros tales como pérdida o acceso no autorizado, destrucción, utilización, modificación o divulgación de datos.
- Transparencia: Debe aplicarse una política general de transparencia acerca de la evolución de los datos personales y de las prácticas y políticas con respecto a ellos. Se debe disponer fácilmente de medios para establecer la existencia y naturaleza de los datos personales, y los objetivos principales de su utilización, así como la identidad y residencia habitual del controlador de datos.
- Participación individual: Un individuo debe tener derecho a:
  - a) obtener de un controlador de datos, o de otra manera, la confirmación de que éste dispone o no de datos que le pertenecen;
  - b) que le comuniquen los datos que le pertenecen en un plazo razonable; a una tarifa, si la hubiere, que no sea excesiva; de manera razonable, y de una forma que pueda comprender fácilmente;
  - c) obtener una justificación si la solicitud formulada en los subapartados a) y b) es denegada, y a impugnar esa denegación; y
  - d) impugnar los datos que le pertenecen y, si esa impugnación tiene éxito, a que los datos sean suprimidos, rectificados, completados o modificados.
- Rendición de cuentas: Un controlador de datos debe dar cuenta del cumplimiento de las medidas que dan efecto a los principios mencionados *supra*.

## 7 Amenazas a la PII y violaciones de esa información en la RFID

Las amenazas a la PII y las violaciones a esa información en la RFID pueden atribuirse a las características de la tecnología RFID sin contacto, a la vulnerabilidad de las comunicaciones inalámbricas y a la posibilidad de la recopilación de información por parte de un tercero a través de un lector RFID. En el apéndice II se describen detalladamente las características de la tecnología RFID.

Además, aumenta la posibilidad de violación de la PII debido a la implantación de la RFID, ya que la información obtenida del marcador RFID por un controlador de datos puede ser utilizada en toda la red, en lugar de utilizarse de acuerdo a las leyes, reglamentos y políticas nacionales y regionales. Esta información también puede ser modificada para obtener la PII. En el siguiente punto se describen las principales amenazas a la PII y violaciones de esa información que plantea la tecnología RFID.

Conviene indicar, sin embargo, que es difícil incorporar mecanismos de seguridad en los marcadores RFID actuales debido a los recursos que puede utilizar un marcador como, por ejemplo, energía electrónica, tiempo de procesamiento, espacio de almacenamiento, etc. En los apéndices I y II se describen las restricciones de la tecnología RFID y las medidas técnicas de protección en el sistema RFID.

### **7.1 Invisibilidad de la recopilación de datos**

La recopilación de datos puede tener lugar sin conocimiento del sujeto a quien pertenecen los datos debido a las características particulares de la tecnología RFID. En un marcador RFID los datos pueden ser leídos sin visibilidad directa puesto que las ondas radioeléctricas atraviesan obstáculos tales como bolsos o vestimentas, y cualquiera que disponga de un lector puede leer los datos en el marcador RFID. Por otra parte, el tamaño de un marcador RFID y de un lector puede ser muy pequeño, y no quedar ningún rastro de su funcionamiento. Esta característica puede ser uno de los motivos de violación de la PII en la tecnología RFID.

### **7.2 Elaboración de perfiles**

El acceso a la información de los marcadores RFID en un objeto que posee o transporta el sujeto a quien pertenecen los datos puede revelar aspectos privados de sus preferencias. En concreto, los perfiles y las deducciones que pueden extraerse de una serie de marcadores RFID transportados por un sujeto a quien pertenecen los datos podrían revelar información de carácter delicado. Además, información tan delicada como la nacionalidad, los datos biométricos o los expedientes clínicos también podría ser revelada en las aplicaciones RFID, como el pasaporte electrónico y la atención de la salud con tecnología RFID, y utilizada directamente para elaborar perfiles y sacar deducciones con respecto al sujeto a quien pertenecen los datos.

### **7.3 Rastreo**

Los sujetos a quienes pertenecen los datos que transportan un marcador RFID podrían ser rastreados, ya que a un marcador RFID se asigna un identificador único. El rastreo es facilitado por la recopilación o el procesamiento de datos temporales y de ubicación, y puede realizarse *a posteriori*, con los datos ya almacenados en una base de datos, o en tiempo real.

## **8 Aplicaciones RFID**

La tecnología RFID se utiliza profusamente en una variedad de aplicaciones, como la atención de la salud, el transporte y la logística, el cibergobierno y los servicios de información en apoyo de las cadenas de suministros y venta al público. En el cuadro 1 se observan las posibles amenazas a la PII presentes en las aplicaciones de uso corriente que utilizan la tecnología RFID.

**Cuadro 1 – Aplicaciones RFID de uso corriente y posibles amenazas a la PII**

Ámbito	Aplicaciones de uso corriente	Información en marcadores RFID	Posibles amenazas a la privacidad
Cadena de suministros	Gestión de inventarios	Producto	Rastreo, elaboración de perfiles de personas que realizan el inventario
	Venta al público (por ejemplo, en supermercados)	Producto	Rastreo, elaboración de perfiles (después de la adquisición de mercancías)
Transporte y logística	Billete de transporte público	ID de usuario, tasación, etc.	Rastreo, elaboración de perfiles
	Peaje de autopistas	ID de usuario, tasación, etc.	Rastreo, elaboración de perfiles
	Rastreo de vehículos	Producto	Rastreo, elaboración de perfiles
	Gestión de fletes/ contenedores	Producto	Rastreo, elaboración de perfiles de personas que manejan los contenedores
Atención de la salud	Rastreo de pacientes	ID de paciente, historia clínica, etc.	Rastreo, elaboración de perfiles, invisibilidad (por ejemplo, VeriChip)
	Prevención de errores en la administración de medicamentos	ID de paciente, historia clínica, recetas, etc.	Rastreo, elaboración de perfiles
	Rastreo de sangre y medicamentos contra la falsificación	Producto	×
Cibergobierno	Pasaporte electrónico	ID personal, nacionalidad, datos biométricos	Rastreo, elaboración de perfiles, falsificación de la PII
Servicios de información	Afiches inteligentes	Producto	×

Como se observa en el cuadro 1, no todas las aplicaciones RFID causan inquietud ante la posibilidad de violación de la PII (ni tampoco posibles problemas). Si la aplicación RFID no incluye al usuario, por ejemplo en algunas aplicaciones de la cadena de suministros, es poco probable que se planteen inquietudes al respecto.

Sin embargo, si, por ejemplo, los trabajadores manejan los contenedores en otras aplicaciones de la cadena de suministros, esa actividad puede controlarse con marcadores RFID.

En las subcláusulas siguientes se facilitan ejemplos de algunas aplicaciones con ciertos servicios en los cuales la violación de la PII podría plantear inquietudes.

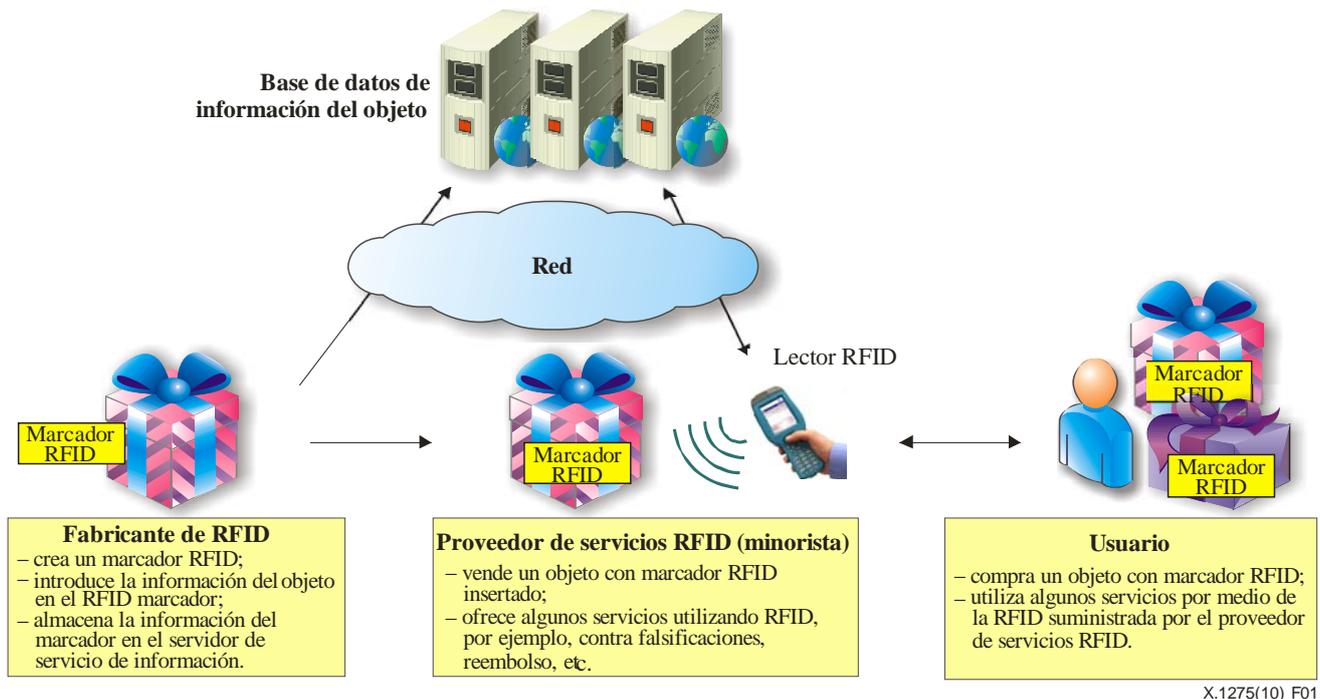
La combinación de lectores RFID y otras aplicaciones (por ejemplo, móviles) permite numerosas relaciones de comunicación que podrían dar lugar a mejores capacidades para el rastreo y la elaboración de perfiles.

