TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 2, mayo-agosto, 2018, p.13- 23 ISSN 1729-3804

DIGITAL DE DOCUMENTOS PDF EN DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID

Diannet Sospedra López[1], Carlos Asiel Pina Orozco[2], Acela María Sanamé Pérez[3]

Universidad de las Ciencias Informáticas, Cuba, Carretera a San Antonio de los Baños km 2½, Torrens, Boyeros, La Habana, CP: 19370
[1]e-mail: dsospedra@uci.cu

RESUMEN

El certificado digital es el documento electrónico generado por una entidad de servicios de certificación que permite identificar a la persona que firma el documento de forma oficial. Se trata de una confirmación de la identidad de la persona, para proteger datos y establecer conexiones de red seguras. A diferencia de la firma manuscrita, la firma digital es difícil de falsificar ya que contiene información codificada que es única del autor de la firma y que puede verificarse. Actualmente en la Universidad de las Ciencias Informáticas (UCI) se utiliza la herramienta DigiSigner versión 4.0, mediante la cual se realiza la firma digital de documentos realizando la solicitud y obtención del certificado digital, los cuales son gestionados por la Dirección de Seguridad Informática (DSI) de la propia universidad. Sin embargo, la DSI detecta la necesidad de realizar la firma de los documentos digitales no solo en las estaciones de trabajo desktop, sino que los usuarios puedan realizar la misma en los dispositivos con sistema operativo Android, teniendo en cuenta su amplia utilización por los directivos, profesores y especialistas de la producción en la universidad. En la presente investigación se expone el resultado obtenido con el desarrollo del sistema PDFDISIG versión 1.0, aplicación para firmar documentos con formato PDF desde dispositivos con sistema operativo Android. Surge a petición de la DSI y es desarrollada por el Departamento de Desarrollo de Aplicaciones del Centro de Telemática (TLM), perteneciente a la Facultad 2 de la UCI.

PALABRAS CLAVE: Android, certificado digital, documento digital, firma digital.

DIGITAL SIGNATURE OF PDF DOCUMENTS IN DEVICES WITH ANDROID OPERATING SYSTEM

ABSTRACT

The digital certificate is provided by the electronic document generated from certification services of a given entity, which in turn allows to identify the person who signed the document in an official way. It is a confirmation of the identity of the person, to protect data and establish secure network connections. Unlike the handwritten signature, digital signature is difficult to counterfeit since it contains encoded

information that is unique to the author of the signature and can be verified. Currently, the DigiSigner version 4.0 tool, is used by the University of Informatics Sciences (UCI), through which the digital signature of documents is made by requesting and obtaining the digital certificate, which are managed by the Directorate of Informatics Security (DSI) of the university itself. However, the DSI detects the need to make the signing of digital documents not only from desktop work stations, but users can perform the same on devices with Android operating systems, taking into account its extensive use by managers, teachers and production specialists at the university. In the present investigation, the result obtained with the development of the PDFDISIG version 1.0 system is presented, an application for signing documents in PDF format from devices with an Android operating system. It arises at the request of the DSI and is developed by the Applications Development Department of the Telematics Center (TLM), belonging to the Faculty 2 of the UCI.

KEYWORDS: Android, digital certificate, digital document, digital signature.

INTRODUCCIÓN

El certificado digital puede ser un elemento muy útil para las organizaciones, permitiendo que hoy día múltiples trámites empresariales puedan realizarse de forma telemática, es decir, utilizando las conexiones de red para ejecutarlos. La utilización de los certificados digitales tiene como ventajas: el ahorro de tiempo, ya que no es necesario realizar gestiones con la administración físicamente, esperando colas y generando atascos; se aporta eficiencia a los recursos humanos de una empresa, puesto que no será necesario que otra persona gestione los documentos más tiempo para recopilar la información que sea necesaria, sin poner en riesgo el envío de la misma fuera de plazo. Todo esto, a su vez, genera un ahorro económico para las corporaciones [1].

