Triple Helix PKI: Desarrollo de la firma digital en Costa Rica con la cooperación Universidad-Industria-Gobierno

Rodrigo A. Bartels
ECCI-CITIC
Universidad de Costa Rica
rodrigo.bartels@ucr.ac.cr

Alejandro Mora Castro
CITIC
Universidad de Costa Rica
alejandro.moracastro@ucr.ac.cr

Ricardo Villalón-Fonseca
ECCI-CITIC
Universidad de Costa Rica
ricardo.villalón@ucr.ac.cr

Gabriela Marín Raventós
ECCI-CITIC
Universidad de Costa Rica
gabriela.marin@ucr.ac.cr

***Resumen*—Este artículo reseña el proceso realizado en Costa Rica para el desarrollo de la infraestructura necesaria para la implementación de la firma digital a nivel nacional, y los actores involucrados desde el año 2002 hasta la actualidad. Este proceso se ha desarrollado mediante la cooperación entre las universidades públicas, la industria y el gobierno, y representa un caso de éxito de este tipo de cooperación a nivel nacional. Se parte de la premisa de que sin relaciones de cooperación no se hubiera podido alcanzar el nivel de desarrollo y avance en firma digital con el que se cuenta actualmente, como ha sucedido en diversos países de la región latinoamericana.**

I. Introducción

El concepto de la Triple Hélice (Triple Helix en inglés) de relaciones de cooperación entre la universidad, la industria y el gobierno fue inicialmente propuesto por Etzkowitz [1], como una evolución de la tradicional relación entre el gobierno y la industria, generada durante la Revolución Industrial, hacia una tripleta universidad-gobierno-industria. La propuesta subyacente es que el potencial para la innovación y el desarrollo económico en una sociedad del conocimiento recae de forma prominente en las universidades, mediante el desarrollo de proyectos híbridos entre las universidades, la industria y el gobierno con el fin de generar nuevo conocimiento así como innovar en los mecanismos para la transferencia del mismo [2].

Este artículo presenta la metodología utilizada y los resultados obtenidos durante 15 años de colaboración entre las universidades públicas, la industria y el Gobierno de la República de Costa Rica para el desarrollo y mejoramiento del Sistema Nacional de Certificación Digital de Costa Rica (SNCD). Mediante el desarrollo de proyectos conjuntos, se ha logrado crear un ecosistema de infraestructuras, aplicaciones de software, estándares y esquemas de certificación que apoyan los servicios esenciales de seguridad del SNCD, en especial el no repudio, la integridad y la confidencialidad. Se parte de la premisa de que sin estas relaciones de cooperación no se hubiera podido alcanzar el nivel de desarrollo y avance con el que se cuenta actualmente, como ha sucedido en diversos países de la región.

El artículo se organiza de la siguiente manera. Inicialmente se presentan los conceptos esenciales para comprender el resto del artículo así como el contexto en el cual se desarrollaron los diversos proyectos de investigación. A continuación se presenta el problema que se busca resolver, la metodología utilizada para organizar los diversos proyectos realizados en el tiempo y sus etapas. Luego, se describe cada etapa en detalle. Finalmente se mencionan las lecciones aprendidas, las conclusiones y el trabajo futuro.

II. Marco Teórico

Una infraestructura de llave pública (PKI por sus siglas en inglés) es un sistema que utiliza certificados digitales emitidos por una entidad de confianza, que se encarga de validar y asegurar la identidad y validez de los certificados emitidos [3]. Es difícil construir un único componente que pueda crear y distribuir de manera segura certificados digitales. Las infraestructuras de llave pública están constituidas por una variedad de componentes, cada uno de los cuales está diseñado para llevar a cabo un conjunto pequeño de tareas [4].

En general las infraestructuras de llave pública son utilizadas en diversos dominios de aplicación para implementar distintos casos de uso, como certificados para sitios web, firmas digitales, certificados de persona física, firma de código para aplicaciones de software, entre otros. El éxito y el correcto funcionamiento de una infraestructura de PKI depende del nivel de confianza que tengan todos los actores entre sí, y en particular hacia la Autoridad Certificadora y sus prácticas de certificación. La CA es el tercero de confianza, es el actor que sostiene la confiabilidad completa del sistema. Por esta razón, desde los inicios de la utilización de Infraestructuras de Llave Pública para la emisión de certificados para uso público, se han desarrollado guías, estándares y prácticas de aseguramiento para la evaluación de las prácticas, procedimientos y procesos de la Autoridad Certificadora, los cuales poco a poco han sido estandarizados y convertidos en normas y estándares internacionales aceptados por la industria [5]. Estos estándares son los que se utilizan como punto de partida para la evaluación y auditoría de Autoridades Certificadoras utilizadas para la emisión de certificados digitales en diversos ámbitos, por ejemplo entidades financieras, organizaciones, empresas y

la implementación de infraestructuras de llave pública a nivel nacional como mecanismo de firma digital con validez legal.