### 8.1 Gestión de la cadena de suministros

Hace mucho tiempo que la tecnología RFID se utiliza para la gestión de la cadena de suministros. Las principales aplicaciones comerciales en la materia que utilizan esa tecnología incluyen gestión de inventarios/activos, venta al público, etc. La venta al público proporciona el servicio de

aplicación RFID más representativo. En la figura 1 se observa un ejemplo de utilización de RFID en una aplicación de venta al público, que ilustra de qué manera se distribuye un marcador RFID.

Las aplicaciones RFID de venta al público son propiciadas por un fabricante que crea un marcador RFID, introduce la información del objeto en ese marcador y lo inserta en el objeto. En este ejemplo, el minorista en cuestión es un proveedor de servicios RFID que vende a un usuario un objeto con un marcador RFID. Por lo general, se han utilizado marcadores pasivos para el sistema RFID en la gestión de la cadena de suministros aplicando contraseñas de desactivación, etc., para proteger la PII del sujeto a quien pertenecen los datos. En algunos casos, por ejemplo en aplicaciones para determinados artículos, la gestión de la cadena de suministros requiere a menudo marcadores pasivos con largo alcance de comunicación incluso para cada artículo.



**Figura 1 – Ejemplo de utilización del RFID en aplicaciones de venta al público**

Las inquietudes por la posibilidad de violación de la PII respecto a la aplicación de venta al público se plantean principalmente después de que un usuario compra un objeto al que se inserta un marcador RFID, puesto que la participación del usuario se produce en el punto de venta únicamente durante este proceso. Cuando un usuario compra un objeto con un marcador RFID insertado, el minorista puede identificar las preferencias de ese usuario estableciendo una relación entre la información del objeto almacenada en el marcador RFID y la información de pago del usuario o la tarjeta de fidelidad, y observando y analizando continuamente las modalidades de compra del usuario. En este caso, el proveedor de servicios RFID se convierte en el controlador de datos, y el usuario en el sujeto a quien pertenecen los datos. Y con un lector, cualquiera puede leer el marcador RFID, a menos que éste se elimine o destruya.

## 8.2 Transporte y logística

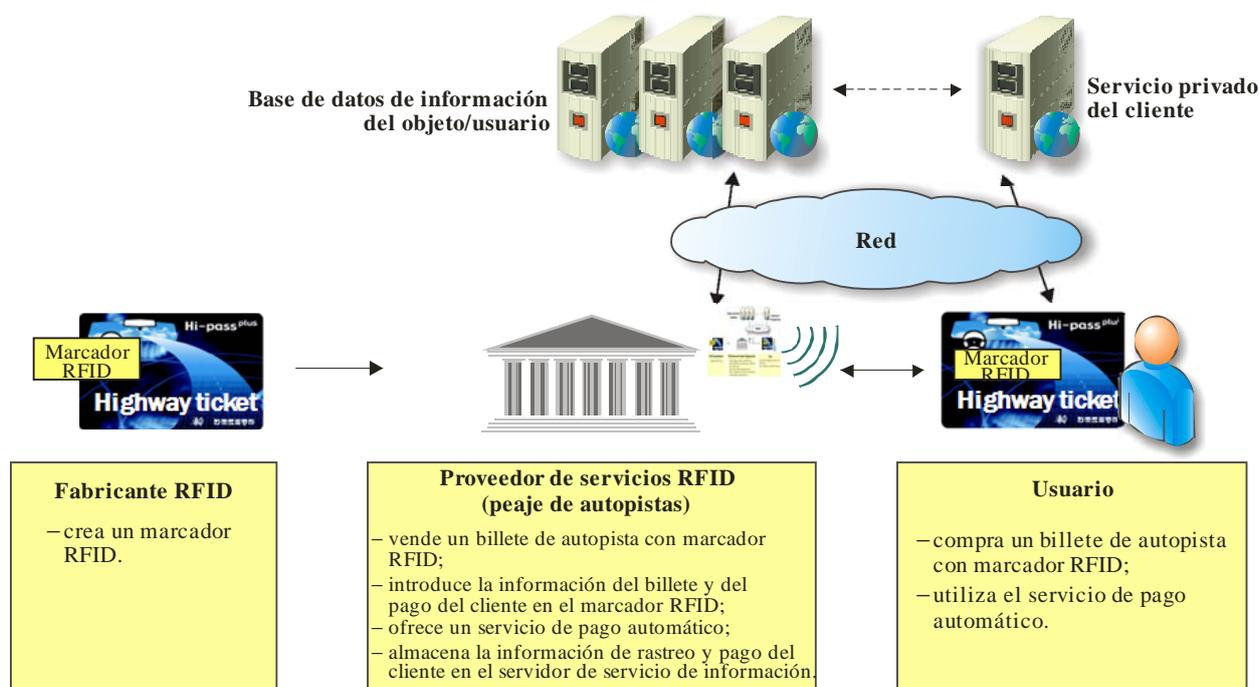
Los sistemas RFID son muy adecuados para ciertas aplicaciones de transporte y logística. Teniendo en cuenta la distribución adecuada de lectores RFID, vehículos equipados con un marcador pueden ser rastreados en una pequeña superficie, como un almacén o una fábrica. Los billetes de transporte público y los sistemas de peaje de autopistas, como los descritos en [b-E-ZPass], son aplicaciones que pueden dar lugar a inquietudes en materia de privacidad en los sectores de transporte y logística.

Hay varias aplicaciones RFID en transporte y logística. En particular, muchos billetes de transporte público y sistemas de peaje de autopistas ya se basan en la tecnología RFID. En la figura 2 se facilita un ejemplo de aplicación de transporte, en el que se observa de qué manera se utiliza un marcador RFID para identificar y rastrear un vehículo en el sistema de peaje de autopistas.

El fabricante de RFID en una aplicación de peaje de autopistas simplemente crea un marcador RFID y lo vende al proveedor de servicios RFID. Dicho proveedor, que ofrece y gestiona un servicio de peaje de autopistas, puede introducir la información de pago de un usuario en un marcador RFID en algunos casos concretos. Esta información almacenada en un marcador RFID es la PII que puede utilizarse para identificar convenientemente al usuario.

Si la información de pago del usuario está asociada a la información de rastreo de movimiento del usuario registrada por el sistema de peaje de autopistas, dicha información puede no obstante amenazar seriamente la privacidad del usuario. En este caso, el proveedor de servicios RFID – el sistema de peaje de autopistas – se convierte en el controlador de datos, y el usuario en el sujeto a quien pertenecen los datos.

Los marcadores pasivos se han utilizado generalmente para el sistema RFID en transporte y logística. En el caso del transporte, con frecuencia se utilizan esquemas criptográficos ligeros (basados en un esquema de encriptación simétrica) para la autenticación entre el marcador y el lector y para asegurar la posterior transmisión de los datos.



