Revista Ciencias Técnicas Agropecuarias
ISSN: 1010-2760
paneque@isch.edu.cu
Universidad Agraria de La Habana Fructuoso Rodríguez Pérez
Cuba

Sepúlveda Peña, Juan Carlos; Núñez Musa, Yulier; Sepúlveda Lima, Roberto; Rosete Suárez, Alejandro

Propuesta de aplicación de un sistema de Infraestructura de Clave Pública (Public Key Infrastructure "PKI") y los Certificados Digitales en la trazabilidad de productos agrícolas

Revista Ciencias Técnicas Agropecuarias, vol. 18, núm. 4, 2009, pp. 75-78
Universidad Agraria de La Habana Fructuoso Rodríguez Pérez
La Habana, Cuba

Disponible en: http://www.redalyc.org/articulo.oa?id=93212367015

COMPUTACIÓN Y MATEMÁTICA APLICADA
APLLIED COMPUTATION AND MATHEMATICS

PUNTOS DE VISTA

Propuesta de aplicación de un sistema de Infraestructura de Clave Pública (Public Key Infrastructure "PKI") y los Certificados Digitales en la trazabilidad de productos agrícolas

Proposal of application of the Public Key Infrastructure (PKI) and the Digital Certificates in the agriculture products traceability

Juan Carlos Sepúlveda Peña[1], Yulier Núñez Musa[1], Roberto Sepúlveda Lima[1] y Alejandro Rosete Suárez[1]

RESUMEN. Hoy día la trazabilidad de los productos y las actividades en la cadena de suministro se han convertido en un nuevo factor a tener en cuenta en la cadena de distribución de alimentos y la agroindustria. Cada vez más, consumidores en muchas partes del mundo demandan de pruebas verificables de trazabilidad como uno criterio importante de la calidad/inocuidad de los productos alimenticios. El presente artículo propone una solución a esta problemática introduciendo el uso de un sistema de Infraestructura de Clave Pública (Public Key Infrastructure "PKI") y los certificados digitales (CD).

Palabras clave: agricultura, certificados digitales, trazabilidad, PKI, alimento.

ABSTRACT. Today the traceability of products and activities in the supply chain has become a new factor in food and agribusiness. Increasingly, consumers in many parts of the world demand for verifiable evidence of traceability as an important criterion of food product quality/safety. The current paper proposes a solution to this problem making uses of Public Key Infrastructure system and the digital certificates.

Keywords: Agriculture, digital certificates, traceability, PKI, food.

INTRODUCCIÓN

El término trazabilidad viene siendo usado ampliamente en varias industrias en los tiempos recientes (Opara, 2003). La trazabilidad (en la agricultura) es un instrumento básico para asegurar la calidad alimentaria a lo largo de la cadena comercial de distribución y conseguir la confianza del consumidor final (Opara, 2003). Su puesta en práctica es cada vez más compleja debido al distanciamiento geográfico y temporal entre la producción y el consumo final (Felipe & Briz, 2004).

Los escándalos producidos en los últimos años en el ámbito de la "seguridad alimentaria" (vacas locas, pollos belgas, fiebre aftosa, etc.) han despertado la inquietud del consumidor final y de los comerciales, que les han llevado a exigir unas "garantías de calidad" en los alimentos consumidos, y ha generado una creciente preocupación por asegurarse de que éstos se produzcan de una forma saludable y respetuosa con el medio ambiente (Oramas, 2002). Así pues, surgen sistemas de producción basados fundamentalmente en "buenas prácticas culturales" y por consiguiente, en la obtención de productos sanos y libres de residuos químicos (Oramas, 2002).

Países como Chile y la Comunidad Europea, entre otros, tienen incluida la trazabilidad de alimentos entre sus normas de buenas prácticas agrícolas.(Bentivegna *et al.,* 2005). Tal es

Recibido 20/01/09, aprobado 18/09/09, trabajo 63/09, puntos de vista.

