Análisis de Seguridad y Privacidad para Sistemas EPC-RFID en el Sector Postal

Joan Melià-Seguí [†], Jordi Herrera-Joancomartí [‡] y Joaquín García-Alfaro [†,‡]

***Resumen*—Mejorar la seguridad y privacidad en instalaciones RFID con etiquetas de bajo coste está centrando la atención de distintos trabajos de investigación gracias a la progresiva adopción de esta tecnología por parte de las empresas del negocio minorista. Aparte del sector minorista, otras industrias del sector logístico, como las empresas de servicios postales, están introduciendo la tecnología RFID para aportar mejoras en sus procesos. Este artículo se centra en las implicaciones de seguridad y privacidad en la implantación de la tecnología EPC RFID en el sector postal. Se define un contexto de amenazas específico para el sector postal y se proponen medidas para mejorar la seguridad y privacidad en las implementaciones actuales de RFID.**

***Palabras Clave*—RFID, EPC, postal, análisis de amenazas, seguridad, privacidad.**

I. Introducción

La identificación por Radiofrecuencia (RFID) con etiquetas electrónicas de bajo coste (*Low-cost tags*, en inglés) se está convirtiendo en una tecnología de éxito para incrementar la eficiencia y la productividad en el sector logístico. En la medida en que el precio de las etiquetas está bajando, los departamentos logísticos de las empresas están prestando mayor atención a la posibilidad de integrar esta tecnología en los procesos de negocio, con el objetivo de mejorar la visibilidad y la precisión de las operaciones logísticas [1].

El despliegue de la tecnología RFID está adquiriendo importancia gracias a la definición del estándar *Electronic Product Code* (EPC) Clase 1 Generación 2 promovido por EPCglobal (http://www.epcglobalinc.org) [2]. La estandarización por parte de EPCglobal cubre la totalidad de la arquitectura RFID, desde la estructura de datos de la etiqueta electrónica a las especificaciones de comunicación por red.

Las etiquetas EPC son vistas por las empresas como la tecnología perfecta para incrementar la visibilidad de sus productos en la cadena de suministro, mejorando de este modo la eficiencia de los procesos logísticos. Desde que Walmart adoptara esta tecnología para sus procesos de suministro, otros líderes de la industra del negocio minorista (*Retail*, en inglés) han seguido los mismos pasos. Precisamente en el momento en que la tecnología EPC está empezando a ser ampliamente usada en el negocio minorista, otras empresas de la industria logística están introduciendo los beneficios de EPC en diferentes sectores empresariales, como por ejemplo las empresas postales. Las estimaciones del mercado global para la RFID en el sector postal son optimistas [3], y en el caso en que el etiquetado a nivel de producto (como por ejemplo las etiquetas de bajo coste de EPC) gane una amplia aceptación, los servicios postales pueden ser la segunda mayor aplicación de la RFID en el mundo tras la cadena de suministro de la venta al pormenor [4].

La información existente sobre implementaciones de RFID en el sector postal es muy escasa. El *Electronics and Telecommunications Research Institute* (ETRI) de Corea del Sur ha desarrollado una aplicación RFID para logística postal, sugiriendo un sistema RFID y una estructura de datos para la etiqueta utilizada en los procesos postales, especialmente para el procesado de paquetería y gestión de palés [5], [6]. China Post ha desarrollado un sistema EPC para el seguimiento de sacos almacenadores de cartas a través de diferentes oficinas y centros de la región de Shanghai [7]. También Correos de España [8], [9] y la compañía postal de Arabia Saudí [10] han mejorado la calidad del servicio gracias al uso de un sistema EPC de seguimeinto de cartas a través de los centros de clasificación y distribución, identificando las zonas donde la entrega de cartas se produce con mayor retraso, permitiendo corregir problemas en los procesos analizados.

Dejando de lado los beneficios potenciales de un sistema de computación ubicua a bajo coste como EPC, esta tecnología implica ciertas desventajas debido a los limitados recursos de computación de las etiquetas de bajo coste. El diseño del sistema EPC se basó en la idea de minimizar el coste por etiqueta (con el objetivo de romper la frontera de 5 céntimos por etiqueta) para hacerlo más atractivo para la industria. Uno de los problemas más destacables de la tecnología EPC es la ausencia de mecanismos de seguridad. Debido a la inseguridad intrínseca asociada a la comunicación inalámbrica, la información de las etiquetas puede ser capturada de forma fraudulenta a varios metros de distancia, revelando el código EPC almacenado en ellas [11], [12].

La principal aportación de este artículo es la definición de un modelo postal RFID, basado en el omnipresente modelo RFID del negocio minorista a lo largo de la cadena de suministro. Este articulo también incluye una definición y clasificación de las amenazas de seguridad y privacidad presentes en el modelo postal de RFID, y una propuesta de soluciones genéricas para las amenazas especificadas.

El resto del artículo se organiza de la siguiente manera. La sección II presenta la metodología usada para construir el modelo postal RFID. La sección III describe las principales amenazas susceptibles en el sistema postal EPC. La sección IV propone un conjunto de medidas de seguridad para el modelo postal EPC propuesto.

[†]Universitat Oberta de Catalunya.
[‡]Universitat Autònoma de Barcelona.

Este trabajo está financiado por el Ministerio de Ciencia y Educación, a través de los proyectos *CONSOLIDER CSD2007-00004* y *TSI2006-03481*, y el programa de becas de la Fundación “la Caixa”.