X.1275(10)\_F02

**Figura 2 – Ejemplo de utilización del RFID en transporte y logística**

En cuanto a los billetes de transporte, se utiliza con frecuencia una tarjeta inteligente sin contacto fabricada con placas de circuitos integrados RFID que COMUNICAN A 13,56 MHz y que tienen corto alcance de comunicación. Cuando se utiliza un marcador de corto alcance, como ocurre en este caso, es posible, al menos técnicamente, utilizar esquemas criptográficos seguros convencionales (incluso asimétricos) con los que se puede atenuar parcialmente el riesgo de filtración de la PII del sujeto a quien pertenecen los datos. Hay que tener en cuenta, sin embargo, que los protocolos que se utilizan en este momento sólo pueden impedir la copia de un marcador (y de esa forma evitar la usurpación del usuario). El marcador ID aún se revela en texto sencillo al inicio de la transacción entre el marcador y el lector. Así, cualquiera pueda leer el marcador ID, lo que plantea inquietudes por la posibilidad de violación de la PII. En cualquier caso, los datos

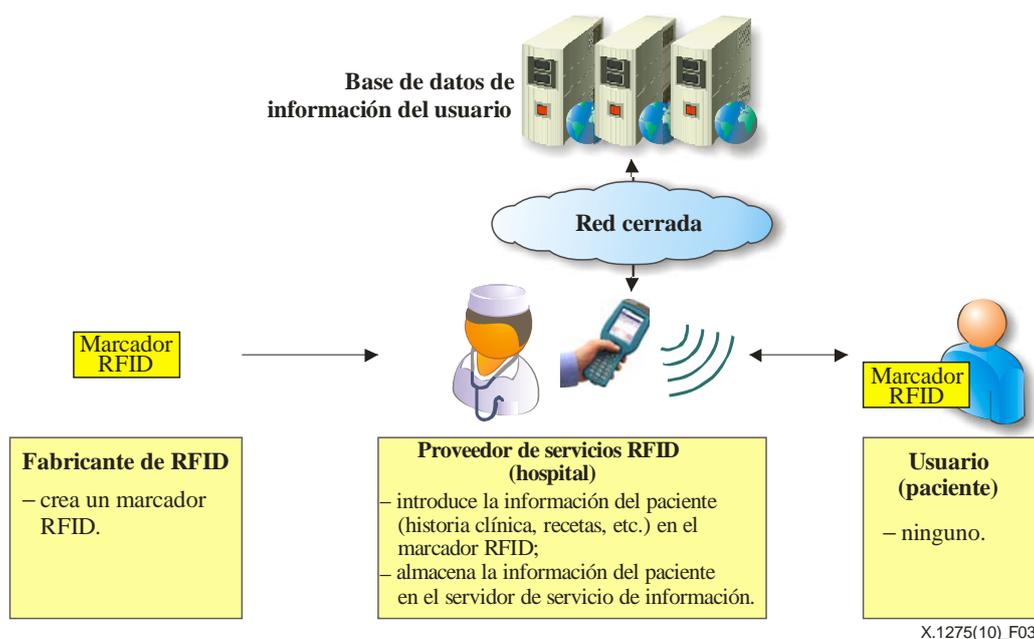
introducidos en la base de datos cuando el usuario interactúa con el sistema han de anonimizarse lo antes posible para reducir las amenazas a la privacidad de los usuarios.

### 8.3 Aplicaciones médicas y de atención de la salud

Aunque hay varias aplicaciones RFID destinadas a la atención de la salud, la utilización de la RFID en ese tipo de aplicaciones puede causar inquietud por la posibilidad de violación de la PII debido al carácter confidencial de los datos. Varias aplicaciones RFID para la atención de la salud incluyen seguimiento de los pacientes por motivos de seguridad y protección, medicamentos sujetos a medidas contra la falsificación, observancia del paciente a las recetas prescritas y rastreo de sangre. Los sistemas RFID ya se utilizan en la industria farmacéutica para facilitar el seguimiento de los medicamentos y evitar falsificaciones o la pérdida resultante de robos durante el transporte. En la figura 3 se observa un ejemplo de utilización de la RFID en aplicaciones de atención de la salud, que muestra cómo se utiliza un marcador RFID.

En relación con la observancia del paciente a las recetas prescritas, el fabricante RFID simplemente crea un marcador RFID y lo vende. El proveedor de servicios RFID, es decir, los médicos y enfermeras del hospital, pueden ser los controladores de datos que introducen y gestionan la información médica del paciente.

En la aplicación que se observa en la figura 2, los médicos o enfermeras del hospital pueden comprobar el historial del paciente en materia de tratamiento y prescripción de recetas leyendo la información contenida en el marcador RFID del paciente y, posteriormente, tomar las medidas adecuadas teniendo en cuenta esa información. En cambio, en las aplicaciones para el seguimiento de los medicamentos, se puede acceder con facilidad a la información del marcador de la persona con el medicamento marcador fuera del hospital o de la farmacia; la enfermedad del paciente también puede deducirse directamente de la información que figura en el marcador RFID. Por lo tanto, el riesgo de revelar la información personal del sujeto a quien pertenecen los datos puede ser mayor que el correspondiente a la aplicación descrita en la figura 2. Por este motivo, si la información médica del paciente, tal como se almacena en un marcador RFID o en la base de datos auxiliar, no se administra ni protege adecuadamente, puede suponer una amenaza directa a la PII del sujeto a quien pertenecen los datos.



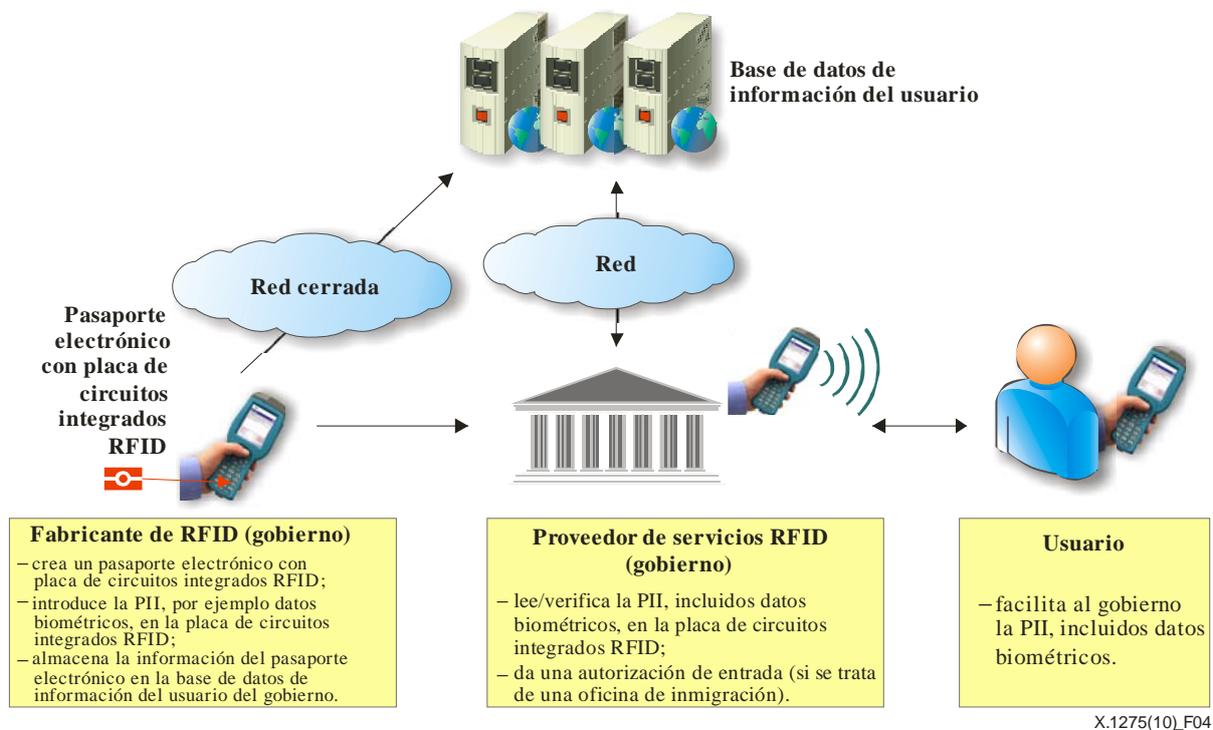
**Figura 3 – Ejemplo de utilización de la RFID en aplicaciones médicas y de atención de la salud**

Por lo general, no se han utilizado marcadores activos con largo alcance de comunicación para el sistema RFID en aplicaciones médicas y de atención de la salud. Sin embargo, en algunos casos puede preferirse el marcador activo con largo alcance de comunicación como, por ejemplo, para controlar el estado de una persona inválida en el hogar.

## 8.4 Cibergobierno

El pasaporte electrónico es la aplicación más habitual de cibergobierno. La placa de circuitos integrados RFID incorporada en él contiene normalmente numerosa PII del sujeto, por ejemplo número de pasaporte, nombre, nacionalidad, fotografía, datos biométricos, etc.; por este motivo, se plantean grandes inquietudes con respecto a la violación de esa información.