III. Contexto

El SNCD es una infraestructura de llave pública utilizada a nivel nacional en Costa Rica para la generación de certificados digitales para los ciudadanos. Un certificado le permite a un ciudadano identificarse y firmar documentos electrónicamente de forma inequívoca y no repudiable, de una forma legalmente válida y vinculante. La Ley 8454 [6] regula a los actores del SNCD y crea la Dirección de Certificadores de Firma Digital (DCFD), un ente adscrito al Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), encargado de administrar, mantener y asegurar la confianza y seguridad del Sistema.

En una infraestructura de llave pública participan diversos actores, cada uno con roles diferentes dentro del proceso para emitir y usar certificados digitales [3]. En el contexto del SNCD, el MICITT es el dueño de los certificados raíz y es el ente encargado de aprobar la creación de Autoridades Certificadoras en el país. El Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos [7] le confirió el grado de Autoridad Certificadora Raíz del SNCD a la DCFD. En la actualidad existe un convenio de cooperación entre el MICITT y el Banco Central de Costa Rica (BCCR), por lo que este último es el encargado de implementar, custodiar y operar la raíz del Sistema.

Actualmente, la única Autoridad Certificadora registrada en el Sistema Nacional de Certificación Digital para la emisión de certificados al público en general es administrada por el Banco Central de Costa Rica y es conocida como CA-SINPE. Esta es la única CA aprobada para la generación de certificados digitales a los ciudadanos. No obstante, la ley permite la implementación de múltiples Autoridades Certificadoras, tanto en el sector público como privado. Además, incluye la posibilidad de la homologación de certificados generados por Autoridades Certificadoras extranjeras. Cada una de estas Autoridades Certificadoras debe cumplir con cada uno de los requisitos que defina el marco legal costarricense para poder operar y emitir certificados digitales en Costa Rica.

IV. Problema

El desarrollo de una PKI es un proceso complejo y costoso, todavía más cuando se quiere utilizar como base para un sistema de firma digital a nivel de un país. Se requiere recurso humano, tanto administrativo como técnico especializado, así como infraestructura. Inclusive a nivel mundial, el uso de firmas digitales a nivel país no es muy alto, por lo que todavía existen muchos problemas de investigación y retos por resolver. En Costa Rica los recursos disponibles de forma individual en cualquier sector de la sociedad no son suficientes para generar el conocimiento necesario que permita alcanzar el nivel necesario para garantizar la seguridad del sistema.

V. Metodología

El proceso de desarrollo de la firma digital en Costa Rica ha contado con la cooperación de diversas personas e instituciones. Para presentar el proceso realizado durante los últimos 15 años, se dividió éste en tres etapas: la etapa inicial, la etapa de mejoramiento y la etapa de expansión. Cada etapa tiene una serie de objetivos específicos. Las siguientes secciones presentan en detalle cada una de estas etapas.

VI. Etapa Inicial

La etapa inicial comprende el período de 2002 a 2012. Durante este período los objetivos primordiales fueron:

1. Definir el marco legal pertinente para la utilización de la firma digital en Costa Rica.
2. Desarrollar la Infraestructura necesaria para la puesta en operación de las Autoridades Certificadoras necesarias.
3. Divulgar y educar a la población sobre la disponibilidad y uso de la firma digital.

Del 2002 al 2005 un grupo de profesionales del sector público (MICITT, Poder Judicial, Registro Nacional de la Propiedad), el sector privado (empresarios e informáticos, Cámara de Tecnologías de Información y Comunicación (CAMTIC)) trabajaron en la definición de la propuesta de la Ley 8454. La ley fue aprobada en el año 2005, establece la Dirección de Certificadores de Firma Digital y le da a ésta la potestad de definir vía reglamento los requisitos y procesos necesarios para la correcta implementación del SNCD. El Reglamento de la Ley 8454 faculta que el Director de la DCFD cuente con la asesoría de un comité de políticas, integrado por representantes de las siguientes entidades: Tribunal Supremo de Elecciones, Banco Central de Costa Rica, Poder Ejecutivo (dicha representación recae en dos funcionarios del Registro Nacional), Poder Judicial, Consejo Nacional de Rectores (CONARE), y Cámara de Tecnologías de Información y Comunicación en representación del sector privado. El Comité asesor es presidido por el Director de la DCFD.