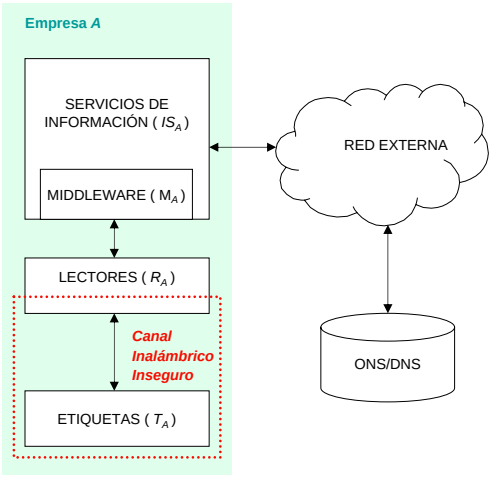

Fig. 1. Red simplificada EPC.

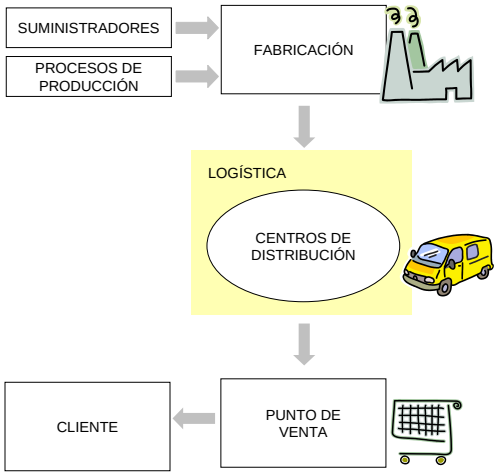

Fig. 2. Ejemplo de aplicación de inicio a fin.

II. Modelo RFID postal basado en el modelo de venta minorista

Como se ha mencionado en la Introducción, el desarrollo de la RFID está creciendo exponencialmente en el sector del negocio minorista debido a la adopción de la tecnología EPC por los líderes de la industria de la cadena de suministro (como Walmart o Metro). Por esta razón, se pueden encontrar en la literatura diferentes propuestas para modelos y ejemplos de implementaciones de EPC [13], [14], [15], [16]. En esta sección, se repasan las propiedades principales del entorno de la venta al detalle, con el objetivo de definir un modelo postal. Dicha identificación nos permite analizar la seguridad del modelo postal de forma similar a como se ha realizado para el entorno de la venta minorista.

Especificado en el estándar [17], un sistema simplificado basado en EPC en una empresa A se puede definir como un conjunto de los siguientes elementos: un conjunto T_A de etiquetas electrónicas y un conjunto R_A de lectores conectados a un middleware M_A y otros sistemas de información IS_A. Además, si es preciso acceder a la información desde el exterior del dominio especificado (empresa A), es necesario habilitar un servidor ONS (Object Name Service). La figura 1 representa el esquema de una red basada en el sistema EPC.

A. Modelo minorista

Walmart se convirtió en un pionero tecnológico cuando solicitó a todos sus suministradores incluir una etiqueta EPC a todos los palés enviados a las tiendas y centros de distribución de la empresa [16]. Galeria Kaufhof (del grupo Metro) ha iniciado un piloto de venta al detalle, siendo la primera aplicación EPC a nivel de producto que incluye el ciclo de inicio a fin [15]. De forma resumida, el circuito se inicia en el proceso de fabricación de la empresa A, cuando la etiqueta electrónica $t \in T_A$ se adjunta a un producto, y finaliza en propiedad del cliente (con la opción de retirar la etiqueta del punto de venta). Como ya han citado algunos autores [13], [14] una aplicación RFID de inicio a fin se puede resumir en cuatro pasos (ver la figura 2).

- Fabricación
- Centros de distribución (logística de entrega)
- Punto de venta
- Cliente

El modelo minorista citado en esta sección se puede clasificar como *open-loop* [18]. Un sistema RFID *open-loop* asume que los objetos etiquetados no vuelven nunca al origen o, si lo hacen, regresan después de un largo periodo de tiempo o para tareas de fin de vida útil del producto. Los objetos etiquetados son habitualmente productos individuales, los cuales quedan permanentemente asociados e identificados para la gestión del ciclo de vida del producto, o aplicaciones de seguimiento y trazabilidad.

Por otro lado también existen sistemas RFID *closed-loop*. Este modelo incluye procesos muy específicos donde los objetos etiquetados son usados o reusados entre un grupo determinado de actores. Casos típicos incluyen el seguimiento de activos reutilizables entre fabricantes y suministradores, como carros de transportes o palés que vuelven continuamente al origen del proceso [19].

B. Modelo Postal

De acuerdo con el modelo minorista, se pretende definir un modelo postal considerando los proyectos y pilotos de EPC RFID actuales, desarrollados por organismos y empresas postales en Corea del Sur, China, Arabia Saudí y España.

El *Electronic and Telecommunications Research Institute* (ETRI) de Corea del Sur ha desarrollado una propuesta de sistema postal RFID incluyendo posibles aplicaciones RFID en el campo de la gestión postal [5], [6]. La propuesta contiene especificaciones para procesado de paqueteria y gestión de palés, una estructura de datos de la etiqueta para procesos postales, y también monitorización en tiempo real y gestión de estadísticas de procesado de paquetería y uso de palés basado en tecnología RFID.