Es fundamental que el marcador RFID integre las medidas de seguridad adecuadas para reducir los riesgos de captura o clonación de los datos que figuran en el pasaporte electrónico, puesto que constituyen la PII más importante y decisiva. En la figura 4 se da un ejemplo de utilización de la RFID en el sistema de pasaporte electrónico y se muestra de qué manera se utiliza una placa de circuitos integrados RFID.



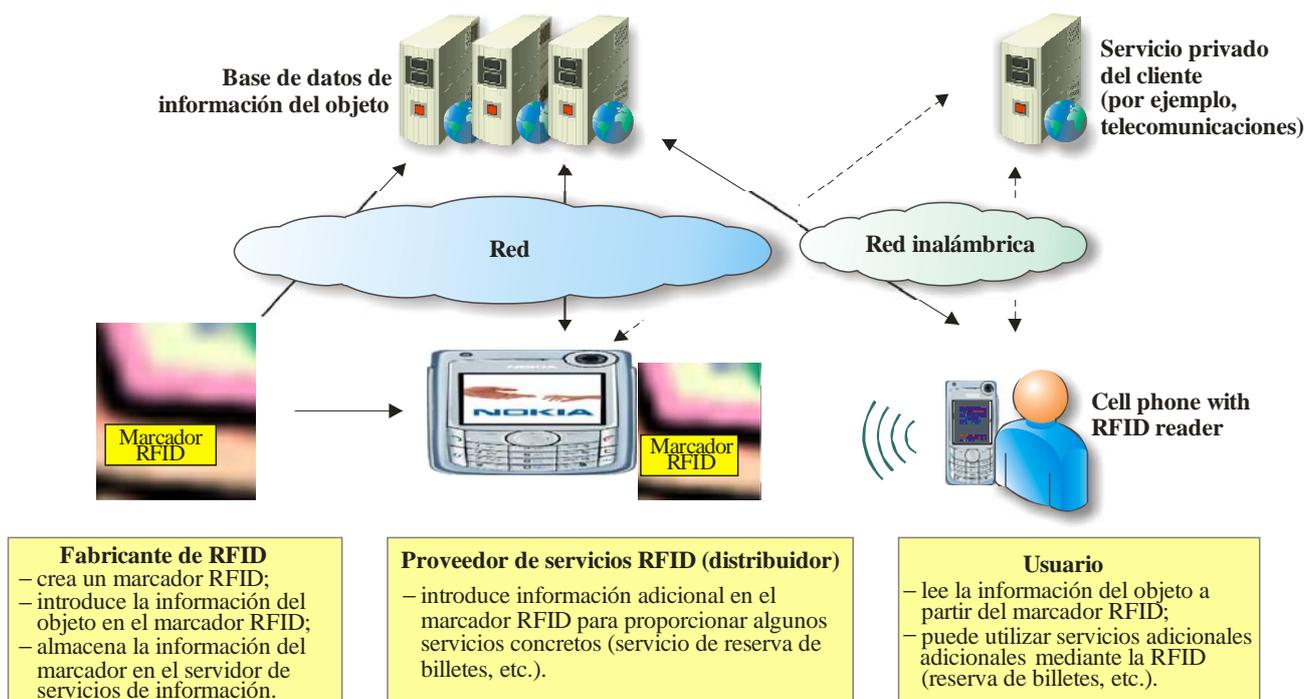
**Figura 4 – Ejemplo de utilización de la RFID en aplicaciones de pasaporte electrónico**

El usuario que desea obtener un pasaporte electrónico biométrico facilita la PII, incluidos datos biométricos, a los ministerios del gobierno, que pueden ser el fabricante de RFID en la aplicación de pasaporte electrónico. Éstos crean un pasaporte electrónico con placa de circuitos integrados RFID e introducen en dicha placa la PII del usuario, incluidos datos biométricos. El proveedor de servicios RFID, por ejemplo la oficina de inmigración, lee la PII de la placa de circuitos integrados RFID y la verifica. Los datos biométricos almacenados en la placa de circuitos integrados RFID del pasaporte electrónico constituyen una de las PII más delicadas puesto que pueden utilizarse para autenticar o identificar al usuario. Si esos datos biométricos se divulgan o modifican, podrían amenazar seriamente la privacidad del usuario. En esta aplicación, tanto el fabricante como el proveedor de servicios RFID pueden ser el controlador de datos y el usuario, el sujeto a quien pertenecen los datos. Los marcadores pasivos con corto alcance de comunicación se han utilizado generalmente en esta aplicación. El pasaporte electrónico admitirá la criptografía.

Sin embargo, los protocolos de seguridad descritos en las normas, por ejemplo [b-OACI], son a veces opcionales o están mal utilizados. Por ese motivo, siguen planteándose grandes inquietudes en materia de privacidad con respecto a las aplicaciones de pasaporte electrónico.

### 8.5 Servicio de información

Los afiches inteligentes constituyen una de las aplicaciones de servicio de información más habituales. En este caso, el lector RFID suele estar ubicado en un dispositivo móvil y el marcador RFID, en un punto fijo. En la figura 5 se da un ejemplo de utilización de la RFID en una aplicación de afiche inteligente y se muestra de qué manera se utiliza un marcador y un lector RFID.



X.1275(10)\_F05

**Figura 5 – Ejemplo de utilización de la RFID en aplicaciones de afiches inteligentes**

El fabricante de RFID de un afiche inteligente crea simplemente una placa de circuitos integrados RFID y la vende al proveedor de servicios RFID. El distribuidor o la sala de cine es un proveedor de servicios RFID que introduce información sobre la película en el marcador RFID integrado en el afiche. Otro ejemplo de servicios de información es el asistente de carretera, servicio que proporciona información al usuario sobre la forma de encontrar fácilmente una ruta. En realidad, estos tipos de aplicaciones no plantean ninguna inquietud en materia de privacidad dado que no utilizan ninguna clase de información privada ni confidencial. Hay que señalar, sin embargo, que la movilidad y los límites de lectura del lector RFID integrado en el dispositivo móvil pueden ser factores que amenazan la privacidad de los usuarios.

## 9 Directrices para la protección de la información de identificación personal

Debido a que, aunque siguen evolucionando, las tecnologías en materia de privacidad y seguridad relativas a la RFID se encuentran en su primera etapa, y a que no se ha hallado ninguna solución "compatible" puesto que el marco de utilización y las características técnicas de los marcadores RFID varían notablemente de una aplicación a otra, podría ser prematuro aplicarlas a todos los servicios RFID. Por consiguiente, estas directrices se refieren principalmente a medidas de protección generales de la PII del sujeto a quien pertenecen los datos y no a medidas técnicas. Sin

embargo, las medidas técnicas no deben ignorarse: se alienta a los diseñadores a que, durante la concepción de una aplicación RFID, tengan en cuenta la adopción de soluciones técnicas de avanzada que puedan ofrecer mayor protección a la privacidad.

## **9.1 Políticas y procedimientos**

Los controladores de datos en el servicio RFID deben formular políticas y procedimientos que rijan el sistema RFID, en particular sobre la utilización adecuada de la PII, y anunciarlas por anticipado. En esas políticas y esos procedimientos debería atribuirse funciones y responsabilidades relativas a la gestión y utilización de la PII. Por otra parte, el controlador de datos debería asignar más responsabilidades a una persona que gestiona y utiliza directamente la PII que a otras.

## **9.2 Restricción en el registro de la PII**

Los controladores de datos en el servicio RFID han de ajustarse al principio de limitación de obtención de datos. Por consiguiente, el controlador sólo procesará los datos pertinentes para el objetivo de diseño del sistema y la PII no se almacenará más tiempo del necesario.

En concreto, los controladores de datos en el servicio RFID no deberán normalmente registrar la PII en el marcador RFID a menos que esté estipulado por ley o haya recibido un consentimiento explícito por escrito del sujeto a quien pertenecen los datos. Toda la PII registrada en los marcadores RFID deberá estar encriptada, si los controladores de datos deben registrar la PII en el marcador RFID. Cuando los controladores de datos necesiten el consentimiento del sujeto a quien pertenecen los datos, se optará de preferencia por el método de aceptación. Los controladores de datos deberán notificar por adelantado al sujeto la finalidad del registro de la PII y su posible utilización.

Los controladores de datos en el servicio RFID deben obtener consentimiento individual, específico para cada elemento de la PII registrado y deberán informar a los sujetos a quienes pertenecen los datos de la finalidad del registro o utilización de esa información.

## **9.3 Información, consentimiento, derecho de acceso, rectificación, derecho de oposición**

Los controladores de datos han de cumplir con el principio de participación individual. Por consiguiente, los controladores de datos en el servicio RFID deben adoptar las medidas pertinentes para ofrecer al usuario información sobre la PII registrada, así como derecho a consentir, acceder, rectificar u oponerse a su PII sin costos para el usuario. Esto es aplicable a la PII codificada en los marcadores RFID y a la PII vinculada a la información almacenada en los marcadores RFID.

