# *Firma Dinámica para personalización RFID mediante protocolo LLRP*

*Firma Dinámica con LLRP*

Alexander Bismark Benitez Antelo
*Postgrado en Informática*
*Universidad Mayor de San Andrés - UMSA*
*La Paz, Bolivia*
alexanderbismark@gmail.com

***Resumen*— La implementación de la Tecnología RFID como herramienta para el seguimiento y trazabilidad de objetos, permite generar niveles de control e identificación con un nivel de imperceptibilidad elevado, puesto que los dispositivos RFID (Tags / etiquetas) pueden ser embebidos y adheridos en casi cualquier objeto.**

**En los procesos de personalización RFID, se deben aplicar medidas de seguridad que permitan garantizar la autenticidad y trazabilidad de los Tags RFID en todos los puntos de control, siendo que por cada paso se debe registrar el evento e información dentro el dispositivo (Tag RFID). Esta información puede ser compartida con terceros permitiendo extender los criterios de trazabilidad que está vinculada al objeto.**

**Cuando la información contenida en los Tag RFID se encuentra sin protección, se torna susceptible a clonación, lecturas no autorizadas u otras, que pueden violar ciertos niveles de privacidad de las personas que portan el objeto donde se encuentra embebido el Tag RFID, para ello se propone aplicar mecanismos de criptografía para generar una firma digital que cambie dinámicamente por cada punto de control RFID, bajo este objetivo se formula que el nivel de seguridad puede ser incrementado cuando la firma digital es renovada constantemente.**

**Se propone que para el almacenamiento de la firma dinámica se pueda utilizar el protocolo LLRP, mismo que sigue los lineamientos de la EPC Global para la administración RFID (middleware, lectores, tags) en conformidad al estándar EPCIS en Tags RFID Clase 1 Generación 2.**

***Palabras clave*— *RFID, EPC, EPC Global, EPCIS, Criptografía, LLRP, firma digital, firma dinámica, seguridad, RFID Clase 1 Generación 2.***

## I. INTRODUCCIÓN

La identificación por radio frecuencia se ha convertido en uno de los pilares tecnológicos de avanzada para los países que efectúan procesos automatizados de gestión, control y trazabilidad de objetos (identificación, traslado, seguimiento, etc.) [1]. Todos ellos con fines de manejo y seguimiento de documentos de identificación, personas, animales, vehículos y consumibles, que deben ser catalogados e identificados de manera única desde su fabricación, uso y baja.

En el esquema básico la tecnología RFID contiene componentes esenciales: tag o etiqueta, una antena, un lector y un middleware, que permiten interrelacionar y obtener la información asociada al objeto.

Cuando se presenta el evento de identificación por radio frecuencia [2], entiéndase a este evento como la acción de los componentes para intercambio de información y detección por ondas de radio gestionados mediante un middleware RFID, se obtiene la información almacenada en el Tag RFID, esta interacción se muestra en la siguiente figura:

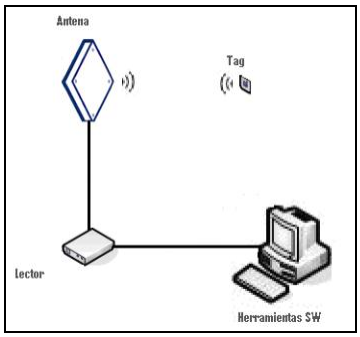


Fig. 1. Componentes básicos de un sistema RFID [3]

## II. OBJETIVO

Proponer mecanismos de personalización de firma dinámica para incrementar la seguridad de la información almacenada en etiquetas RFID

## III. HIPÓTESIS

La implementación de mecanismos de personalización de firma dinámica con criptografía asimétrica mediante protocolo LLRP, permitirá incrementar la seguridad y anti-clonación en etiquetas RFID

RFID: Radio Frequency Identification (Identificación por radio frecuencia) cuyo objetivo es transmitir la identidad por ondas de radio.
EPCIS: Electronic Product Code Information Service (Servicio de información de códigos electrónicos de productos), servicio de información diseñado para el intercambio de información y gestión de trazabilidad para dispositivos RFID
LLRP: Low Level Reader Protocol (Protocolo de lectura de bajo nivel) protocolo estandarizado para gestión de lectores RFID