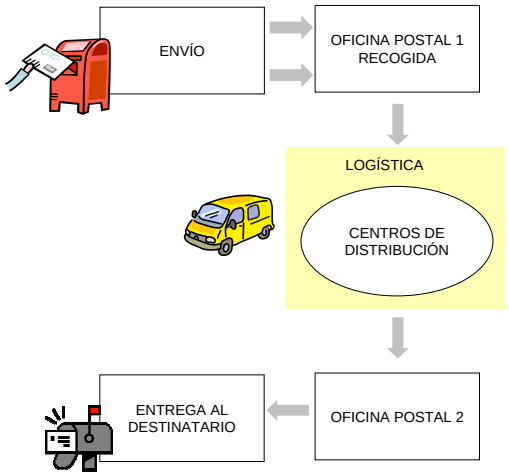

Fig. 3. Modelo Postal RFID.

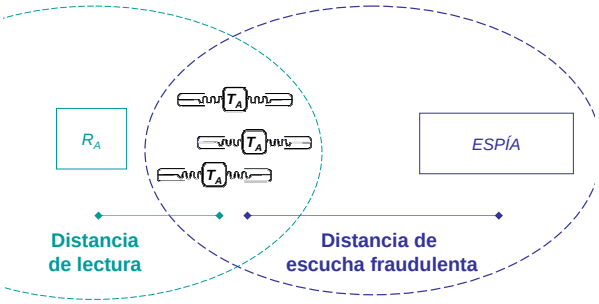

Fig. 4. Canal inalámbrico inseguro de RFID.

Más allá de estas propuestas, algunas empresas postales han dado los primeros pasos desarrollando diferentes aplicaciones con RFID [20]. Es el caso de Correos en España, que ha provisto todos sus centros de distribución (DC) con un sistema EPC para el seguimiento de medidas de calidad de servicio [9]. El sistema funciona de la siguiente manera; usuarios seleccionados dentro del programa de calidad se envían cartas con otros usuarios o oficinas postales de distintas regiones. Estas cartas contienen una etiqueta EPC t_Q y cada región postal está gestionada por un DC en donde se ha implementado un sistema EPC en cada muelle de carga y descarga (lectores y antenas R_Q). Estos lectores recogen la información de los RFIDs y la envian a la aplicación de calidad (incluida en un software middleware M_Q) de un sistema de información IS_Q. Este proceso es constantemente repetido por más de cinco mil cartas etiquetadas, obteniendo un mapa de tiempos de entrega en tiempo real.

Siguiendo con la idea de aplicaciones RFID de inicio a fin, Saudí Post está instalando buzones individuales equipados con una etiqueta EPC (e-boxes) para la mejora de la calidad de servicio y control de la actividad del cartero [10]. El proyecto saudí, como el de Correos y la propuesta del ETRI, pueden ser clasificados como aplicaciones *open-loop* siguiendo un esquema similar.

La figura 3 resume los diferentes pasos de los proyectos RFID citados, definiendo un modelo postal genérico RFID que puede ser aplicado a otras aplicaciones postales. La definición de cada uno de los procesos postales se describe a continuación:

- Envío del cliente: Un usuario envía una carta con etiqueta $t \in T_P$ a cualquier destino. Los carteros pueden ir equipados con un lector móvil RFID R_P o un sistema empotrado en el carrito del correo o en la furgoneta de reparto, para realizar la primera traza RFID. También los buzones pueden incorporar una identificación RFID (un buzón etiquetado o un lector RFID empotrado en el buzón).

- Oficina Postal 1 / Recepción en oficina: La oficina postal es el primero de los puntos por los que pasan las cartas, y donde son clasificadas y distribuidas en un primer nivel (los envíos locales son entregados sin pasar por ningún otro punto adicional). Dependiendo del producto, el usuario puede acudir directamente a la oficina postal donde la carta o el paquete es etiquetado en el proceso de recepción, salt'andose de este modo el paso anterior.

- Centros de distribución (DC): La red de DC's distribuye el tráfico postal de / a toda su región. Cada DC está provisto de un sistema RFID R_P en todas las posibles entradas o salidas, con lo que la ID de la etiqueta, el dia, la hora exacta, y el muelle donde los camiones de transporte están cargando o descargando el correo, son automáticamente registrados por la aplicación que gestiona el sistema RFID M_P.

- Oficina Postal 2: La oficina postal de recepción recibe el correo clasificado y listo para ser entregado por parte del cartero.

- Entrega al destinatario: El cartero entrega el correo a todos los destinatarios. Este es el último punto en el que la empresa postal tiene la oportunidad de hacer el seguimiento del correo mediante RFID (por ejemplo usando un lector móvil R_P). Los buzones también pueden ir provistos de identificación RFID (mediante una etiqueta o un lector incluido en el propio buzón).

A parte del modelo de aplicación que acabamos de describir, existen también aplicaciones postales del modo *closed-loop* donde el objeto a rastrear no son las cartas sino los contenedores de las mismas. Este es el caso de la gestión de sacos almacenadores de cartas de China Post [7] y la gestión de carros de Correos en España [8]. Sin embargo, como veremos más adelante, el modo *closed-loop* es menos succeptible a amenazas de seguridad que el *open-loop* puesto que se desarrolla en entornos más controlados.

Tabla I
CONTEXTO DE AMENAZAS DEL SISTEMA POSTAL RFID.