### **9.3.1 Información**

Los controladores de datos deberán notificar al sujeto a quien pertenecen los datos una indicación de los marcadores RFID anexos, de la instalación del lector RFID y de los terceros a quienes se pueden haber divulgado los datos por rectificación o supresión de bloqueo, a menos que ello sea imposible o suponga un esfuerzo desproporcionado.

#### **9.3.1.1 Indicación del marcador RFID insertado**

Para un marcador RFID integrado o insertado, incluso después de que el usuario haya comprado o recibido el objeto, los controladores de datos en el servicio RFID tendrán que dar previamente al usuario (antes de que adquiera el objeto) las siguientes explicaciones o indicar la información sobre el objeto o su utilización de forma clara:

- El hecho de que se inserta un marcador RFID y su ubicación.
- Naturaleza y función del marcador RFID.
- Tipo de información registrada en el marcador RFID.

- Finalidad o utilización de la información registrada en el marcador RFID.
- Información de contacto del encargado oficial de la protección de los datos, de conformidad con la cláusula 9.9.

Cabe señalar que, si el marcador no está destinado a ser utilizado por el sujeto a quien pertenecen los datos una vez adquirido el objeto, el marcador deberá ser desactivado por el servicio RFID o los controladores de datos en el momento en que el usuario adquiriera el objeto marcador, a menos que el usuario decida mantener el marcador en funcionamiento.

### **9.3.1.2 Indicación de instalación del lector RFID**

El que instala un lector capaz de leer la información de un objeto con un marcador RFID integrado o insertado (o la PII registrada en el marcador RFID y distribuida a los sujetos a quienes pertenecen los datos) indicará como verificador dónde y por qué motivo está instalado el lector de manera que el sujeto a quien pertenecen los datos pueda detectarlo fácilmente. La notificación incluirá, como mínimo, la identidad del operador y un punto de contacto donde los usuarios puedan obtener la política de información.

Si un lector RFID está integrado en un PDA (agenda personal) o un teléfono celular, el alcance de la lectura del lector debe ser restringido para limitar la obtención de la PII a través del marcador RFID.

### **9.3.2 Consentimiento**

Los controladores de datos han de obtener por adelantado el consentimiento del sujeto a quien pertenecen los datos. En las transacciones al por menor y logísticas, donde el principio de desactivación está configurado por defecto, los controladores de datos pueden obtener el consentimiento del sujeto a quien pertenecen los datos mediante un acuerdo escrito específico, un formulario de registro de usuario, un correo electrónicos, etc. En cualquier otro caso, como una aplicación de pasaporte electrónico biométrico, no es necesario el consentimiento del usuario porque existe la obligación jurídica de obtención de la PII y su almacenaje en el marcador.

### **9.3.3 Derecho de acceso, rectificación y derecho de oposición**

El sujeto a quien pertenecen los datos debe poder obtener del controlador de datos, sin limitaciones a intervalos razonables y sin excesivos retrasos o gastos:

- confirmación de si sus datos están o no siendo procesados e información sobre, como mínimo, el objetivo del procesamiento, la categoría de los datos concernidos y los receptores o tipos de receptores a quienes se divulgan los datos;
- comunicación, en formato inteligible, de los datos que se procesan y de cualquier información disponible sobre su origen;
- información sobre la lógica de cualquier procesamiento automático de los datos relativos al sujeto, al menos en el caso de las decisiones automatizadas.

Además, en el servicio RFID son necesarios los controladores de datos para tomar las medidas oportunas a fin de proporcionar al usuario un método de corrección, modificación y destrucción de la PII de los datos en cuestión sin que ello suponga coste alguno para el usuario.

Esto es aplicable a la PII codificada en los marcadores RFID, así como a la PII vinculada con la información almacenada en los marcadores RFID.

En concreto, si el marcador no es útil para el sujeto a quien pertenecen los datos (por ejemplo, en el sector al por menor, cuando un usuario adquiere un objeto marcador), los controladores de datos han de desactivar, suprimir o destruir el marcador, como se indica en el punto 9.5, a menos que el sujeto solicite que se mantenga en funcionamiento.

## **9.4 Restricciones a la obtención y vinculación de PII**

Los controladores de datos en el servicio RFID han de notificar al sujeto a quien pertenecen los datos cuándo obtienen la PII registrada en el marcador o almacenada en una base de datos mediante su vinculación con la información de objeto del marcador. Si los proveedores del servicio RFID necesitan utilizar la PII para fines distintos de los previstos o para ofrecer tal información a un tercero, deberán informar convenientemente al sujeto a quien pertenecen los datos y obtener por adelantado y por escrito su consentimiento.

### **9.4.1 PII registrada en un marcador RFID**

Los controladores de datos en el servicio RFID han de notificar al sujeto a quien pertenecen los datos, o indicarlo de manera claramente visible, que pueden obtener la PII registrada en el marcador RFID y obtener por adelantado su consentimiento.

Cuando los controladores de datos obtengan la PII, deberán adoptar determinadas medidas de certificación para el lector y el marcador RFID, como un protocolo de autenticación entre el marcador RFID y el lector y entre el lector y la base de datos extrema. En este contexto, por "medida de certificación" se entiende el esquema criptográfico para el almacenaje del identificador del marcador RFID en la base de datos auxiliar y la PII utilizada para identificar y autenticar al lector RFID y al controlador de datos.

Desde el punto de vista de la protección de la PII, sin embargo, cabe señalar que los protocolos de autenticación existentes entre el marcador y el lector sólo son eficaces si el marcador almacena más información que su identificador, pues con los actuales protocolos de transmisión RFID, el ID del marcador mismo no está protegido.

### **9.4.2 PII vinculada a la información de objeto en el marcador RFID**

Si los controladores de datos quieren vincular la información de objeto registrada en el marcador RFID con la PII, normalmente, antes de facilitar el marcador, enviarán por adelantado una notificación a tal efecto al sujeto a quien pertenecen los datos, lo indicarán de manera fácilmente visible y obtendrán su consentimiento específico. Cuando los controladores de datos vinculen la información de objeto del marcador RFID a la PII, habrán de adoptar determinadas medidas de certificación para el lector RFID, como una contraseña o un protocolo de autenticación entre el lector y el marcador RFID.

Si la PII se obtuvo sin intención de vincularla a la información de objeto, pero se ha de vincular posteriormente, los controladores de datos deberán notificar su intención al usuario y obtener nuevamente su consentimiento específico a fin de ajustarse a los requisitos jurídicos.

## **9.5 Desactivación del marcador RFID una vez cumplido el objetivo**

Los marcadores RFID incorporados o anexos serán eliminados, destruidos o permanentemente desactivados por el proveedor del servicio RFID o los controladores de datos en el momento en que el usuario adquiere o recibe el objeto marcador (punto de venta), a menos que el usuario decida mantener el marcador en funcionamiento o así lo exijan las leyes o reglamentos. Aunque el usuario decida mantener operativo el marcador, los controladores de datos deberán facilitar su eliminación, destrucción o desactivación permanente con ulterioridad. Se han de notificar al usuario las consecuencias de la desactivación.

La desactivación ha de ser la regla general, pero puede que no sea la solución adecuada para todas las aplicaciones. Por ejemplo, si el marcador se utiliza para acceder al historial médico y farmacéutico de un paciente en una aplicación sanitaria y se desactiva, resultará más difícil que haya una continuidad en el tratamiento del paciente. La desactivación puede ser obligatoria en aplicaciones de gestión e la cadena de suministros, mientras que puede dejarse en manos del usuario en aplicaciones de transporte y logística. En el caso de las aplicaciones sanitarias y de cibergobierno, la desactivación no es aplicable por motivos de salud pública o por ley. El fabricante

RFID o el controlador de los datos en el servicio RFID pueden emplear determinadas medidas técnicas para desactivar el marcador RFID, como la eliminación de la contraseña, el RFID zapper, etc. No obstante, si la desactivación de un marcador RFID va en contra del interés público o el interés del usuario, los controladores de datos han de explicarlo al usuario o indicarlo de manera clara y visible en el objeto.