[1] Ing., Prof. Aux., Instituto Superior Politécnico José A. Echeverría (ISPJAE), Calle 114 No. 11901 e/119 y 127. Marianao, Ciudad de La Habana, Cuba, CP 19390, tel: (53) (7) 266 3801, E-✉: jcarlos@ceis.cujae.edu.cu http://www.cujae.edu.cu

la importancia actual en la trazabilidad de alimentos que existen normas que rigen su implementación y explotación. Tal es el caso de las normas ISO 22005:2007, ISO 9000:2000 e ISO 8402 (ISO, 2009) (Juste & Moltó, 2001) por nombrar algunas.

Según Opara (2002), la trazabilidad en la cadena de productos agrícolas facilita:

- La identificación de las prácticas de producción.
- La identificación de la historia del producto a través de registros verificables.
- La segregación, aislamiento y elaboración de registros de productos defectuosos.

El mismo autor señala 6 elementos que a su juicio debe contener un sistema de trazabilidad de suministros integrada de productos (Opara, 2002 y Opara, 2003).

- Trazabilidad del producto: determinación de la localización física del ítem en cualquier momento.
- Trazabilidad del proceso: determinación del tipo y secuencia de los eventos ocurridos al producto.
- Trazabilidad de las entradas: determinación del tipo, fuente, suministrador etc. de los ingredientes usados para crear el producto.
- Trazabilidad de afecciones: para la traza de enfermedades y peligros biológicos.
- Trazabilidad genética: para determinar la constitución genética del producto, incluyendo variedad, tipo, origen y alteraciones en la estructura básica del ADN.
- Trazabilidad de mediciones: trazabilidad de mediciones individuales realizadas al producto tales como calidad, atributos de seguridad etc. a través de una cadena continua de mediciones.

Sin embargo, a criterio de los autores del presente artículo debiera incluirse un séptimo elemento que garantice la auditabilidad del sistema y el no repudio de los datos y eventos registrados en cada momento. Esto puede lograrse haciendo uso de la criptografía y de un sistemas de llave privada/llave pública (PKI) y certificados digitales (Sepúlveda & Sepúlveda, 2005).

Trazabilidad en la cadena de suministros

Una completa y total trazabilidad es imposible (Golan *et al.,* 2004) el cumplimiento de determinadas directivas en cada uno de los estadios en la cadena de producción y suministro puede garantizar un nivel de seguridad y fiabilidad aceptable para la mayoría de los consumidores.

Trazabilidad del producto: En el momento de la cosecha se debe registrar como mínimo, la parcela y la fecha de recolección.(Juste & Moltó, 2001). Con el uso de computadores de a bordo puede registrarse de forma automatizada las coordenadas geospaciales de donde fue recolectado el producto. (Lago *et al.,* 2008). Igualmente usando la tecnología actualmente disponible puede garantizarse la trazabilidad del producto en cualquier estadio de la cadena de suministro (Chen *et al.,* 2008).

Trazabilidad del proceso: Las nuevas tecnologías de la informática y las comunicaciones (NTIC), permiten llevar un registro de todas las operaciones y manipulaciones realizadas al producto, desde su cosecha en bruto hasta su procesamiento final. El registro de cada una de estas operaciones puede realizarse usando dispositivos conocidos como RFID (Chen *et al.,* 2008).

Trazabilidad de las entradas: Las tecnologías de agricultura de precisión permiten el tratamiento diferenciado de una misma parcela durante la aplicación de los insumos. Para esto se usan los mapas de aplicabilidad del producto, los cuales se confeccionan con antelación y se le suministran a los encargados de irrigar el producto en el campo. Esto permite poder contar con una trazabilidad de los distintos productos aplicados al cultivo.

Trazabilidad de las afecciones: La trazabilidad de enfermedades es más difícil de automatizar, y en el estadio actual de tecnología la opción más viable económicamente es la introducción manual de los datos a partir de un riguroso examen del campo.

Trazabilidad genética: Este tipo de trazabilidad es usado principalmente cuando se trabaja con organismos genéticamente modificados. Esta información debe acompañar al producto durante toda la cadena de distribución hasta llegar al consumidor final.