Se realizó un trabajo de investigación en coordinación entre la DCFD, el BCCR y el TEC para estudiar los formatos que se podían utilizar en Costa Rica para los certificados digitales, el resultado es la Política de Formatos que está vigente actualmente. Además se conformó un sub comité con funcionarios del Ente Costarricense de Acreditación (ECA), MICIT, BCCR y la Universidad de Costa Rica, que laboró en el año 2007 en la interpretación de la norma ISO 17021:2007, con el objetivo de establecer una guía para la implementación de los procesos necesarios para ejercer su cumplimiento, y continuar de esta forma el camino hacia la adopción de estándares internacionales.

En esta etapa, con la puesta en operación de la Autoridad Certificadora del BCCR para la emisión de certificados de personas físicas y jurídicas, el SNCD entró en una fase en la que el principal objetivo fue la emisión de certificados y educación y capacitación de los habitantes, empresas y entes de gobierno para el uso de firma digital. En abril del 2014, con el anuncio de la directriz gubernamental 067-MICITT-H-MEIC [8], que facultó al ciudadano costarricense a exigir la prestación de servicios por medio de la firma digital en todas las entidades de Gobierno y el llegar a más de 100.000 certificados emitidos, los diversos actores involucrados del SNCD iniciaron un proceso de auto evaluación, con el objetivo

Cuadro I
PLAN DE PROYECTOS FIRMA DIGITAL UCR – MICITT – BCCR 2013 - 2016, PROYECTOS EN DESARROLLO, AVANZADOS O CONCLUIDOS

Proyecto	Estado
Evaluación de requisitos para la CA Nacional	Concluido, listas las recomendaciones. Pasa a ser proyecto de certificación Webtrust
Modelo para auditar aplicaciones	Listo borrador de la propuesta técnica, en revisión MICITT/BCCR
Esquemas de certificación de CA y aplicaciones de software	Listos borradores, en revisión con MICITT y realizando ajustes para tener primera versión completa

de mejorar y prepararse para un uso masivo de la firma digital. Este proceso es el que inicia la segunda etapa.

VII. SEGUNDA ETAPA

Con los principales componentes del SNCD en operación, el siguiente objetivo fue el aseguramiento de la calidad de los componentes del sistema, especialmente en términos de seguridad. Para esto se crearon varios proyectos de investigación entre el MICITT, el BCCR y el Centro de Investigaciones en Tecnologías de Información y Comunicación (CITIC) de la Universidad de Costa Rica. También se hizo un esfuerzo inicial con un proyecto de graduación de estudiantes de la Universidad Nacional. Un breve resumen de estos proyectos se muestran en el cuadro I.

El primer proyecto consistía en analizar estándares internacionales para la certificación de Autoridades Certificadoras en PKI y evaluar su aplicabilidad dentro del SNCD. El problema que se identificó fue que se concluyó que la definición de los requisitos estipulados en el Artículo 11 del Reglamento a la Ley 8454 no eran lo suficientemente claros, factibles y apegados a la realidad y necesidades nacionales. El proyecto de investigación nació de la necesidad de sustentar si algún estándar existente a nivel internacional podía ser utilizado como base para la definición de los requisitos de implementación de una Autoridad Certificadora dentro del SNCD de Costa Rica. Los resultados obtenidos se pueden consultar en [9].

El segundo proyecto consistió en definir un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en una aplicación de software dentro del SNCD. El problema que se identificó fue que había una carencia de regulaciones a nivel nacional para garantizar el aseguramiento de la información de las aplicaciones de software que implementan mecanismos de firma digital dentro del SNCD lo cual supone un riesgo para la confianza y el no repudio de dicho sistema. Para conseguirlo, se utilizó un enfoque sistémico y sistemático, que soporta aplicaciones de software desarrolladas con diferentes tecnologías e infraestructuras, y a través del cual se valoraron riesgos, se definieron políticas de seguridad, y se establecieron objetivos de control. Como resultado, se propuso una guía de implementación cuya finalidad es servir de herramienta para evaluar el cumplimiento de un conjunto de requisitos de seguridad de la información, definidos para aplicaciones de software que utilizan firma digital en Costa Rica. Los resultados se pueden consultar en [10].