## **9.6 Información sobre los proveedores de servicio y los controladores de datos**

Los proveedores de servicio y los controladores de datos han de elaborar y publicar una política de información concisa, exacta y fácilmente comprensible para cada una de sus aplicaciones. Esta política ha de incluir, como mínimo, lo siguiente:

- identidad y dirección de los controladores;
- objetivo del sistema RFID;
- qué datos procesará el sistema, sobre todo si se van a procesar datos personales, y si se va a controlar la ubicación de los marcadores;
- un resumen de la evaluación de la protección de la privacidad y los datos;
- los riesgos probables para la privacidad, de haberlos, relativos a la utilización de marcadores en la aplicación y las medidas que los particulares pueden adoptar para reducir tales riesgos.

## **9.7 Medidas de organización y técnicas para proteger la PII**

- Cuando utilizan el sistema RFID para registrar y recopilar la PII o vincular la información del objeto del marcador RFID a la PII, los controladores de datos en el servicio RFID deben tomar medidas de seguridad técnica y de organización para proteger la PII del sistema RFID con objeto de impedir la pérdida, el robo, la filtración, la alteración o el deterioro de información de interés. Las medidas de organización y operacionales para proteger la PII son, entre otras, las siguientes:
  - plan de gestión interna de la seguridad;
  - análisis de riesgos, análisis de la amenaza a la privacidad y evaluación de las consecuencias sobre la privacidad;
  - educación sobre la privacidad en el servicio RFID, etc.
- Las medidas técnicas para proteger la PII son, entre otras, las siguientes:
  - control de acceso y auditoría de la base de datos auxiliar;
  - control de acceso para impedir que cualquier lector pueda acceder a la información almacenada en el marcador;
  - encriptación de la PII almacenada en el marcador y en la base de datos auxiliar;
  - utilización de protocolos factibles entre el lector y el marcador para proteger la transmisión de la PII, por ejemplo protocolos criptográficos o todo tipo de técnicas adecuadas;
  - utilización de marcadores con identificadores de marcador aleatorios a fin de reducir los riesgos de rastreo;
  - certificación de lectores RFID válidos;
  - desactivación del marcador RFID, por ejemplo, contraseña de desactivación, desactivador de RFID, etc.;
  - restricción de la capacidad del lector y el marcador, por ejemplo, interferencia activa, detección de sensor RFID, marcador fragmentado, marcador bloqueador, etc. [b-Juels];
  - medidas de seguridad para reducir los riesgos derivados de la PIA para la privacidad.

Téngase en cuenta que las medidas técnicas y de organización enumeradas son sólo algunas de las medidas de protección de la PII. En el futuro podrán añadirse nuevas medidas, pues la investigación en esta esfera está en curso.

## **9.8 Evaluación de las consecuencias del sistema RFID en la privacidad**

Cuando los proveedores de servicios RFID y los controladores de datos utilizan el sistema RFID para registrar y recopilar la PII o vincular la información del objeto del marcador RFID a la PII deben hacer todo lo posible para garantizar la no violación de esa información por el análisis y la evaluación de cualquier posibilidad de filtración o de amenazas a la PII que acompañan la utilización del sistema RFID antes de que éste se implante, teóricamente en la etapa de diseño.

Debido a la gran variedad de posibilidades de configuración técnica y de utilización, no hay una solución que se adapte a todas las aplicaciones RFID. Por lo tanto, una evaluación podría contribuir a determinar las consecuencias en la privacidad (según distintos puntos de vista, por ejemplo, el jurídico y el relativo a los aspectos técnicos) y a encontrar las mejores estrategias para su atenuación. A continuación se describe un posible proceso de evaluación de consecuencias para la privacidad (PIA). La PIA ha de abarcar todo el sistema RFID.

- Paso 1: Iniciación del proyecto.

Este paso determina el alcance de las actividades que ejecuta la PIA, organiza el equipo de ejecución de la PIA y aplica las herramientas de la PIA para reflejar el alcance definido.

- Paso 2: Análisis del flujo de datos.

La finalidad de esta medida es trazar un diagrama u organigrama de la información de identificación personal de modo que el objetivo del análisis de riesgos se pueda verificar identificando la información de identificación personal manipulada por el servicio de evaluación de las consecuencias y los elementos de información que contengan dicha información.

Concretamente, en este paso se identifica qué PII se recopila, utiliza, almacena, elimina o se facilita a un tercero a través de qué método en un diagrama u organigrama. Además, se describe el papel y la responsabilidad de la persona a cargo de cada paso (recopilación, utilización, almacenamiento y eliminación) de la manipulación de la PII.

- Paso 3: Análisis de los factores y riesgos de violación de la información de identificación personal.

En este paso se identifican las amenazas contra los elementos de la información de identificación personal y sus vulnerabilidades, y se realiza un análisis de riesgos al respecto.

- Paso 4: Plan de mejora y planificación de la gestión de riesgos.

En este paso se determina el nivel de riesgo que requiere una gestión entre los diferentes riesgos identificados en el análisis de riesgos con respecto a la información de identificación personal, y se preparan varios métodos de control para atenuar y gestionar cada riesgo.

- Paso 5: Informe de los resultados de la PIA.

Siendo uno de los más decisivos del proceso, este paso consiste en redactar y presentar informes sobre la PIA y sus resultados.

Los informes de la PIA deben contemplar el resultado de los contenidos examinados en todos los procesos del análisis, desde el resultado de la PIA hasta el método de control y gestión de riesgos para los riesgos identificados en relación con la información de identificación personal.

El proceso PIA descrito es sólo un ejemplo y el proceso real puede adaptarse a necesidades específicas o basarse en otros procesos PIA externos existentes.

## **9.9 Designación del responsable oficial de la protección de los datos**

Los controladores de datos deberán nombrar a un responsable oficial de la protección de los datos encargado, en concreto, de mantener un registro de información detallada de las operaciones de procesamiento que realizan los controladores de datos, incluida información sobre las evaluaciones de consecuencias en la privacidad y de las medidas de seguridad de las aplicaciones RFID, y de tramitar sin tardanza las quejas o solicitudes de los usuarios para ejercer sus derechos.

## Apéndice I

### Características y restricciones del marcador RFID

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

#### I.1 Clasificación y características de los marcadores RFID

En este punto se explican las características de la clasificación de marcadores RFID, así como el motivo por el cual las técnicas de seguridad no pueden aplicarse fácilmente a un marcador pasivo. Por lo general, los marcadores RFID se pueden clasificar en marcadores pasivos y activos. En el cuadro I.1 se observa esa clasificación.

**Cuadro I.1 – Clasificación y características de los marcadores RFID**

Características	Marcadores pasivos	Marcadores activos
Fuente de energía	Energía transmitida por el lector	Batería interna
Alcance de comunicación	3 m o menos	100 m o más
Tiempo de vida	Ilimitado	Según la duración de la batería
Almacenamiento de datos	Pequeño almacenamiento de datos de lectura/escritura (bytes)	Gran almacenamiento de datos de lectura/escritura (Kbytes)
Aplicaciones habituales	Gestión de inventarios, venta al público, control de equipajes/ plataformas de carga, tarjetas de seguridad, etc.	Aplicaciones complejas con rastreo de personas, etc. (Atención de la salud o control de superficies, peaje de autopista, etc.)

Dado que los marcadores pasivos no tienen una fuente interna de energía, utilizan la energía transmitida por el lector RFID, para enviar una señal al lector. El alcance de comunicación de los marcadores pasivos es de aproximadamente 3 m o menos. En el caso de la banda 13,56 MHz, el alcance se sitúa en torno a 4-10 cm, pero puede ampliarse con una antena de gran alcance. El marcador en ondas decimétricas tiene mayor alcance de comunicación, aproximadamente de 3 a 7 m.

A diferencia de los marcadores pasivos, los marcadores activos tienen su propia fuente de energía que les permite enviar una señal al lector. El alcance de comunicación de los marcadores activos es de unos 100 m o más, pero su tiempo de vida útil depende de la duración de la batería. Además, los marcadores activos son más grandes y más costosos que los marcadores pasivos.

Por lo general, un sistema que funciona en bandas de ondas kilométricas (125/135 kHz) o de ondas decamétricas (13,56 MHz) es un sistema pasivo. Los sistemas que funcionan en bandas de ondas decimétricas (433/900 MHz, 2,45 GHz) y en bandas de microonda pueden ser pasivos o activos.

El marcador de ondas kilométricas es sumamente utilizado en la seguridad, la gestión de activos y la verificación de autenticidad de un producto debido al corto alcance de exploración del marcador, en tanto que el marcador de ondas decamétricas se utiliza en los servicios de transporte ferroviario, la logística y la distribución, debido a su alcance de exploración de 30 m+. En particular, la banda 13,56 MHz se incorpora y utiliza en las tarjetas de crédito o las tarjetas de pago de transporte. El pasaporte electrónico y la comunicación de campo cercano (NFC) son otros ejemplos de aplicaciones que utilizan la banda 13,56 MHz.