Trazabilidad de las mediciones: Durante el traslado y almacenamiento del producto deben garantizarse determinadas condiciones de almacenamiento y preservación de este. Por tal motivo debe realizarse una traza del comportamiento de dichas condiciones de almacenamiento y el registro de cualquier desplazamiento fuera de los parámetros estipulados.

Seguridad de la información

Con el auge actual de las técnicas de procesamiento electrónico de la información, existen cuatro objetivos de la seguridad a tener en cuenta para el manejo de la misma: la confidencialidad, la Autenticidad, la Integridad y el No Repudio (Bruce, 1993) (Menezes *et al.,* 1996) (Sepúlveda & Sepúlveda, 2005).

Una particularidad de los documentos auténticos es su integridad. Si un documento es auténtico entonces es integro pero no viceversa. Estos problemas, confidencialidad, integridad, autenticidad y no-repudio se resuelven mediante los componentes tecnológicos de una ciencia denominada "Criptografía". Se debe aclarar que el término documento electrónico es aplicable a cualquier dato digital, susceptible de ser procesado electrónicamente.

El término criptografía puede definirse como: Procesos, ciencia y arte de conservar mensajes y datos de forma segura. La criptografía se utiliza para asegurar la confidencialidad, la integridad de los datos y la autenticación (origen de datos

y entidad), y para evitar el rechazo. (Sepúlveda & Sepúlveda, 2005).

La criptografía incluye primitivas tales como: Cifrado y descifrado de información, funciones resúmenes criptográficas y firmas digitales, entre otras (Bruce, 1993) (Menezes *et al.,* 1996)**.**

Infraestructura de Clave Pública (PKI) y Certificados Digitales (CD): Los algoritmos de cifrado, atendiendo tipo de clave empleado se clasifican en: cifrado de clave simétrica y cifrado de clave pública (o asimétrica). (Menezes *et al.,* 1996*).* Descifrar un mensaje con una clave pública proporciona la garantía de que el mensaje fue cifrado por el dueño de la clave privada asociada a esta, lográndose la autenticidad del emisor (Sepúlveda & Sepúlveda, 2005). Con el objetivo de garantizar seguridad y confianza en una comunicación electrónica entre las partes involucradas, se emplea una Infraestructura de Clave Pública cuya base es la criptografía asimétrica o de clave pública (Adams & Lloyd, 2002) (Raina, 2003). El principal objetivo de un sistema PKI es la gestión y distribución de claves públicas, la cual es llevada a cabo por una Autoridad Certificadora (AC). La PKI en sentido general se basa en un modelo de confianza, en el cual los usuarios confían que las claves públicas gestionadas por dicha PKI son auténticas (Adams & Lloyd, 2002). La AC emplea Certificados Digitales para distribuir una clave pública. Un certificado digital es una credencial electrónica que relaciona la información del titular de dicho certificado con su clave pública. La firma digital es un preciso método criptográfico que permite adjuntar a un mensaje la identidad de la persona o equipo que lo originó y asegura la integridad y el no repudio del mensaje (Menezes *et al.,* 1996). Existen varios algoritmos de cifrado de clave pública tales como RSA (Menezes *et al.,* 1996), ELGamal (Menezes *et al.,* 1996) y el de Curvas Elípticas (ECC) (Menezes *et al.,* 1996), entre otros. Se recomienda el empleo de ECC para esta aplicación por emplear tamaños de bloques pequeños, implementaciones rápidas en software y hardware y menos tamaño de clave respecto a otros algoritmos asimétricos (Jurisic & Menezes, 1997) (Vivek *et al.,* 2008).

Aplicación de las PKI y los CD a la trazabilidad

A continuación se propone la aplicación de las PKI y los certificados digitales en cada uno de los elementos de trazabilidad enunciados por (Opara, 2002) y (Opara, 2003).

Los autores proponen la realización de dos firmas a cada documento. Una firma digital con una clave privada contenida en el propio dispositivo y que identifica al aparato de forma unívoca. Dicha llave privada debe ser almacenada dentro del equipo en una zona donde no se tenga acceso desde el exterior. Y la otra firma con una llave privada que identifique al operador que realiza la tarea. La clave privada de este último puede ser almacenada en un dispositivo de almacenamiento externo de la cual el operador sea el propietario y único responsable. Se sugieren doble firma ya que el aparato no tiene responsabilidad legal, pero es importante tener registrado cual aparato realizó la labor.