Finalmente, a partir de los resultados de estos proyectos se crearon esquemas de certificación utilizando los estándares ISO-17067 e ISO-17065. Los resultados se pueden consultar en [11]. Con los proyectos anteriores, en la etapa de revisión y consulta pública el siguiente objetivo fue la expansión y mejoramiento de los procesos de firma e interacción entre los distintos componentes. Los proyectos que se encuentran en ejecución actualmente se presentan a continuación.

VIII. TERCERA ETAPA

La tercera etapa incrementó el número de proyectos que se están realizando. Esta etapa inició a finales de 2016 y se encuentra en ejecución actualmente. Un breve resumen de los proyectos en ejecución se presenta en el cuadro II. Con el conocimiento adquirido durante el proyecto de evaluación de las CA se está realizando un proceso de mejoramiento de la Política de Certificado Nacional. Además, se está en el proceso de migrar de ISO-21188 a Webtrust como estándar para la certificación de CAs. Estos se están realizando entre el MICITT, el CITIC, el Centro de Informática de la UCR y el BCCR.

También se están realizando un par de desarrollos de software, para integrar Shibboleth, una herramienta para la implementación de Single Sign On, y un componente universal de firma, validación y autenticación (FVA) que está desarrollando el BCCR. También se está desarrollando un componente de firma para el suite de LibreOffice. Estos desarrollos serán liberados como software libre para el uso de la comunidad.

Adicionalmente se está realizando un proceso de evaluación de los perfiles de los formatos para los certificados y una aplicación modelo para el correcto uso de las mejores prácticas de programación en aplicaciones que interactúan con certificados digitales.

IX. LECCIONES APRENDIDAS

Todos los proyectos desarrollados en la segunda y tercera etapa se han realizado con distintos tipos de recursos: investigadores docentes, investigadores estudiantes (pregrado y posgrado), proyectos finales de graduación de Maestría, tanto de la UCR, del Tecnológico de Costa Rica (TEC) y de la Universidad Nacional (UNA). Se han incluido expertos de la realidad nacional, así como funcionarios del Banco Central y del Ministerio de Ciencia, Tecnología y Comunicaciones.

El aporte de las instituciones de educación superior ha sido principalmente en proveer resultados de alta calidad, con sustento académico, mediante la utilización de metodologías de investigación para la obtención de resultados: además el acceso a recurso humano en términos de investigadores y estudiantes con la disponibilidad de realizar estas investigaciones. Cabe destacar que el beneficio es bidireccional, ya que la Universidad se beneficia de la oportunidad de aportar a la

Cuadro II
PLAN DE PROYECTOS FIRMA DIGITAL UCR – MICITT – BCCR 2017 - 2018, PROYECTOS EN PROPUESTA O INICIANDO EL DESARROLLO

Proyecto	Estado
Versión mejorada del CPS Nacional	En desarrollo la propuesta (proyecto graduación)
Evaluación/certificación Webtrust	En elaboración con UCR, MICCIT y BCCR
Autenticación con firma Shibboleth+FVA	En desarrollo la infraestructura y la integración con FVA
Componente para firmar LibreOffice	Avanzando en el desarrollo e iniciando interacción con personal de desaarrollo de BCCR
Aplicación ejemplo de OIDs	En desarrollo la propuesta (proyecto graduación)
Perfiles de formatos para certificados	En desarrollo la propuesta (proyecto graduación)
Software Modelo Infosec-Tree	En búsqueda de recursos y pre-propuesta
Estándar ISO	En búsqueda de recursos y pre-propuesta

realidad nacional, obtener espacios de investigación para sus estudiantes y la generación de publicaciones de alta relevancia para el país.

Lo destacable de este proyecto con respecto a otros de cooperación entre distintos sectores es que la cantidad de conocimiento generado a nivel técnico, legal, administrativo y científico es grande en comparación con la cantidad de recursos que los diversos proyectos han tenido a su disposición.

X. CONCLUSIONES

Este artículo presenta la metodología y resultados obtenidos durante un proceso de colaboración de 15 años entre distintos actores del Gobierno de Costa Rica, la industria y las universidades públicas para el desarrollo y mejoramiento del Sistema Nacional de Certificación Digital.