## I.2 Restricciones de los marcadores pasivos

Numerosos expertos que trabajan en el sector de la RFID señalan que, con miras a fomentar ese mercado, el precio del marcador RFID debe ser inferior a 5 centavos. Este requisito pone límites a los recursos que pueden ser utilizados por un marcador, como la energía eléctrica, el tiempo de procesamiento, el espacio de almacenamiento y el número de puertas.

Para que cuesten menos de 5 centavos, los marcadores RFID sólo podrán almacenar centenares de bits, tener 5-10 K puertas lógicas y un alcance de comunicación de unos pocos metros. De todas esas puertas, únicamente entre 250 y 3 000 se puede destinar a funciones de seguridad. Asimismo, deben tenerse en cuenta las restricciones de energía puesto que la mayoría de los marcadores RFID actualmente en uso son pasivos.

A menudo, la legislación impone límites a la potencia de radiación de los lectores y, por ese motivo, la capacidad de alimentar el marcador es limitada. Con la tecnología actual, aún sin restricción de costos, la utilización de sistemas criptográficos de seguridad normalizados se limita a marcadores de corto alcance. En marcadores con un alcance de varios metros, la energía radiada por el lector no es suficiente para alimentar las numerosas puertas necesarias con miras a cumplir funciones criptográficas de seguridad.

Según [b-CRYPTREC], se necesitan 6~13 K puertas para aplicar un algoritmo de encriptación asimétrico, y también un número similar de puertas para aplicar una función hash. Por ejemplo, se requieren 20~30 K puertas para aplicar la norma de encriptación avanzada (AES, *advanced encryption standard*). Está en curso de elaboración un algoritmo de encriptación ligera a efectos de aplicarlo a un marcador RFID. Sin embargo, no se ha facilitado plenamente la creación de un algoritmo de encriptación en un marcador debido a esas limitaciones en los recursos.

## Apéndice II

### Medidas técnicas para proteger la PII en el sistema RFID

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

Se están elaborando diversas tecnologías de protección de la PII para reducir al mínimo la amenaza de invasión de la privacidad en los servicios de aplicación RFID. Se trata en particular de las nuevas tecnologías descritas a continuación dado que la tecnología de encriptación y autenticación actual diseñada para proteger la privacidad no puede aplicarse debido a la limitación de recursos de los marcadores RFID.

#### II.1 Marcador de desactivación con contraseña

Como método más habitual de protección de la privacidad del usuario, esta técnica se basa en que un marcador RFID puede tener una etapa "desactivada" o "activa". En caso necesario, el lector envía la orden "desactivar", incluida una contraseña (32 bits) para desactivar la función del marcador. Sin embargo, el marcador de desactivación sólo se puede utilizar en algunas aplicaciones, puesto que la función de identificación automática, que es la fuerza de la tecnología RFID, no puede utilizarse una vez que la orden de desactivación se ha aplicado. Por ejemplo, si la función del elemento del marcador insertado con un marcador RFID está desactivada tras la compra, su devolución o restitución puede ser imposible dado que no puede recuperarse la historia del producto. Además, el marcador de desactivación no es suficientemente seguro para proteger la PII dado que sólo tiene una contraseña de 32 bits y la funcionalidad de desactivación puede ser vulnerable a un ataque por denegación de servicio en el que el agresor desactiva todos los marcadores que lo rodean.

#### II.2 Protección privada con tecnología física

##### II.2.1 Jaula de Faraday

La jaula de Faraday es una tecnología que impide que el lector de RFID ilegal explore la información del marcador alterando la transmisión de la señal inalámbrica de un lector, utilizando un contenedor fabricado con un material especial que bloquea las emisiones radioeléctricas. Para bloquear la señal inalámbrica, se utiliza una bobina metálica. Pese a tener aplicaciones de utilidad en ciertos ámbitos, la utilización de la jaula de Faraday es relativamente limitada dado que la función de protección de la privacidad se pierde cuando el elemento se retira del contenedor.



X.1275(10)\_FIL1

Figura II.1 – Porta documentos con jaula de Faraday

## II.2.2 Marcador de bloqueo

El marcador de bloqueo es una tecnología elaborada por RSA en 2003. Este marcador RFID especial impide la filtración de la información del marcador causada por los intentos de un lector ilegal de perturbar la comunicación de los marcadores vecinos generando una señal sin sentido. Por ejemplo, un marcador RFID contiene un bit especial asignado como "público" o "privado". Para el elemento de suministro médico insertado en este marcador, el bit especial se fija a "público" antes de su venta, pero se cambia a "privado" en el momento de la compra. Cuando el elemento de suministro médico con un marcador "privado" se inserta en un contenedor utilizando un marcador de bloqueo, éste fija la información del marcador a "privado", con lo cual no puede ser leído por otros; de esta forma, se protege la privacidad del comprador.

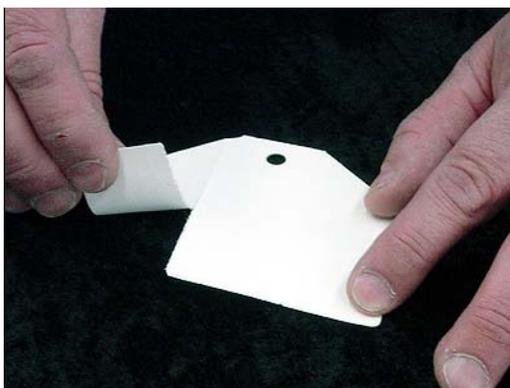
## II.2.3 Interferencia activa

La interferencia activa perturba el funcionamiento de todos los lectores RFID situados cerca del dispositivo, utilizando un dispositivo que emite una onda de gran interferencia. De esa forma, esta tecnología impide la filtración de información personal dado que bloquea la información del marcador RFID.

Cabe señalar que el marcador de bloqueo y la interferencia activa son tecnologías simples que pueden utilizarse fácilmente para lanzar ataques de denegación de servicio. Además, es posible ofrecer soluciones sólo a nivel de usuario y no soluciones que puedan integrarse en el servicio RFID.

## II.2.4 Marcador fragmentado

El marcador fragmentado, creado por IBM para compensar las deficiencias de la instrucción de desactivación, acorta la distancia de comunicación de un marcador suprimiendo parte de la línea de conexión de la antena situada dentro de un marcador. Se puede disminuir al mínimo la posibilidad de violación de la privacidad mediante el rastreo de localización desde un sitio remoto reduciendo considerablemente la distancia de la información y manteniendo al mismo tiempo inalterable la función de almacenamiento de información de un marcador.



X.1275(10)\_FII.2

**Figura II.2 – Marcador fragmentado**

## II.2.5 RFID zapper

El RFID zapper fue presentado en el Chaos Communication Congress de 2005. Se trata de un dispositivo electrónico que puede desactivar permanentemente los marcadores RFID pasivos. El RFID zapper está diseñado para no dañar los dispositivos a que pueden estar anexos los marcadores RFID, contrariamente a otros métodos como la interferencia activa y el marcador fragmentado.

## II.3 Protección de la privacidad mediante una tecnología criptográfica

A continuación se presentan soluciones que utilizan protocolos criptográficos ligeros para ofrecer una mejor seguridad y protección de la privacidad al nivel del marcador. Las soluciones propuestas aún no están lo suficientemente maduras para poder utilizarse eficazmente en una aplicación real, pero es un tema que se está investigando mucho. Aunque hoy en día no sean aplicables, las soluciones propuestas dan una buena idea de cómo serán las soluciones del futuro. Es probable que estos protocolos exijan la modificación de los actuales protocolos de radiocomunicaciones normalizados [b-ISO/CEI 14443], [ISO/CEI 18000] o estudios en EPCGlobal.

### II.3.1 Bloqueo por troceo

Siendo uno de los métodos representativos de la tecnología criptográfica, el bloqueo por troceo (*hash lock*) transmite la información del marcador al lector autorizado y la base de datos auxiliar basándose únicamente en la dificultad de calcular una función inversa de una función de troceo unidireccional. Como se describe en detalle en la figura II.3, sólo se proporciona metaID en respuesta a la petición de información del marcador del lector, que luego se transmite a un lector tras verificar la información de autenticación legalmente obtenida por el lector a partir de la base de datos auxiliar. Sin embargo, este método plantea el problema de que se puede rastrear el usuario puesto que un metaID es un valor estadístico y podría haber sido utilizado como un identificador de marcador.