Una firma digital, identifica a la persona que firma un documento. A diferencia de la firma manuscrita, la firma digital es difícil de falsificar porque contiene información codificada que es única del autor de la firma y que puede verificarse fácilmente. La mayoría de las firmas digitales se conocen como firmas de aprobación [2]. También existen las firmas de certificación digital; estas son las que se utilizan para certificar documentos y en la mayoría de los casos el propio autor es el único que puede certificarlo. Este tipo de firma certificada permite avalar el contenido y la integridad del documento, así como establecer permisos para ciertos cambios que puedan ocurrir en el documento según el propósito del mismo. Es decir, al certificar un documento, el autor puede bloquear o permitir cambios que terceras personas puedan hacerle al contenido del documento. Como ejemplo se podrían citar el agregar o eliminar páginas al documento, rellenar tablas o formularios, comentar sobre el contenido, etc. El bloqueo o acceso a todas estas operaciones puede definirse para usuarios específicos en el proceso de certificación, el cual solamente es llevado a cabo gracias al uso de ID digitales.

El ID digital, es una identificación digital que permite diferenciar y representar la identidad de la persona frente a entidades o personas con las que se comunica electrónicamente [3]. Este ID es comparado en varias bibliografías como un carnet de identidad digital el cual almacena el nombre, correo electrónico, el nombre de la empresa que emitió su ID digital, un número de serie con fecha de caducidad, etc. Este tipo de identificación digital, se almacena regularmente de manera local en el equipo o computadora donde se elaboran los documentos a firmar y están dentro de ficheros contenedores con extensión ".p12". Estos ficheros albergan una clave privada que solo el autor debe conocer y una pública para compartir los documentos firmados. Este fichero llamado “.p12”, está protegido con una contraseña que

la Autoridad Certificadora (Certification Authority o CA) le asigna para proteger la confidencialidad del mismo y para que solo el propietario de ese ID digital lo pueda manipular.

La Universidad de las Ciencias Informáticas (UCI), desde su creación se ha dedicado a la producción y comercialización de software, insertándose en esta compleja industria mediante convenios de cooperación con varias naciones e instituciones [4]. Desde el año 2015 se comenzó a fomentar en la universidad el uso y empleo de las firmas digitales utilizándose diferentes herramientas desarrolladas en la propia institución que faciliten la obtención de un certificado digital mediante la Autoridad Certificadora UCI [5]. El proceso de obtención de los certificados digitales es gestionado por la Dirección de Seguridad Informática (DSI) de la universidad, la cual define un conjunto de pasos a seguir para su correcto funcionamiento [6]:

1. Solicitar el certificado digital: para solicitar un certificado digital el usuario debe llenar los datos de la planilla de solicitud que se encuentra publicada en el sitio https://seguridad.uci.cu. Luego este recibirá un correo electrónico enviado por la CA UCI con el usuario y la contraseña para generar su certificado.
2. Obtención del certificado digital: para obtener el fichero contenedor del certificado digital, fichero conocido como ".p12". Estos ficheros contienen la clave privada y el certificado de clave pública asociado a su usuario. Para ello se accede al enlace de la CA UCI y se selecciona la opción de "Generar mi certificado digital", el cual debe ser almacenado por el usuario.
3. Cambio de contraseña del certificado digital: una vez guardado el archivo ".p12" es necesario que el usuario cambie la contraseña que se le envió por correo para mayor seguridad.
4. Obtención e instalación del certificado digital de CA: la instalación de este certificado permitirá a las aplicaciones o software clientes verificar que un determinado certificado es válido.

La DSI ha detectado la necesidad de realizar la firma de los documentos digitales no solo en las estaciones de trabajo desktop, sino que los usuarios puedan realizar la misma en los dispositivos con sistema operativo Android, teniendo en cuenta su amplia utilización por los directivos, profesores y especialistas de la producción en la universidad. En la presente investigación se expone el resultado obtenido con el desarrollo del sistema PDFDISIG versión 1.0, aplicación para firmar documentos con formato PDF desde dispositivos con sistema operativo Android. Surge a petición de la DSI y es desarrollada por el Departamento de Desarrollo de Aplicaciones del Centro de Telemática (TLM), perteneciente a la Facultad 2 de la UCI.

DESARROLLO

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes. Es el documento electrónico generado por una entidad de servicios de certificación que permite identificar a una persona ante terceros de forma oficial. Se trata de una confirmación de identidad, que contiene información usada para proteger datos o establecer conexiones de red seguras. [1]

Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona). Los certificados digitales sólo son útiles si existe

alguna CA que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo reconozca.