Contexto	Postal	Modelo	Aplicación
Dentro de la cadena de suministro	Incluye todos los DC, así como el transporte entre ellos y las áreas de clasificación de las oficinas postales.	Centros de distribución	Open-loop & closed-loop
Zona de transición	La zona de la oficina postal donde el correo etiquetado es entregado a / desde el cliente.	Oficina postal 1	Open-loop
		Oficina postal 2	
Fuera de la cadena de suministro	Incluyendo todas las localizaciones externas, especialmente los buzones.	Envío desde el origen	Open-loop
		Entrega al destinatario.	

III. AMENAZAS EN EL MODELO RFID POSTAL

Como todos los sistemas de información, la arquitectura EPC padece amenazas relacionadas con la privacidad y seguridad de la información gestionada por el sistema, más aún considerando que el canal de comunicaciones que utiliza la tecnología RFID es potencialmente inseguro [21], debido a que no se garantiza la confidencialidad de los datos transferidos entre etiquetas y lectores, y no existe autenticación entre etiqueta y lector. Teniendo en cuenta esta problemática, la mayoría de amenazas de seguridad y privacidad en sistemas EPC tendrán por objetivo la interfaz inalámbrica [22], [23]. Este artículo se centra en las principales amenazas relacionadas con la falta de medidas de autenticación y seguridad de las etiquetas EPC [24] y la inseguridad del canal de comunicaciones entre etiquetas y lectores [25] (figura 4), por lo que se asumirá que la comunicación entre lectores y middleware (red cableada) se realiza de forma segura. Para estudios de otros dominios de seguridad se puede ver [22], [23], [26] o [27].

Volviendo al modelo RFID postal, analizamos las amenazas para el sistema EPC postal (definido en la sección II) en base a la experiencia y a la literatura publicada sobre el negocio minorista. En [28] los autores han definido los tres principales contextos para las etiquetas EPC basados en el sector minorista: *Dentro de la cadena de suministro*, *zona de transición* y *fuera de la cadena de suministro*. En la tabla I se definen los contextos mencionados basados en el modelo postal y la clase de aplicación.

Las amenazas se seguridad y privacidad en los sistemas EPC en el modelo de cadena de valor, han sido analizados por diferentes autores ([29], [21], [28]). La figura 5 representa una adaptación de las amenazas detectadas para el sector minorista, al modelo postal basado en el contexto de amenazas de [28] y el modelo postal definido en la sección II. En este diagrama también podemos observar que las aplicaciones *closed-loop* son menos susceptibles a las amenazas que los *open-loop*. La siguiente lista es un conjunto de amenazas activas y pasivas que aplican a la cadena postal RFID:

- Suplantación: Amenaza que responde a la intención del atacante de falsear su identidad (o la de sus recursos) por la de un usuario legítimo del sistema, con el objetivo de vulnerar la autenticación. En el caso de la RFID, un equipo lector ilegítimo dentro de la cadena postal, podría suplantar a uno de legítimo, obteniendo fraudulentamente información del sistema. Puesto que el sistema EPC no dispone de mecanismos de autenticación, el atacante no encontrará ninguna dificultad para conseguir la misma información que podría obtener un usuario dentro del sistema. Esta amenaza es especialmente relevante debido a que la información almacenada en el código EPC puede revelar información importante sobre el usuario como su código de cliente, el código postal o el valor del envío, así como las estrategias de la empresa postal[22], [23]. Un ejemplo de esta amenaza sería un ataque *man-in-the-middle* (MitM o intermediario, en castellano) en el que con la ayuda de un lector compatible EPC se explota la ausencia de autenticación segura entre etiqueta y lector (R_A y T_A) para vulnerar el proceso de la cadena postal.

- Manipulación: Tiene como objetivo vulnerar la integridad de un objeto, en el caso de la RFID, modificando la información almacenada en la memoria de la etiqueta $t \in T_A$. Manipulando los datos almacenados en una etiqueta EPC se podría conseguir la falsificación de los productos en el propio proceso postal. Clonar la identidad de un envío postal es un ejemplo de esta amenaza.

- Denegación de Servicio (DoS): Amenaza que tiene por objetivo limitar la disponibilidad del servicio. Por ejemplo, un atacante puede usar un lector RFID para transmitir una señal interferente con el objetivo de inhabilitar los canales de RF, o incluso desactivando permanentemente el funcionamiento de las etiquetas electrónicas con la opción *kill* facilitada por el estándar

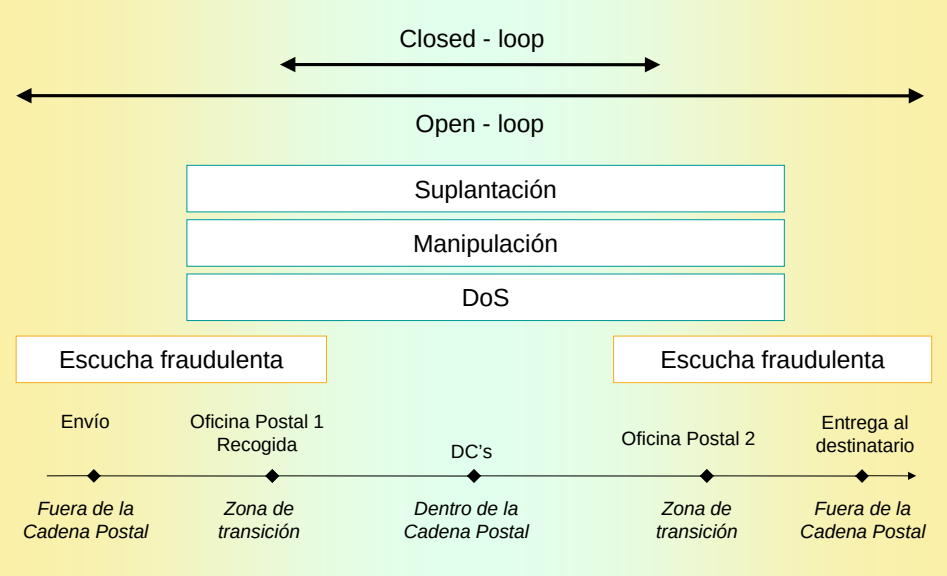

Fig. 5. Modelo de amenazas propuesto para EPC postal.