Aplicación de las PKI y los CD a la trazabilidad del producto: Primero se debe recalcar el hecho de que el uso de las NTIC y computadores de a bordo son parte integrante de la agricultura de precisión (Sepúlveda *et al.,* 2008) (Esquivel, 2009). Por tanto la funcionalidad de "firma de documentos" puede ser realizada por el propio computador de a bordo. Durante la cosecha del producto el computador de a bordo debe registrar cada una de las parcelas cosechadas a partir de las coordenadas espaciales obtenidas del sensor de GPS (Sepúlveda *et al.,* 2009). Igualmente debe ir recopilando la información pertinente a fecha y hora de recolectado el producto. Cada vez que se vaya a cambiar de contenedor o recipiente de almacenamiento del producto, el computador de a bordo debe firmar el "documento" que contiene la información anteriormente mencionada. Los contenedores donde se acopia el producto tienen que estar equipados con dispositivos de identificación, como los RFID, de forma tal que puedan ser identificados posteriormente en la cadena de suministro y seguirle la pista al producto.

Aplicación de las PKI y los CD a la trazabilidad del proceso: Cada una de las maquinarias encargadas de realizar alguna manipulación u operación al producto debe contener un dispositivo capaz de leer el identificador del contenedor o producto para registrar la operación y el producto al cual le fue realizada dicha operación. Una vez realizada la manipulación debe procederse a dejar registrada la firma de la operación realizada así como la identificación del producto al cual se le realizó dicha manipulación.

Aplicación de las PKI y los CD a la trazabilidad de las entradas: Esta puede ser realizada de forma similar a la propuesta de trazabilidad del producto. Sin embargo la información a registrar en este caso es el tipo de insumo irrigado en el campo así como la fecha de realización.

Aplicación de las PKI y los CD a la trazabilidad de las afecciones y trazabilidad genética: La trazabilidad de enfermedades y la trazabilidad genética son datos que deben ser entrados de forma manual en el sistema ya que según la bibliografía consultada no se constato la existencia de una tecnología viable económicamente para la automatización de este proceso. Para garantizar la fiabilidad de la información introducida en el sistema, esta debe ser firmada por parte del operador encargado de su introducción.

Aplicación de las PKI y los CD a la trazabilidad de las mediciones: El uso de RFID como identificador del producto puede garantizar la trazabilidad de los eventos ocurridos durante la transportación y/o almacenamiento del producto. El dispositivo de chequeo debe ser capaz de registrar y firmar los datos medidos.

CONCLUSIONES

- El sistema propuesto garantiza la trazabilidad del producto desde recolección en el campo hasta su llegada al cliente final, incluyendo la información de los eventos ocurridos durante su transportación y almacenaje. El uso de las PKI y los CD garantizan la auditabilidad del sistema y una mayor confianza de los consumidores en la trazabilidad del producto. Su implementación no implican grandes gastos económicos adicionales en aquellas empresas que ya tienen implementado un sistema de agricultura de precisión y de trazabilidad tradicional.

REFERENCIAS BIBLIOGRÁFICAS

ADAMS, C.; S. LLOYD: *Understanding PKI: Concepts, Standards, and Deployment Considerations,* 2 edn, Addison Wesley, USA, 2002,

BENTIVEGNA, M.; R. KAPLAN.; P. FELDMAN: *Boletín informativo sobre Buenas Prácticas Agrícolas para Productos Fruti-Hortícolas Frescos*, *[en línea] 2005. Disponible en:* [http://www.alimentosargentinos.gov.ar/programa_calidad/boletin-calidad/Boletin_BPA_frutihorticola.pdf] *[Consulta: mayo 18 2009].*

BRUCE, S.: *Applied Cryptography: Protocols, Algorithms, and Source Code,* 618 pp., *In C*, John Wiley & amp; Sons, Inc., USA, 1993.