Es importante ser capaz de verificar que una CA ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la CA después de autentificar la identidad de un sujeto, firma el certificado digitalmente. Los certificados tienen un período de validez que va de unos meses a unos pocos años. Durante el tiempo que el certificado es válido la CA que lo generó mantiene información sobre el estado de ese certificado. La información más importante que guarda es el estado de anulación, que indica que el período de validez del certificado ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en este. Las razones de anulación de un certificado son varias: la clave privada del sujeto se ha visto comprometida, la clave privada de la CA se ha visto comprometida o se ha producido un cambio en la afiliación del sujeto (por ejemplo, cuando un empleado abandona una empresa).

FIRMA DIGITAL PDFDISIG

PDFDISIG surge con el objetivo de desarrollar una herramienta que permita firmar documentos digitales en dispositivos con sistema operativo Android, para así facilitar a los directivos de la universidad una aplicación. Mediante esta aplicación, desde cualquier dispositivo que contenga Android como sistema operativo, se habilitará firmar digitalmente un documento utilizando el certificado digital generado por la CA de la universidad. A continuación, se especifican las diferentes herramientas y tecnologías utilizadas para su desarrollo.

Librería iText

Para la manipulación de los archivos PDF se utiliza la librería iText, disponible bajo una licencia de código abierto. iText es una librería de código abierto gratuita para crear y manipular ficheros PDF. Permite al desarrollador utilizar las siguientes funcionalidades [7]:

- Servir un PDF a un navegador.
- Crear documentos dinámicos a partir de un fichero XML o una base de datos.
- Usar funcionalidades interactivas de los PDF.
- Añadir marcadores de página, número de página, marcas de agua, códigos de barras, etc.
- Separar, concatenar y manipular páginas PDF.
- Rellenar automáticamente formularios PDF.
- Añadir firmas digitales a un fichero PDF.

Es por esta última característica que ha sido necesario incluir la librería en el proyecto facilitando el desarrollo de la solución. Sin embargo, iText hace uso de Bouncy Castle como proveedor de seguridad, el cual contiene un paquete de algoritmos criptográficos necesarios para realizar las operaciones de creación y verificación de las firmas específicamente. La plataforma Android, desafortunadamente, cuenta con una versión reducida de Bouncy Castle, haciendo que la instalación de una versión actualizada de las bibliotecas sea difícil debido a conflictos con el classloader. Como alternativa para dar solución a esta problemática se utiliza Spongy Castle, que no es más que la propia biblioteca Bouncy Castle con varios ajustes para que funcione en Android.

Seguridad

La aplicación utiliza un archivo contenedor con formato ".p12". Como mecanismo de seguridad este archivo se encuentra encriptado y protegido con contraseña, la cual es solicitada al usuario en el momento de adjuntar una firma a un documento. De esta forma todo el esquema de seguridad y de protección de la información de los usuarios recae en la autenticación del fichero contenedor que limita el acceso al certificado y la clave privada incluida dentro del mismo.

Arquitectura

El sistema tiene una arquitectura basada en capas, permitiendo la creación de una aplicación adaptable, basándose en las ideas de reutilización de código y separación de conceptos para facilitar el desarrollo y el posterior mantenimiento. La capa de persistencia de datos contiene los modelos y otra capa de abstracción subyacente sobre el ORM que implementa el Patrón Repositorio. La capa de vistas abarca todas las clases que permiten darle vida a las interfaces, separando estas en tres grupos principales: Activities, Fragments y Preferences. Por último, la capa de presentación, que contiene todas las interfaces con que interactúa el usuario, las cuales son construidas en XML, donde se definen los componentes visuales y su estructura.

Gestor de Base de Datos

Se utiliza SQLite 3.x como motor de bases de datos, el cual tiene como característica fundamental que es gestor ligero siendo ideal para dispositivos móviles. Además, no necesita un servidor de base de datos y es relativamente simple su utilización, pues se pueden crear y manejar bases de datos de forma sencilla y con toda la potencia que brinda el lenguaje SQL. Cubre todo el modelo de la solución exceptuando los parámetros de configuración de la aplicación que son gestionadas por las preferencias compartidas de Android.

Tecnología ORM

ORMLite 4.49. es un proyecto Open Source que provee un mapeo relacional de objetos entre clases de Java y bases de datos SQL, por lo que soporta SQLite y Android [8]. Posee potentes clases DAO (conocido como patrón Data Access Object) abstractas y se pueden construir consultas simples o complejas con facilidad debido a su flexibilidad.