[2].

- Escucha fraudulenta o revelación de información: Como se ha comentado en secciones previas, el canal de comunicación entre lectores R_A y etiquetas T_A es fácilmente accesible dada la inseguridad del canal inalámbrico, con lo que la confidencialidad del servicio es fácilmente vulnerable. El escaneo ilegítimo de la comunicación se puede realizar simplemente usando un lector RFID compatible. Amenzas a la privacidad personal como seguimiento (en inglés, *tracking*) y análisis de perfiles y preferencias (en inglés, *profiling*/*clustering*) están incluidas en esta categoría [28].

Por otro lado, los buzones o incluso las cartas etiquetadas pueden sufrir ataques físicos como el robo de la etiqueta, su desactivación o la substitución por una nueva. Esta amenaza solo es posible en entornos no controlados, como fuera de la cadena de suministro, donde se produce el envío o la entrega al destinatario. No se incluye en el análisis por tratarse de una amenaza que requiere una acción física, por lo que serían necesarias soluciones alternativas para esta amenaza fuera del campo de estudio de este artículo.

IV. Medidas de seguridad para el modelo RFID postal

Las aplicaciones RFID para el sector postal se encuentran en un estado inicial comparado con el sector minorista y por este motivo no se han desarrollado análisis de seguridad en este campo, si bien ya hemos visto que aplicaciones postales con RFID están siendo implementadas actualmente.

Centrándonos en el análisis de amenazas por contexto definido en la sección III, observamos que el servicio postal de categoría *open-loop* está más expuesto a riesgos de privacidad y seguridad. Como se puede observar en la figura 5, los procesos de interacción entre usuario y oficina postal (al principio y al final de la aplicación) se encuentran fuera de la cadena de suministro y en la zona de transición, por lo que son los que más riesgo entrañan desde el punto de vista de la seguridad y la privacidad.

La literatura relacionada con la seguridad de sistemas RFID con etiquetas de bajo coste, ofrece soluciones de mejora de seguridad modificando los protocolos de comunicaciones [30] o las características del chip del estándar C1G2 [2], [31]. La implementación de estas propuestas no son viables en las instalaciones actuales de EPC porque las modificaciones de los protocolos o las características del chip no siguen el estándar EPC Class 1 Gen 2. Incluso las soluciones que requieren un número de puertas lógicas disponible en el encapsulado actual tampoco son implementables puesto que también requerirían una modificación del estándar.

En los siguientes apartados se enumeran un conjunto de soluciones actuales y propuestas para el modelo postal EPC que sí son implementables puesto que no requieren la modificación del estándar. Para analizar la idoneidad de estas medidas, se utilizará el escenario postal definido en la sección II, y específicamente las amenazas por contexto decritas en la

tabla I y la figura 5.

A. *Medidas de seguridad presentes en la tecnología EPC*

EPCglobal facilita una opción de seguridad en la propia etiqueta conocida como **kill command** [2]. Activable con un password de 32 bits, este comando desactiva el funcionamiento de la etiqueta de forma permanente. Esta utilidad soluciona amenazas como *escuchas fraudulentas* pero elimina cualquier opción de ofrecer servicios de postventa al cliente. Además, las etiquetas pueden ser desactivadas en el momento de la entrega al cliente, pero no antes (incluyendo el contexto closed-loop, donde amenazas como *manipulación* y *suplantación* son posibles), porque todas las características de seguimiento y trazabilidad se perderán. Del mismo modo, esta solución no se adapta a las amenazas por *DoS* porque el resultado deseado es desactivar el funcionamiento de la etiqueta electrónica, que es precisamente la función del comando *kill*. Resumiendo, dada la singularidad del modelo RFID postal, las etiquetas estarán expuestas fuera de la cadena postal tanto al principio como al final del envío (ver la figura 3), por lo que la desactivación total no es una medida adecuada para la mejora de la seguridad y la privacidad en el sector postal.

Adicionalmente el estándar también contempla una contraseña de acceso (Access password en inglés) [2] también de 32 bits que activado, bloquea la escritura en la memoria de la etiqueta. Esta medida puede solucionar amenazas de *manipulación* si el atacante no conoce la contraseña.

B. *Medidas de seguridad implementables a alto nivel*

Las siguientes aproximaciones a soluciones de seguridad y privacidad para RFID han sido propuestas en diferentes publicaciones [32], [33], [28], [29] y en este apartado se evalua su idoneidad para el modelo postal.