CHEN, R.-S., C. CHEN; C YEH; Y. CHEN; C. KUO: *Using RFID Technology in Produce Traceability* pp.10, In Wseas Transactions, China, 2008,

ESQUIVEL, M.: La Agricultura de Precisión en Cuba, Experiencias y Retos, En **VI Congreso Internacional de Geomática. XIII Convención Internacional de Informática.***,* Palacio de las Convenciones, La Habana, Cuba, 2009.

FELIPE, I.; J. BRIZ: Seguridad y trazabilidad alimentaria en el contexto internacional. Crisis y evaluación de riesgos, Secretaría de Estado de Turismo y Comercio, Colombia, 2004.

GOLAN, E., B. KRISSOFF; F. KUCHLER; L. CALVIN; K. NELSON; G. PRICE: *Traceability in the U.S. Food Supply: Economic Theory and Industry Studies,* United States Department of Agriculture (USDA). Agricultural Economic., Washington, DC 20036, USA, 2004.

ISO 2009: *Sitio Web oficial de la Organización Internacional de Estándares. (ISO) [en línea] Disponible en:* [http://www.iso.org] *[Consulta: mayo 18 2009].*

JURISIC, A.; A. J. MENEZES: "Elliptic Curves and Cryptography", Dr. Dobb's Journal, 4-12, 1997.

JUSTE, F.; E. MOLTÓ:. "Tecnología de poscosecha, calidad de los productos, trazabilidad" *Dossiers Agrari.,* vol. 8, 37-46, 2001.

LAGO, C.; C. PEÑA; F. FERNÁNDEZ; A. CAMACHO: Utilización de la tecnología GPS en la generación automática de mapas de rendimiento en el cultivo de la caña de azúcar, En: **III Taller de Informática aplicada. 14 Convención Científica de Ingeniería y Arquitectura (CCIA2008),** Palacio de las convenciones, Ciudad de La Habana, Cuba, 2008.

MENEZES, A. J.; A. VANSTONE; C. V OORSCHOT: *Handbook of Applied Cryptography*, 816pp., .CRC Press, Inc., USA, 1996.

OPARA, L. U.: "Engineering and Technological Outlook on Traceability of Agricultural Production and Products", *CIGR Journal of Scientific Research and Development,* vol. IV, 2002.

OPARA, L. U.: 'Traceability in agriculture and food supply chain: a review of basic concepts, technological implications, and future prospects", *CIGR Journal of Scientific Research and Development,* vol. I, 2003.

ORAMAS, J. J.: "La trazabilidad y cultivos controlados e integrados', In: **Jornada Autonómica de la Comunidad Canaria,** Sta. Cruz de Tenerife, Islas Canarias, 2002.

RAINA, K.: *PKI, Security Solutions for the Enterprise: Solving HIPAA,* E-Paper Act, and Other Compliance Issues, Wiley, USA, 2003.

SEPÚLVEDA, J. C., T. HERNÁNDEZ; L. CRUZ; L. GONZÁLEZ; C. GONZÁLEZ; R. SUÁREZ; S. LIMA; L. NEYRA; R. URIBAZ: Modelo de referencia para sistemas de análisis de datos de computadores de a bordo, En **Evento UCIencia 2008,** Universidad de Ciencias Informáticas, Ciudad de La. Habana, Cuba, 2008.

SEPÚLVEDA, J. C., C. LAGO; R. SEPÚLVEDA; A. ROSETE; Y. TIRADO; I. LANZA; L. NEYRA: *Modelo de referencia para sistemas informáticos de análisis de datos de computadores de "A Bordo"* Mapping Interactivo., No. 132, La Habana, Cuba, 2009.

SEPÚLVEDA, J. C.; R. SEPÚLVEDA: Certificados Digitales, Características y Aplicaciones en la Seguridad de Documentos Digitales, En: **Seguridad en Cómputo e Inteligencia Artificial,** Sede de Pereira y Manizales. Universidad Nacional de Colombia, 2005.

VIVEK, K; A. VIVEK SONNY; S. RAMESH: "Elliptic curve cryptography", *ACM,* vol. 9, 1-8, 2008.