Lenguaje de Programación Nivel Negocio

Se utiliza Java por ser el lenguaje de programación seleccionado por Google para dar soporte a los desarrolladores de aplicaciones Android, por lo que posee una amplia documentación que cuenta con tutoriales, foros y códigos de ejemplo sobre cada API de este sistema operativo.

Tecnología Ambiente Integrado de Desarrollo (IDE)

Como IDE se utiliza Android Studio 2.3, disponible de forma gratuita bajo la licencia de Apache 2.0, este ofrece un entorno de desarrollo claro y robusto; facilidad para probar el funcionamiento de las

aplicaciones en varios tipos de dispositivos y entre otras características posee un completo editor con múltiples herramientas para agilizar el desarrollo.

RESULTADOS Y DISCUSIÓN

A continuación, se describen las funcionalidades que brinda el sistema PDFDISIG. Inicialmente la primera pantalla que muestra la aplicación es el logo del apk (Figura 1).

Figura 1: Logo del sistema PDFDISIG

Una vez iniciada la aplicación se abre directamente el listado de archivos PDF con los que se ha trabajado recientemente. Dentro de la misma vista la aplicación permite buscar los documentos que se encuentran almacenados en el dispositivo al que se desea plasmar la firma digital (Figura 2).

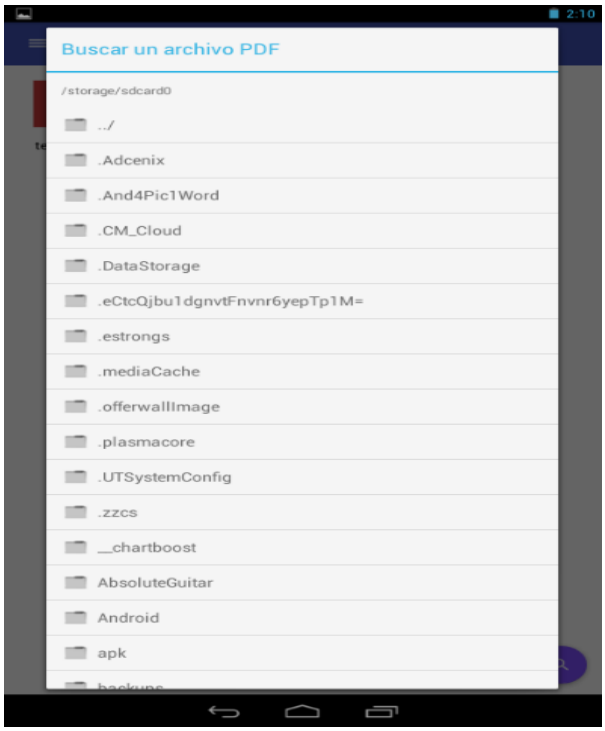

Figura 2: Buscar un archivo PDF

Una vez cargado y abierto el documento la aplicación muestra en la parte inferior las opciones Adjuntar firma y Verificar firma. Al seleccionar la opción Adjuntar firma aparece una ventana con las siguientes opciones de firma (Figura 3):

- Contraseña del archivo contenedor: se debe escribir la contraseña del keystore. En caso en que la contraseña sea incorrecta se muestra el mensaje “Contraseña incorrecta o archivo contenedor corrupto”.

- Motivo de la firma: opcionales.
- Ubicación: opcional.
- Usar servidor TSA: marcar solo si se desea utilizar un servidor TSA.
- Opciones de visualización de firma: debe seleccionar si desea una descripción, una imagen o ambas.