En primera instancia se trabajó en el desarrollo del marco legal y de las Autoridades Certificadoras necesarias para el desarrollo de una PKI para proveer firma digital en Costa Rica. En segunda instancia, se inició un proceso de aseguramiento de la calidad de los distintos componentes del SNCD. Para esto se realizaron proyectos de investigación entre el MICITT, el BCCR y la UCR. El objetivo fue evaluar cuáles estándares internacionales se podían utilizar para implementar procesos de aseguramiento de la calidad, especialmente para dos componentes: Autoridades Certificadoras y aplicaciones de software. La tercera etapa inició en 2017 e incluye la expansión de los servicios disponibles de firma digital, tanto a nivel gubernamental como de la industria.

Es importante recalcar que gracias a la colaboración entre los actores antes mencionados, Costa Rica ha desarrollado un Sistema Nacional de Certificación robusto y se encuentra al frente de los esfuerzos relacionados con firma digital en América Latina (junto con Brazil y Chile), sirviendo de modelo para otros países para el desarrollo de sus infraestructuras de llave pública, como El Salvador y Panamá.

Finalmente, los resultados obtenidos en los proyectos desarrollados han generado productos tales como estándares, metodologías de aseguramiento de la calidad, de análisis de riesgos nuevos realizados tras proyectos de investigación de validez científica, y están siendo evaluados para ser propuestos como estándares internacionales en el campo.

XI. TRABAJO FUTURO

El trabajo futuro se divide en dos grupos. Primero, se deben completar los proyectos que están actualmente en ejecución. Estos brindarán un ecosistema más fácil de utilizar y permitirá un desarrollo más ágil de aplicaciones de software que utilicen firma digital. En segundo lugar, varios de los estándares y esquemas desarrollados serán propuestos como normas técnicas nacionales y posteriormente como estándares internacionales, lo que pondrá al país como parte de los contribuyentes al estado del arte en firma digital y PKI.

AGRADECIMIENTOS

La realización de este trabajo de investigación no hubiera sido posible sin la colaboración del MICITT, y del Banco Central de Costa Rica. Además, se agradece la ayuda obtenida del Centro de Investigaciones en Tecnologías de la Información y Comunicación, el Posgrado en Computación e Informática, la Escuela de Ciencias de la Computación e Informática, y el Centro de Informática, todos de la Universidad de Costa Rica. Gracias por fomentar el trabajo de investigación y el apoyo al mejoramiento de la realidad nacional mediante este tipo de proyectos de investigación.

REFERENCIAS

[1] *The Triple Helix – University-Industry-Government Relations: A Laboratory for Knowledge Based Economic Development*, vol. 14, 1995.
[2] S. U. T. H. R. Group. The triple helix concept. [Online]. Available: https://triplehelix.stanford.edu/3helix_concept
[3] A. W. Johannes A. Buchmann, Evangelos Karatsiolis, *Introduction to Public Key Infrastructures*. Springer, 2013.
[4] T. Housley, Russ; Polk, *Planning for PKI*. Wiley Computer Publishing, 2001.
[5] J. Stapleton and W. C. Epstein, *Security without Obscurity: A Guide to PKI Operations*. Auerbach Publications, 2016.
[6] *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*, vol. CXXVII, 2005.
[7] A. B. Edwin Solorzáno, "Reglamento a la ley de certificados, firmas digitales y documentos electrónicos," Dirección de Certificadores de Firma Digital, Tech. Rep., 2006.
[8] *Masificación de la implementación y el uso de la firma digital en el sector público costarricense*, vol. 79, 136.
[9] R. A. Bartels, "Análisis de estándares internacionales para la certificación de autoridades certificadoras y su aplicabilidad en el sistema nacional de certificación digital de costa rica," Ph.D. dissertation, Universidad de Costa Rica, 2016.
[10] A. Mora, "Definición de un proceso de aseguramiento de la información para los componentes tecnológicos, que utilizan certificados y firma digital en una aplicación de software dentro del sistema nacional de certificación digital," Ph.D. dissertation, Universidad de Costa Rica, 2017.
[11] V. R. Bartels R., "Diseño de un esquema de certificación para las autoridades certificadoras del sistema nacional de certificación digital de costa rica," *Simposio de Informática en el Estado*, 2017.