## IV. ETIQUETAS DE IDENTIFICACIÓN POR RADIO FRECUENCIA - TAGS RFID

Uno de los componentes analizados son los Tags RFID, puesto que conforme la aplicabilidad que se requiera para una implementación se deben considerar algunos aspectos y diferencias como: modo de operación activo / semi-activo / pasivo, frecuencia de operación, distancia de lectura [4], costo unitario de fabricación, capacidad de almacenamiento. Estas variables pueden ser consideradas como primarias, la siguiente figura presenta los rangos de operatividad en frecuencia y familias de Tags RFID, donde se pueden apreciar las diferencias entre las mismas: [1]

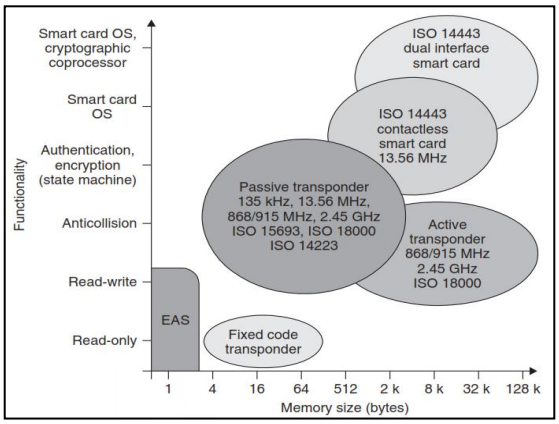


Fig. 2. Clasificación RFID acorde a funcionalidad [3]

Uno de los tipos de Tags Rfid con mayor imposición en el mercado son los Tags RFID Clase 1 Generación 2, que opera en las frecuencias 868 a 925 MHz normado por el estándar ISO 18000-6C o 18000-6B, donde se encuentran los lineamientos de comunicación, intercambio de información y la especificación de los bancos de memoria para este tipo de Tags. Esta operación, se presenta en la siguiente figura:

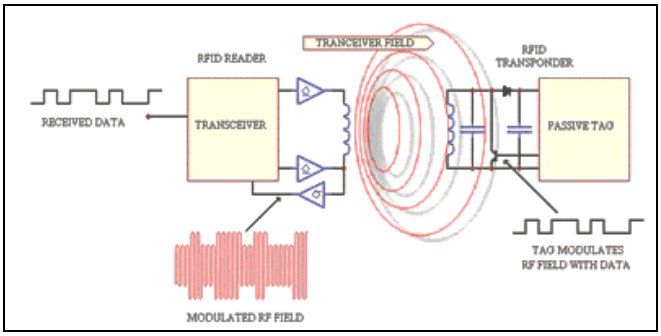


Fig. 3. Diagrama de comunicación RFID Clase 1 Generación 2 [6]

*Bancos de memoria de los Tags RFID Clase 1Gen. 2*

La particularidad más importante de los Tags RFID Clase 1 generación 2, está en su capacidad de personalización puesto que a diferencia otros tiene los siguientes bancos de memoria: TID, EPC, USER, Access password y Kill password y Reservada [5], todas ellas con opciones bloqueo dinámico o bloqueo permanente en el proceso de grabado [6] [7]. Las capacidades estándares de almacenamiento se muestran en la siguiente tabla:

TABLA 8. DISPOSICIÓN DE BANCOS DE MEMORIA

| # Banco | Nombre | Dirección | Numero de Bit | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 10b | TID (ROM) | 10h-1Fh | TID[15:0] | | | | | | | | | | | | | | | |
| | | 00h-0Fh | TID[31:16] | | | | | | | | | | | | | | | |
| 01b | UII (EEPROM) | 70h-7Fh | EPC[15:0] | | | | | | | | | | | | | | | |
| | | 60h-6Fh | EPC[31:16] | | | | | | | | | | | | | | | |
| | | 50h-5Fh | EPC[47:32] | | | | | | | | | | | | | | | |
| | | 40h-4Fh | EPC[63:48] | | | | | | | | | | | | | | | |
| | | 30h-3Fh | EPC[79:64] | | | | | | | | | | | | | | | |
| | | 20h-2Fh | EPC[95:80] | | | | | | | | | | | | | | | |
| | | 10h-1Fh | Protocolo de control de bits[31:16] | | | | | | | | | | | | | | | |
| | | 00h-0Fh | CRC-16 | | | | | | | | | | | | | | | |
| 00b | RESERVED (EEPROM) | 30h-3Fh | Access password[15:0] | | | | | | | | | | | | | | | |
| | | 20h-2Fh | Access password[31:16] | | | | | | | | | | | | | | | |
| | | 10h-1Fh | Kill password[15:0] | | | | | | | | | | | | | | | |
| | | 00h-0Fh | Kill password[31:16] | | | | | | | | | | | | | | | |