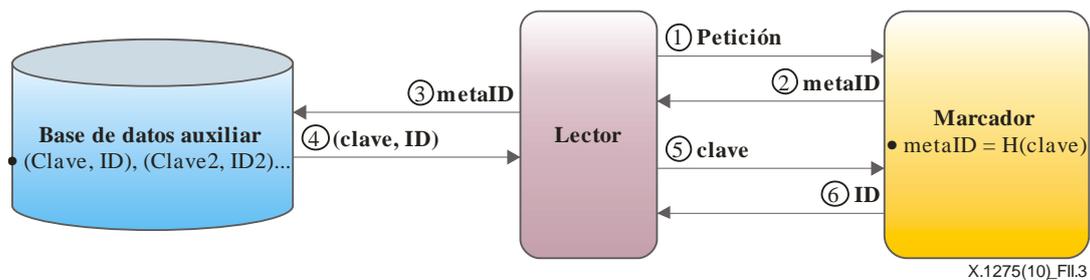


Figura II.3 – Bloqueo por troceo

La técnica de bloque por troceo aleatorizada es uno de los métodos propuesto para resolver el problema del rastreo del usuario en la técnica actual de bloque por troceo. Como se describe en detalle en la figura II.4, esta técnica puede impedir el rastreo creando un marcador que genera un valor diferente cada vez que se accede a la información del marcador, utilizando un generador de números aleatorios con una función de troceo. Aunque han sido propuestas otras técnicas basadas en una función de troceo, como la cadena de troceo, se ha comprobado su falta de practicidad [b-Weis].

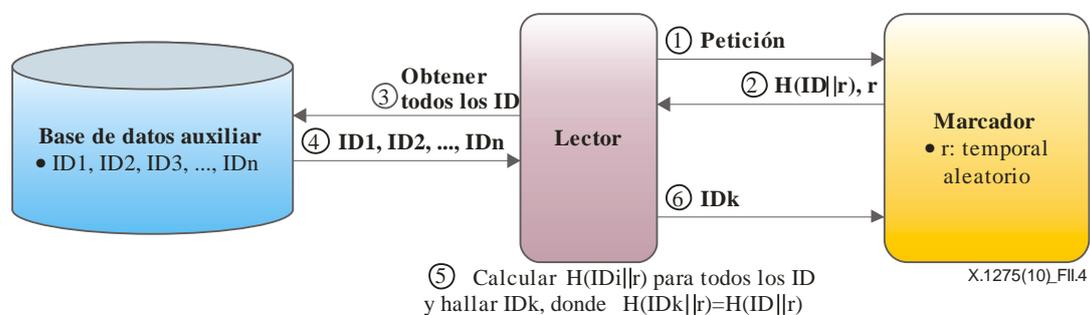


Figura II.4 – Bloqueo por troceo aleatorizado

### III.3.2 Reencipción

El método de reencipción sólo autoriza a la base de datos auxiliar o al lector con la clave pública de la base de datos auxiliar a recopilar la información del marcador, dado que la base de datos auxiliar o el lector legales encriptan periódicamente el identificador del marcador con la clave pública y guardan la información generada en un marcador. El protocolo de reencipitación se basa en ElGamal y consiste en dos fases. En un primer momento, la base de datos auxiliar genera C utilizando su clave pública y un número aleatorio, y guarda C en un marcador. La segunda fase se describe detalladamente en la figura II.5.

Este método se puede aplicar a una nota de valor elevado. Una vez que se emplea este método, la encriptación periódica impide el rastreo de la información del marcador RFID. Sin embargo, existe la amenaza de filtración de la información por escuchas telefónicas durante la transmisión de clave pública dado que se utiliza un método de encriptación de clave pública. Por otra parte, los métodos basados en la encriptación de clave pública, como la reencipción, no pueden aplicarse a un marcador pasivo de bajo precio utilizando la tecnología actualmente disponible.

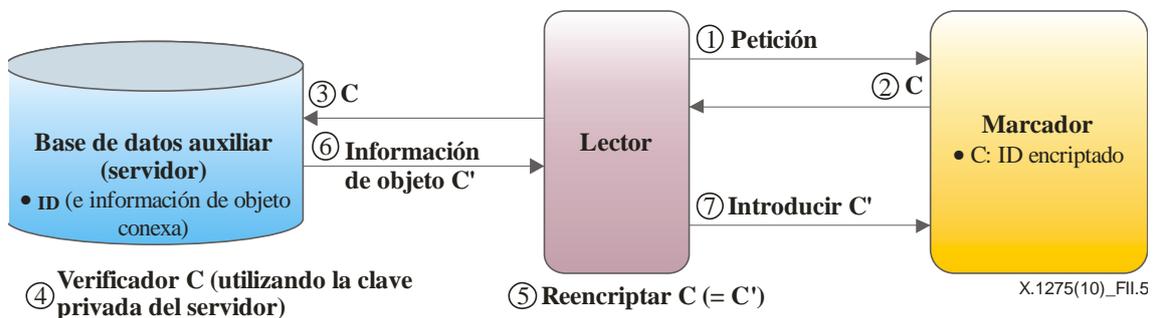


Figura II.5 – Reencipitación

## Bibliografía

- [b-Council of Europe] Consejo de Europa, "*Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*", 1981. <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>
- [b-CRYPTREC] Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", marzo de 2003, Information-technology Promotion Agency of Japan.
- [b-DSTI/ICCP] "*RFID, OECD Policy Guidance, A Focus on Information Security and Privacy, Applications, Impacts and Country Initiatives*", Reunión ministerial de los países de la OCDE sobre el futuro de la economía de Internet, Seúl, Corea, 17-18 de junio de 2008.
- [b-EC1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Boletín Oficial L 281, 1995. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf)
- [b-EC2] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>
- [b-EPIC] Electronic Privacy Information Center, "*Guidelines on Commercial Use of RFID Technology*", julio de 2004.
- [b-E-Zpass] <http://www.ezpass.com/static/info/howit.shtml>
- [b-ICAO] ICAO, Doc 9303, *Machine Readable Travel Documents*, Part 1 Volume 2, 6th edition 2006.
- [b-IPC] Information and Privacy Commissioner/Ontario, "*Privacy Guidelines for RFID information Systems (RFID Privacy Guidelines)*", junio de 2006.
- [b-Isamu Y] Isamu Y., Shinichi S., Akira I. y Satoshi I., "*Secure Active RFID tag System*", 7th International Conference on Ubiquitous Computing, septiembre de 2005.
- [b-ISO 22307] ISO 22307:2008, "*Financial services – Privacy impact assessment*", agosto de 2008.
- [b-ISO/IEC 14443] ISO/IEC 14443:2008, Identification cards – Contactless integrated circuit cards – Proximity cards.
- [b- Japan] MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Government of Japan, "*Guidelines for Privacy Protection with Regard to RFID Tags*", julio de 2004.
- [b-Juels] Juels, A., Rivest, R.L. y Szydlo, M., "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*", ACM Conference on Computer and Communications Security, 2003.
- [b-Junichiro] Junichiro Saito, Jae-Cheol Ryou y Kouichi Sakurai, "*Enhancing privacy of Universal Re-encryption scheme for RFID tags*", Embedded and Ubiquitous Computing 2004.

- [b-Korea] MIC (Ministry of Information and Communication) of Korea, "*RFID Privacy Protection Guideline*", julio de 2005.
- [b-NIST] NIST SP 800-98, "*Guidance for Securing Radio Frequency Identification (RFID) Systems*", septiembre de 2007.
- [b-OECD] OECD, "*Guideline on the Protection of Privacy and Transborder Flows of Personal Data*", 1980.
- [b-Peris-Lopez] Pedro Peris-López y otros, "*M<sup>2</sup> AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*", 3rd International Conference on Ubiquitous Intelligence and Computing, septiembre de 2006.
- [b-PIA Canada] Treasury Board of Canada Secretariat, "*Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*", 2002.  
[http://www.tbs-sct.gc.ca/pubs\\_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp](http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp)
- [b-PIA Korea] MIC (Ministry of Information and Communication) of Korea, "*Privacy Impact Assessment Guideline for Private Sector*", diciembre de 2005.
- [b-Simon L1] Simson L. Garfinkel, Ari Juels y Ravi Pappu, "*RFID Privacy: An Overview of Problems and Proposed Solutions*", IEEE Security and Privacy, 2005.
- [b-Simon L2] Simson L. Garfinkel y Beth Rosenberg, "*RFID: Applications, Security, and Privacy*", Addison-Wesley Professional, julio de 2005.
- [b-ACNUR] Asamblea General de las Naciones Unidas, "*Principios rectores sobre la utilización de ficheros computadorizados de datos personales*", 1990.  
[http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08\\_PDF/G9010708-pdf](http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08_PDF/G9010708-pdf)
- [b-Weis] S. Weis y otros, "*Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems*", Security and Pervasive Computing 2003.



## 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
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
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