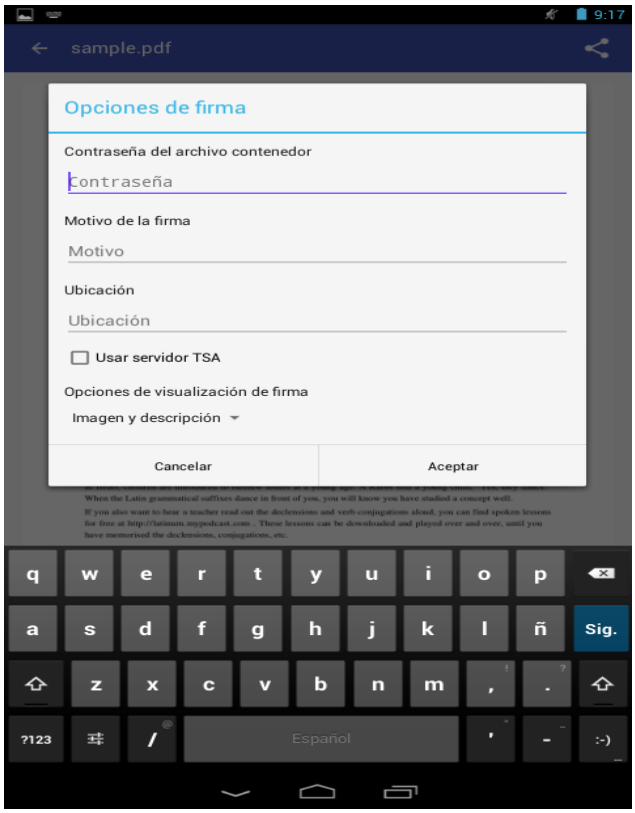

Figura 3: Adjuntar Firma

Si el usuario intenta firmar un documento dos veces con el mismo certificado la aplicación mostrará el mensaje “El documento ya ha sido firmado usando ese certificado”. En caso en que se desee utilizar un servidor TSA y no se pueda establecer la conexión, la aplicación muestra el mensaje “Conexión fallida con el servidor TSA”.

Cuando el documento es firmado se muestra el mensaje “Operación exitosa”. Al seleccionar la opción de Verificar se muestra una ventana con las propiedades de la firma (Figura 4). En caso de que el usuario intente verificar un documento que no ha sido firmado la aplicación muestra el mensaje “El documento no ha sido firmado”.

Se brinda la opción de compartir el documento firmado utilizando las diferentes aplicaciones que contiene el dispositivo que permitan enviar el documento. La aplicación cuenta con un menú lateral donde se encuentran las diferentes acciones a realizar o consultar dentro del apk: recientes, historial de firmas, ajustes, ayuda & comentarios (Figura 5). El menú se accede deslizando el dedo de izquierda a derecha en la pantalla o a través del icono que se encuentra en la parte superior izquierda.