## V. SERVICIO DE INFORMACIÓN DE CÓDIGOS DE PRODUCTO ELECTRÓNICO – EPCIS

EPCIS es un estándar de la EPC Global, que permite compartir información de los Tags RFID en base al código del banco de memoria EPC, para garantizar la trazabilidad, fue concebido para compartir información detallada acerca de objetos físicos o digitales entre organizaciones. El estándar EPCIS requiere del uso del EPC (Código Electrónico de Producto) [8] [9] [6], el estándar se aplica a todas las situaciones y eventos que pueden ocurrir con los objetos y su traspaso, por lo tanto el EPC tiene relevancia para efectos de vinculación de acciones asociadas a un código.

*Componentes arquitectónicos del estándar EPCIS*

Los componentes lógicos de esta arquitectura, son modularizados para desacoplar bloques lógicos en busca de la autonomía de procesos que posteriormente bajo el concepto de integración de un todo, pueden orquestar y satisfacer las necesidades de explotación de información en base a los siguientes procesos [4]:

- Identificación: las organizaciones como necesidad esencial requieren clasificar a un objeto o producto de manera univoca asignándole un código de identificación.
- Captura: las organizaciones requieren registrar las acciones y eventos acontecidos sobre un objeto o producto que interactúa con sus procesos de negocio, esta acción vincula el objeto físico con la información lógica.
- Intercambio: las organizaciones requieren compartir la información de un objeto y los eventos o acciones asociadas al mismo, mediante una codificación que permita acceder a la información asociada, esto involucra también que se deben establecer los mecanismos de intercambio seguro de información.

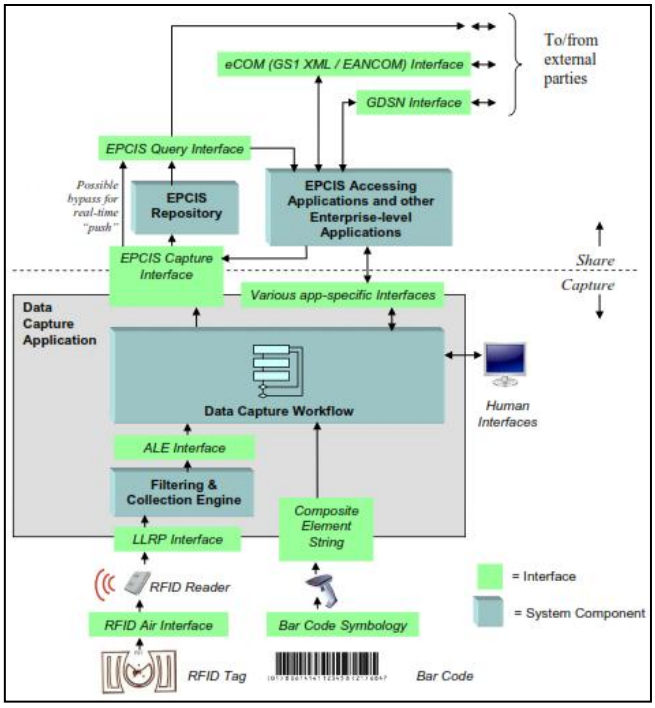


**Fig. 4. Modelo Arquitectónico EPCIS [9] [2]**

*Codificación EPCIS*

Los aspectos importantes dentro de la arquitectura EPCIS, radican en la forma de representación de las consultas de gestión de información, basados en el código EPC, a continuación se expone la figura esquemática para los grupos de bits asociados en la representación del EPC [10]:

**Fig. 5. Esquema de 96 bits para el EPC RFID Clase 1 Generación 2 [4]**

El manejo de direcciones web sobre internet es denominado URI (Uniform Resource Identifier) para los EPC se denomina Identidad Pura EPC (Pure Identity EPC), la definición para codificación es representada de manera uniforme por cada organización en base al estándar EPCIS [4], permitiendo cumplir con los lineamientos en el intercambio, personalización y firma digital si corresponde [7, 11], bajo este punto la información contenida en los mismos resulta un punto de investigación, debido a que la apertura de brechas de seguridad se originan a partir de los intentos no autorizados de lectura, escritura o clonación de códigos, como los más relevantes.