- La reescritura de la ID o cifrado es el concepto de medidas como *ID relabeling* o *encryption* usados en [32], [33], [28], [34], [35]. Estas soluciones aprovechan la posibilidad de escritura múltiple de la etiqueta para evitar amenazas como *escuchas fraudulentas* o *suplantación*. Ambas soluciones responden a la misma idea: enlazar en un base de datos segura la ID real de la etiqueta y un *pseudo ID* que puede ser un simple pseudónimo o un valor cifrado del mismo ID. Como las tareas de cifrado se realizan en el IS, la única restricción en términos de elegir el algoritmo de cifrado es la potencia del servidor en donde la tarea vaya a ser realizada. Una vez que el pseudónimo ya se ha calculado, se escribe en la memoria de la ID de la etiqueta[1], y el pseudónimo y la ID real son ambos guardados en una base de datos segura a la que el resto del sistema pueda acceder. Esta medida no soluciona un posible ataque de *manipulación* al final de la cadena postal, o en contextos donde las etiquetas no se reescriben. La *DoS* no se soluciona con esta medida, porque las etiquetas perderían toda su funcionalidad.

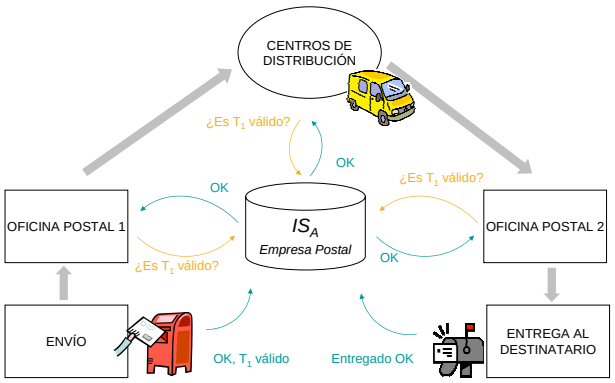

Fig. 6. Modelo del TTR.

- El apantallamiento de etiquetas, citado en [29], propone una solución con apantallamiento (por ejemplo una bolsa metálica) para evitar la activación de la respuesta de la etiqueta electrónica. Esta opción es útil para evitar amenazas a lo largo de la cadena postal, pero si el correo circula apantallado en el proceso de distribución ningún tipo de trazabilidad o mecanismo de distribución puede ser realizado. De modo que esta propuesta soluciona amenazas específicas como *escuchas fraudulentas*, *manipulación* y *suplantación*, pero por contra no se puede usar ningún tipo de sistema RFID a lo largo de la cadena postal. Esta medida no aplica a *DoS* porque incluso asegurando la funcionalidad del sistema, el apantallamiento no ofrece la oportunidad al sistema de leer el contenido de la etiqueta.

- La interferencia activa de señales de RF citado en [29] consiste en ocupar los canales útiles de RFID mediante el uso de un transmisor (un caso de *DoS* intencionado), de este modo acciones como *escuchas fraudulentas* o *suplantación* pueden ser evitadas en las cercanías del punto de control. Aplicar esta medida significa la pérdida del seguimiento de los productos en el entorno de la interferencia activa, por lo que implementaciones como las propuestas en [9], [5] o [15] no se pueden llevar a cabo. Amenazas como *manipulación* no se solucionan con esta medida, si consideramos que la interferencia activa no puede ser realizada ubicuamente. Esta medida no es aplicable para *DoS*.

- Trusted Tag Relation (TTR) se basa en el concepto de una configuración mediante pasos de confianza. Siguiendo la idea de [36] una etiqueta $t \in T_A$ es validada por un agente autorizado al principio del proceso postal (por ejemplo la propia empresa postal

[1]Este proceso se puede realizar en cada punto de lectura, pero las funciones de escritura requiren sensiblemente más tiempo que únicamente lectura [2], por lo que no todos los puntos de control pueden realizar esta acción (por ejemplo, lectores dedicados a tareas de distribución, o escaneando el contenido de un camión descargándose, necesitan escanear una gran cantidad de etiquetas en muy poco tiempo).

Tabla II
SOLUCIONES PARA AMENAZAS DEL MODELO POSTAL RFID.

Medidas de seguridad	**Amenazas en el modelo postal**			
	Escucha fraudulenta	DoS	Manipulación	Suplantación
Kill	-		-	-
Apantallamiento	-		-	-
Interferéncia activa	-		-	-
Reescritura / cifrado de ID	X		-	X
TTR			X	
PSR		X	X	
MAC			X	
(-) Resuelve una amenaza específica, pero no es aplicable al modelo postal. *(X) Resuelve la amenaza y es compatible con la implementación RFID postal.*				

A) mediante el escaneo de la carta con un lector RFID móvil R_A conectado al sistema de información IS_A, y marcando el estatus de *válido* (ver figura 6) en una base de datos del IS_A. Los siguientes pasos confiarán en la información de la etiqueta t solo si en el paso anterior se ha validado la integridad de la información almacenada en t. Esta medida ayuda a identificar más facilmente acciones de *manipulación*, si bien no es válida para casos de *escuchas fraudulentas* o *suplantación* porque no se modifica la t_{ID} en todo el proceso. Tampoco soluciona escenarios de *DoS* porque los lectores no podrían trabajar correctamente.

- Printed Support Redundancy (PSR) es una medida de seguridad física, que puede considerarse una copia de seguridad de la ID en la misma etiqueta. La idea pasa por imprimir la información de la ID de la etiqueta t_{ID} en la propia etiqueta (únicamente si está protegido por un sobre o no tiene visibilidad directa, para no revelar información visualmente) codificado en formato de código de barras o similar. Esta copia de seguridad ofrece la oportunidad de comprobar si la información t_{ID} es correcta, o incluso recuperar la ID si la etiqueta está dañada o desactivada [2]. Esta solución es la única que puede ofrecer la información de la etiqueta en un caso de *DoS*, pero también es válido para amenazas de *manipulación* (comparando la t_{ID} con la información impresa). *Escuchas fraudulentas* o *suplantación* no se solucionan con esta medida por los mismos motivos que en TTR.

- ID con *message authentication code* consiste en concatenar una ID reducida, con un código de autentificación del ID con el objetivo de mejorar la integridad de la información almacenada en la etiqueta. Si se supone que nuestra cadena postal necesita sólo 50 bits de información (equivalente a más de un millón de combinaciones por habitante en España) para determinar la ID de la etiqueta electrónica, los 46 bits restantes (en el caso de EPC C1G2) pueden ser usados para proteger el contenido de la ID principal, y detectar posibles casos de *manipulación*. La utilización de una función *hash* con una clave k que solo conoce la empresa postal puede ser un sistema para la obtención del código de autentificación. De esta manera la ID final sería el resultado de concatenar la ID original, con el resultado de aplicar una función *hash* con clave k a la suma *XOR* de k y ID_{50bits}:

$$ID_{96bits} = ID_{50bits} | H_k(ID_{50bits} \oplus k)_{46bits}$$

El cálculo se realizaría en IS_A o en R_A, y el resultado se almacenaría en la ID de la etiqueta. Es importante resaltar que un ataque de fuerza bruta (dada la limitación de bits marcada por la ID de la etiqueta) acabaría revelando k y por tanto daría la oportunidad al atacante de manipular la ID de las etiquetas con un MAC correcto. Utilizar una gran diversidad de contraseñas (en función del producto postal, código postal, ciudad de destino, fecha de envío, etc...) puede mejorar la integridad de los datos del sistema.

Los análisis de seguridad de las secciones IV-A y IV-B se resumen en la tabla II. Esta tabla muestra la idoneidad de las soluciones presentadas para cada amenaza dentro de los contextos de RFID postal.

V. CONCLUSIÓN

Como resultado de la incorporación masiva de la tecnología RFID en la lógistica de la cadena de suministro, se han considerado y analizado amenazas relativas a la seguridad y la privacidad para detectar los puntos débiles de los sistemas RFID, intentando conseguir mejoras mediante propuestas de seguridad y privacidad. La previsión optimista de adopción de la tecnología RFID por parte del sector postal abre un nuevo campo para el análisis de la seguridad y privacidad basado en la singularidad del modelo postal.

En este artículo, se han analizado implementaciones actuales de tecnología EPC para el entorno postal, definiendo un modelo postal basado en la existencia de literatura científica e implementaciones reales. Además se han trasladado al modelo postal los análisis de seguridad existentes para el sector minorista, obteniendo cuatro amenazas principales: escuchas fraudulentas, DoS, manipulación y suplantación. Finalmente,

se han analizado medidas de seguridad actuales con el objetivo de determinar su aplicabilidad en el entorno postal.

Las medidas de seguridad actuales se centran en resolver amenazas específicas (ataques pasivos como escuchas fraudulentas o acciones de suplantación) pero solo medidas relacionadas con *reescritura de la ID* o *cifrado* pueden ser aplicadas en determinados casos al modelo postal de RFID dado la singuralidad de la cadena postal, y la necesidad de mayor tiempo para la escritura que para la lectura de las etiquetas. Finalmente se proponen tres medidas de seguridad para detectar ataques de *manipulación* relacionadas con el modelo postal, o incluso recuperar la información de las etiquetas en situaciones de *DoS*. Las soluciones propuestas pueden ser usadas de forma separada o en combinación dependiendo de el contexto en el que se apliquen.

Las líneas futuras de investigación a desarrollar se centran en identificar problemas concretos de seguridad al inicio de la cadena postal, en donde el sistema es más vulnerable, y encontrar soluciones que no requieran una modificación de la tecnología actual para poder ser implementadas en proyectos actuales.

REFERENCIAS

[1] Motorola, "RFID technology and EPC in retail," http://symbol.com/products/whitepapers/rfid_and_epc_in_retail.html, White Papers, 2004, web document.

[2] EPCglobal, "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860-960 MHz," http://www.epcglobalinc.org/standards/, Tech. Rep., 2005.

[3] U. P. U. (UPU), "A market hungry for chips," http://www.upu.int/union_postale/2007/en/3-4.html, Tech. Rep., 2007.

[4] IDTechEx, "RFID for postal and courier services 2007-2017," http://www.idtechex.com/products/, Tech. Rep., 2007.

[5] J.-H. Park, J.-H. Park, and B.-H. Lee, "RFID application system for postal logistics," *Management of Engineering and Technology, Portland International Center for*, pp. 2345–2352, june 5-9 Aug. 2007.

[6] Y. Choi, J. Won, and J. Park, "An experimental testbed for parcel handling with RFID technology," *Advanced Communication Technolgoy - ICACT*, vol. 1, no. 20-22, p. 6pp, february 2006.

[7] R. Journal, "China post deploys EPC RFID system to track mail-bags," http://www.rfidjournal.com/article/articleprint/2487/-1/1/, Tech. Rep., 2006.