*Proyecto Fosstrack*

El proyecto Fosstrack es una plataforma que implementa las especificaciones de la EPC Global, donde uno de los componentes más importantes de esta investigación radica en la gestión del Middleware RFID, uno de los módulos componentes de este proyecto es la plataforma Accada que contiene tres módulos principales.

- EPCIS, con el repositorio, interfaces de captura e interfaces de consultas (Capture Interface, Query Interface) además de la aplicación de captura y acceso (ALE Interface) [12]
- Filtering & Collection Middleware, módulo que permite el seguimiento, diferenciación y enlace mediante el middleware que permite la gestión integral de las lecturas RFID [12].
- Reader, este módulo permite efectuar la interacción con los Tags a bajo nivel (nivel de protocolo) como LLRP (Low Level Reader Protocol), este último permite efectuar las acciones de personalización de los Tags RFID [12] [13].

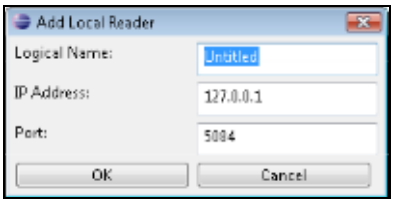


**Fig. 6. Plataforma Fosstrack, configuración de lector RFID [13]**

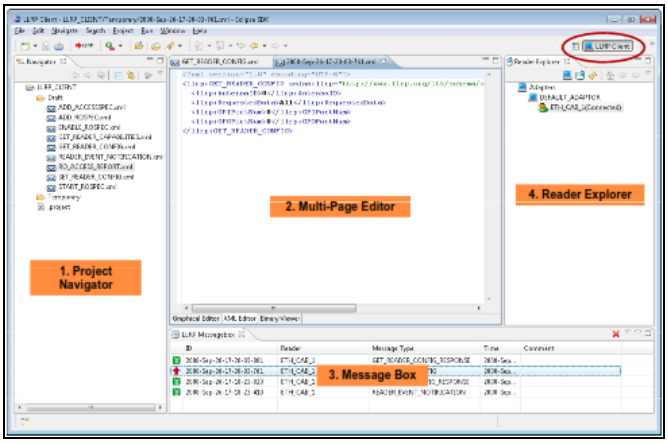


**Fig. 7. Interfaz de administración para comandos I/O de protocolo LLRP para tags RFID [14] [3]**

*Protolocolo LLRP*

Este protocolo permite el acceso y control RFID mediante la operación de comandos por ondas de radio, donde se proveen los formatos y procedimientos de comunicación entre el lector y el cliente.

La compatibilidad del protocolo LLRP permite la funcionalidad entre el lector y los Tags RFID Clase 1 Generación 2, cuyas características soportan el bloqueo

TID: Tag Identification, se refiere al banco de memoria único distribuido a nivel mundial regulado por la EPC Global.

EPC Global: Entidad reguladora del sistema de código EPC, permite asesorar y homologar las aplicaciones en la industria así como la integración entre empresas.

permanente [4] la misma esta implementada en Fosstrack en su componente Accada.

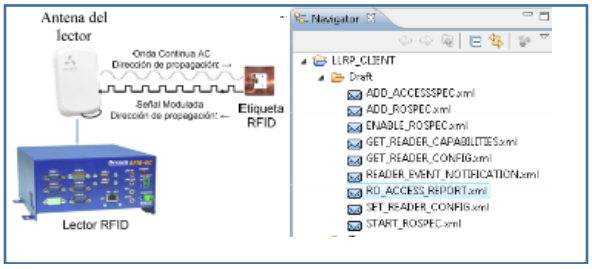


**Fig. 8. Mecanismo e interfaz de administración personalización mediante protocolo LLRP en tags RFID Clase 1 Generación 2 [7] [5]**

## VI. PLANTEAMIENTO DE SOLUCION

*Firma Dinámica Basada en RSA*

El RSA es un cripto-sistema de clave pública para encriptar mensajes, también se aplica para autenticar documentos y transacciones (firmas digitales). [13] [3]