[8] Sybase, "Correos, the spanish postal service," http://www.ianywhere.com/success_stories/spanish_post.html, Tech. Rep., 2006.

[9] R. Journal, "Spain's post office improves delivery speed," http://www.rfidjournal.com/article/articleprint/3209/-1/1/, Tech. Rep., 2006.

[10] M. B. Anzzan, *Saudi Post RFID Implementations*, Saudi Post, www.upu.int, 2007, presentation on-line.

[11] K. Deeb, "Efficiency, privacy and security analysis of ubiquitous systems in the retail industry," *Innovations in Information Technology*, pp. 1–6, November 2006.

[12] W.-M. S. Inc., "Help: Electronic product code (EPC)," http://www.walmart.com, Tech. Rep., 2007.

[13] J. Sounderpandian, R. V. Boppana, S. Chalasani, and A. M. Madni, "Models for cost-benefit analysis of RFID implementations in retail stores," *Systems Journal, IEEE*, vol. 1, no. 2, pp. 105–114, Dec. 2007.

[14] G. Roussos, "Enabling RFID in retail," *Computer, IEEE*, vol. 39, no. 3, pp. 25–30, March 2006.

[15] R. Journal, "Metro group's galeria kaufhof launches UHF item-level pilot," http://www.rfidjournal.com/article/articleprint/3624/-1/1/, Tech. Rep., 2007.

[16] ——, "Wal-mart opts for EPC class 1 v2," http://www.rfidjournal.com/article/articleprint/641/-1/1/, Tech. Rep., 2003.

[17] EPCglobal, "The EPCglobal architecture framework," http://www.epcglobalinc.org/standards/, Tech. Rep., 2007.

[18] P. Schmitt, F. Michahelles, and E. Fleisch, *An adoption Strategy for an Open RFID Standard*, 1st ed., Auto-ID Labs, www.autoidlabs.com, september 2005, withe Paper - Business Processes & Applications.

[19] E. Flelsch, J. Ringbeck, S. Stroh, C. Plenge, L. Dittmann, and M. Strassner, *RFID - The Opportunity for Logistics Service Providers*, 1st ed., Auto-ID Labs, www.autoidlabs.com, september 2005, witeh Paper Series.

[20] B. Oztaysi, S. Baysan, and P. Dursun, "A novel approach for economic-justification of RFID technology in courier sector: A real-life case study," *RFID Eurasia, 2007 1st Annual*, pp. 1–5, 5-6 Sept. 2007.

[21] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *International Conference on Security in Pervasive Computing – SPC 2003*, ser. Lecture Notes in Computer Science, D. Hutter, G. Müller, W. Stephan, and M. Ullmann, Eds., vol. 2802. Boppard, Germany: Springer-Verlag, March 2003, pp. 454–469.

[22] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Analysis of threats to the security of EPC networks," *Sixth Annual Communication Networks and Services Research (CNSR) Conference, IEEE Computer Society, Halifax, Nova Scotia, Canada*, May 2008.

[23] ——, "Security threats on EPC based RFID systems," *5th International Conference on Information Technology: New Generations (ITNG 2008), IEEE Computer Society, Las Vegas, Nevada, USA*, April 2008.

[24] D. R. Thomson, N. Chaudhry, and C. W. Thompson, "RFID security threat model," *Conference on Applied Research in Information Technology*, 2006.

[25] D. C. Ranasinghe and P. H. Cole, "Confronting security and privacy threats in modern RFID systems," *Signals, Systems and Computers, 2006. ACSSC '06. Fortieth Asilomar Conference on*, pp. 2058–2064, Oct.-Nov. 2006.

[26] D. S. Kim, T.-H. Shin, and J. S. Park, "A security framework in RFID multi-domain system," *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pp. 1227–1234, 10-13 April 2007.

[27] B. Fabian and O. Gnther, "Security challenges of the EPC network," *To appear in Communications of the ACM*, 2008.

[28] S. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy IEEE*, vol. 3, no. 3, pp. 34–43, May/June 2005.

[29] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in *11th IFIP International Conference on Personal Wireless Communications*, ser. Lecture Notes in Computer Science, vol. 4217. Springer-Verlag, September 2006, pp. 159–170.

[30] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication - a review of RFID product authentication techniques," Printed handout of Workshop on RFID Security – RFIDSec 06, Ecrypt, Graz, Austria, July 2006.

[31] D. Ranasinghe, D. Engels, and P. Cole, "Low-cost RFID systems: Confronting security and privacy," in *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

[32] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, february 2006.

[33] K. H. Wong, P. C. Hui, and A. C. Chan, "Cryptography and authentication on RFID passive tags for apparel products," *Computers in Industry*, vol. 57, no. 4, pp. 342–349, May 2006.

[34] S. Weis, S. Sarma, and D. Engels, "RFID systems and security and privacy implications," in *Cryptographic Hardware and Embedded Systems – CHES 2002*, ser. Lecture Notes in Computer Science, B. Kaliski, c. Kaya ço, and C. Paar, Eds., vol. 2523. Springer-Verlag, August 2002, pp. 454–469.

[35] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," Printed handout of Workshop on RFID Security – RFIDSec 06, Ecrypt, July 2006, graz, Austria.

[36] A. Solanas, J. Domingo-Ferrer, A. Martínez-Ballesté, and V. Daza, "A distributed architecture for scalable private RFID tag identification," *Computer Networks, Elsevier*, vol. 51, no. 9, January 2007.