La seguridad está basada en el principio que: "no existe una manera rápida y sencilla de factorizar cantidades que son producto de dos números primos largos" [15]

El principio del algoritmo permite diferenciar claramente el tiempo computacional que se debe aplicar para romper al criptosistema, como encontrar el modulo y los primos ***p*** y ***q***, este principio puede ser aplicado en la firma digital aplicada a los Tags RFID, bajo las siguientes consideraciones:

*Tamaño del banco de memoria de usuario:* El banco de memoria de usuario (User Memory Bank) consta 512 a 1024 bits, normalmente por costos de fabricacion se utilizan normalmente los de 512 bits.

*Tiempo de escritura y verificacion de la firma dinamica:* Los tiempos de escritura y verificacion son reducidos puesto que se tratan de objetos que estan en movimiento, según el estandar 18000-6C pata Tags Rfid C1G2 los tiempos adecuados para este proceso estan en relacion a la distancia del lector, la potencia de irradiación y la impedancia del aire, tambien estan inmersos los aspectos de anticolicion entre Tags RFID para permitir una lectura/escritura simultanea. *[3]*

*Fortaleza de la clave para firma dinamica en Tags RFID*: En la generacion de llaves publica y privada se deben seguir los siguientes pasos:

Paso 1: Se eligen 2 números primos **p** y **q** de forma aleatoria del orden de 10 a 200, donde la longitud deberá ser similar en bits.

Paso2: Se calcula ***n*= *p**q***, donde n es el modulo entre ambas claves, Publica y Privada.

Paso 3: Se calcula ***φ*(n)=(*p*-1)(*q*-1)**, donde ***φ*(n)** es la funcion de Euler.

Paso 4: Se escoge un entero positivo ***e*** menor que ***φ*(n)**, que sea primo relativo de ***φ*(n),** ***e*** se da a concocer como el exponente de la clave pública, se recomienda que $e > \frac{n}{2}$, donde ***e*** sera la llave publica.

Paso 5: Se determina un numero ***d*** (mediante aritmética modular) que satisfaga la congruencia $d \equiv e^{-1} Mod(\varphi(n))$ , mismo que suele calcularse mediante le algoritmo de Euclides extendido; ***d*** será nuestra clave privada.

Paso 6: En función de los valores ***e*** y ***d*** se puede iniciar el proceso de cifrado que estará dado por: $c=m^e(mod(n))$, donde ***m*** es el mensaje original expresado en forma numérica y ***c*** es el mensaje cifrado, se cifra con la clave pública.

Paso 7: El proceso de descifrado, que está dado por $m=c^d(mod(n))$, donde ***m*** es el mensaje original expresado de forma numérica y ***c*** es el mensaje cifrado, se descifra con la llave privada.

***Algoritmo:***

*Seleccionar dos números primos grandes*

$p = 83$

$q = 89$

*Calcular n*

$$n = p*q = 83*89 = 7387 \quad (1)$$

*Calcular* $\varphi(n)$ (2)

$$\varphi(n) = (p-1)(q-1) = (83-1)(89-1)$$

$$\varphi(n) = 7216$$

*Seleccionar e como primo relativo de* $\varphi(n)$

$e = 5009$

*Calcular* $d$*, se calcula el MCD entre e y* $\varphi(n)$ *luego se aplica Modulo y* $\varphi(n)$
(4)

$d = 2753$

*Cifrado de mensaje, texto RFID a su numérico equivalente en ASCII* [12]

$RFID \rightarrow 82,70,73,68$

*Se aplica la formula* $c=m^e(mod(n))$
(5)

$$c1 = 82^{5009} \left(mod(7387)\right) = 6473$$

$$c2 = 70^{5009} \left(mod(7387)\right) = 6621$$

$$c3 = 73^{5009} \left(mod(7387)\right) = 2994$$

$$c4 = 68^{5009} \left(mod(7387)\right) = 5172$$

*Para el proceso de personalización RFID con Firma Dinámica se efectúa la conversión de los dígitos en su equivalente hexadecimal*

*6473 = 0x1949h*

*6621 = 0x19DDh*

*2994 = 0x0BB2h*

*5172 = 0x1434h*

*La firma quedará como la cadena*

*0x194919DD0BB21434h*

*Entonces para la personalización se aplica en envió de comandos de la API del protocolo LLRP para la personalización u grabado de la firma generada: ProgUserData, ProgG2AccessPwd (prueba efectuada sobre un lector Alien).*

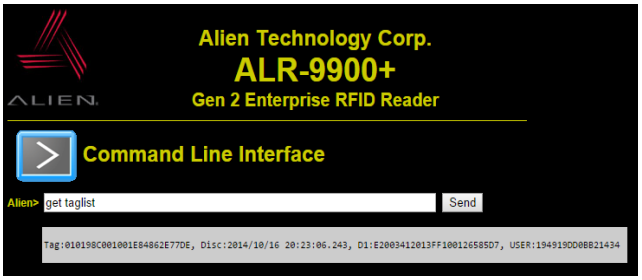


Fig. 7. Prueba de concepto del proceso de personalización con Firma Dinámica bajo un lector RFID Alíen 9900

*Descifrado de mensaje (este proceso puede ser el interpretado inverso del proceso de personalización)*

*c1=6473, c2=6621, c3=2994, c4=5172*

*Para descifrar aplicamos la formula* $m = c^d \left(mod(n)\right)$ (6)

$$m1 = 6473^{2753} \left(mod(7387)\right) = 82$$

$$m2 = 6621^{2753} \left(mod(7387)\right) = 70$$

$$m3 = 2994^{2753} \left(mod(7387)\right) = 73$$

$$m4 = 5172^{2753} \left(mod(7387)\right) = 68$$

*Mensaje Original:*

*82,70,73,68 → RFID*

*Modelo Propuesto para la Firma dinámica RFID:* El modelo arquitectónico EPCIS describe los lineamientos de trazabilidad, que se pueden aplicar para el control de paso de los objetos que tienen Tags RFID implantados, entonces el paso de cifrado para proteccion de los bancos de memoria en funcion del algoritmo y los pasos citados puede ser aplicado NxN las cantidades de Tags Rfid con lectores RFID dentro del Sistema EPCIS para una organización donde se maneja esta tecnología.

El modelo propuesto tiene una composición Ad-Hoc en la interacción Lector y Tag RFID, donde se hace uso del protocolo LLRP y los comandos que permiten efectuar procesos I/O de personalización en los Tag RFID; la firma dinamica será aplicada sobre los bancos de memoria EPC y USER.

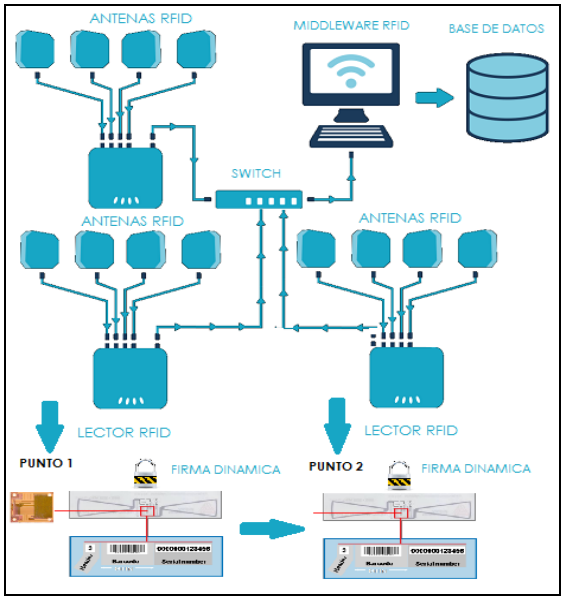


Fig. 8. Esquema físico propuesto para la personalización RFID con firma dinámica

*Procedimiento de firma dinámica:* La firma dinámica debe ser aplicada en cada paso de control RFID, garantizando que el paso del objeto por el punto este registrado y además se suscriba información sobre el evento de control bajo el punto de lectura/ecritura, de esta manera se podría generalizar el modelo de 1xN hacia NxN puntos y las veces que fueran necesarias para garantizar una corecta trazabilidad de la información suscrita en el Tag RFID, esta información posteriormente puede ser compartida con terceros a efectos de consulta del objeto donde se implanto el Tag RFID.

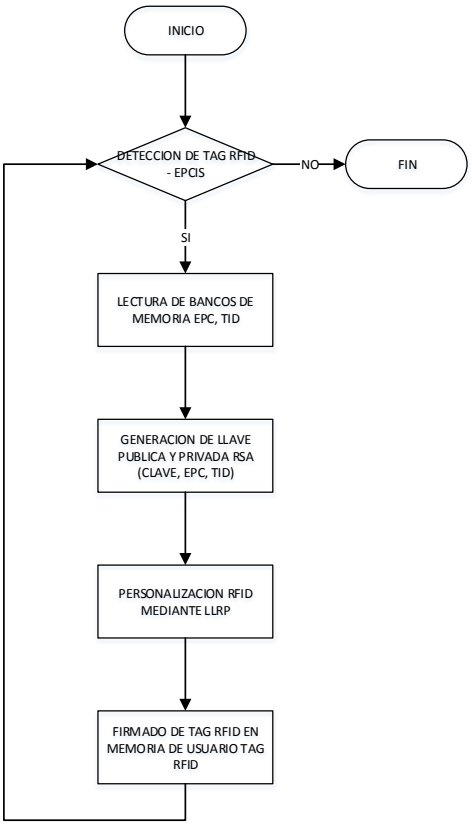


Fig. 9. : Diagrama de flujo del procedimiento de firmado dinámico RFID

## REFERENCIAS


[1] S. E. S. J. R. W. Stephen b. MIles, RFID Technology and Applications, Cambridge University Press, 2008.

[2] W.-R. Hansen, RFID for the optimizacion of Business Processes, John Wiley & Sons Inc., 2008.

[3] P. P. Lopez, Lightweight Cryptography in Radio Frecuency Identification (RFID) Systems, Universidad Carlos III de Madrid, 2008.

[4] L. C. U. Guide, «http://fosstrak.googlecode.com,» [En línea]. Available: http://fosstrak.googlecode.com/svn/wikires/llrp/LLRP_Commander_User_Guide.pdf. [Último acceso: 15 10 2013].

[5] K. Finkenzeller, «RFID HandBook, Fundamentals and Applications in Contactless Smart Cards, Radio frecuencia Identification and Near-Fiel Communication,» John Wiley & Sons Inc, 2010.

[6] M. S. N. M. a. P. S. S. Mandeep Kaur, «http://www.ijcee.org,» [En línea]. Available: http://www.ijcee.org/papers/306-E794.pdf. [Último acceso: 15 03 2014].

[7] A. Cavoukian, «www.ipc.on.ca,» [En línea]. Available: http://www.ipc.on.ca/images/resources/up-rfid.pdf. [Último acceso: 10 05 2014].

[8] A. P. M. P. Daniel Hunt, RFID A guide to radio frecuency identification, John Wiley & Sons Inc, 2007.

[9] Libera, «http://www.libera.net,» [En línea]. Available: http://www.libera.net/uploads/documents/whitepaper_rfid.pdf. [Último acceso: 10 03 2014].

[10] E. G. E. V. Portal, «http://www.epcisvp.com,» [En línea]. Available: http://www.epcisvp.com/EVP/Public/UserGuide_v2.pdf. [Último acceso: 12 12 2013].

[11] S. A. W. a. D. W. E. Sanjay E. Sarma, «http://www2.wiwi.hu-berlin.de,» [En línea]. Available: http://www2.wiwi.hu-berlin.de/is/internetoekonomie/downloads/rfid/kernprobleme_Security/RFID%20Systems%20and%20Security%20and%20Privacy%20Implications.pdf. [Último acceso: 18 11 2013].

[12] F. U. Bes, Implementation of Fosstrack EPCIS RFID System, Czech Technical University, 2012.

[13] J. m. Segui, Lightweight PRNG Low Cost Passive RFID Security Improvement, Universitat Oberta de Catalunya, 2011.

[14] L. G. Client, «http://fosstrak.googlecode.com,» [En línea]. Available: ttp://fosstrak.googlecode.com/svn/llrp/tags/llrp-1.2.0/src/site/resources/pdf/report.pdf. [Último acceso: 25 01 2014].

[15] S. B. &. S. Paine, RSA Security's Official Guide to Cryptography, Mc Graw Hill, 2001.

[16] E. Network, «http://www.gs1.org,» [En línea]. Available: http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_1-standard-20140520.pdf. [Último acceso: 25 04 2014].