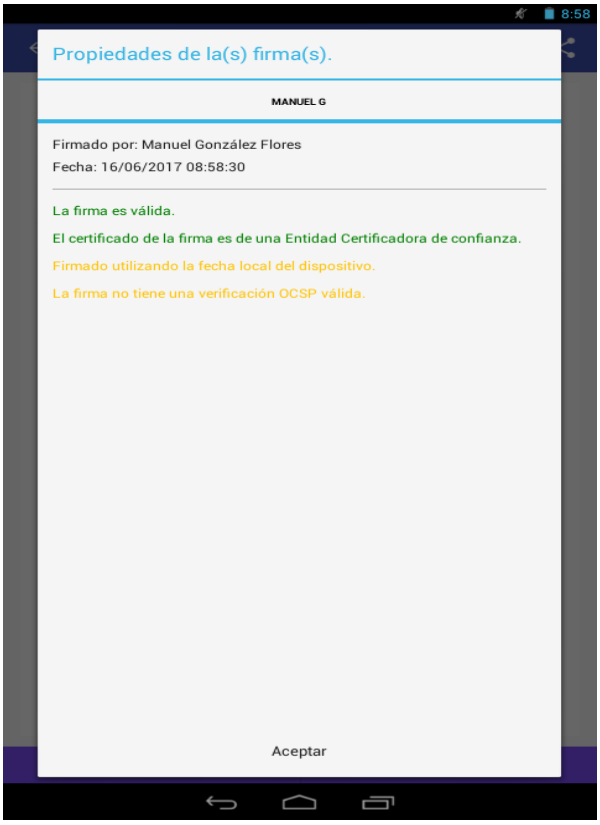

Figura 4. Verificar firma

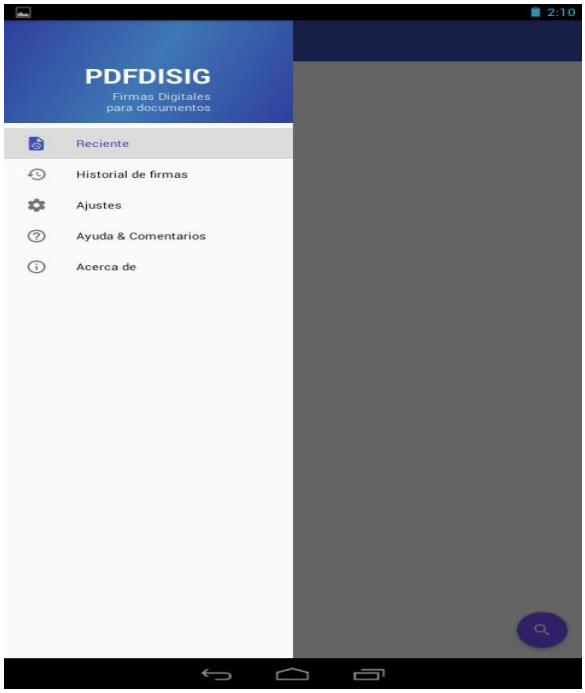

Figura 5. Menú lateral

El historial de firmas muestra el listado de los documentos que han sido firmados y permite visualizarlo. En la sección de Ajustes se muestra un conjunto de opciones que deben ser especificados por el usuario, divididos en las categorías que se describen a continuación (Figura. 6).

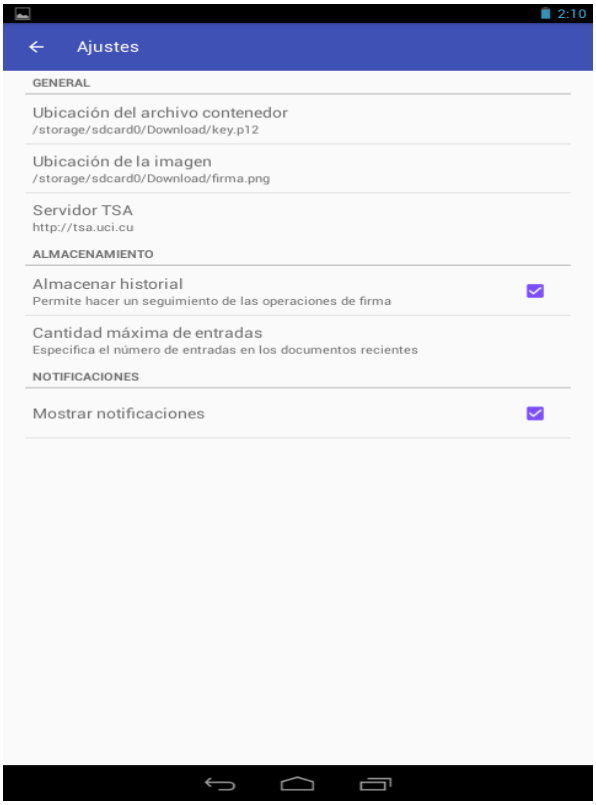

Figura 6. Ajustes

Dentro de la categoría General se deben especificar:

- Ruta del keystore: se debe ubicar dentro del dispositivo la ruta del archivo contenedor del p.12.
- Imagen de firma: se debe seleccionar la ubicación de la imagen de la firma que se desea plasmar en el documento.
- Servidor TSA: se especifica la dirección del servidor TSA que se desea utilizar.
- Almacenamiento: en esta categoría el usuario permite o no dentro del almacenamiento del historial mantener un registro de las operaciones de firmado. Además, debe especificar el máximo número de entradas que se mostrarán en los documentos recientes.
- Notificaciones: permite seleccionar si desea que la aplicación muestre las notificaciones.

Mediante la sección de Ayuda & Comentarios se da respuesta a las principales interrogantes que puedan surgir para realizar la firma y configurar la aplicación. Permite además enviar vía correo los comentarios que deseen realizar (Figura. 7).

Figura 7. Ayuda & Comentarios

CONCLUSIONES

La aplicación PDFDISIG cumple el objetivo por el cual fue desarrollado, mediante la obtención de un certificado digital por la CA de la UCI, los usuarios logran firmar documentos PDF mediante un dispositivo con sistema operativo Android. Actualmente el sistema se encuentra liberado por la DSI y Dirección de Informatización de la UCI, quienes consideraron que está lista para su empleo por los especialistas, profesores y directivos de la organización. Aun siendo una pequeña solución tiene un gran potencial de desarrollo e integración con otras herramientas ya utilizadas en la universidad que gestionan las versiones de los documentos generados en los proyectos de desarrollo de software. Por lo que se consideró importante en su diseño fomentar un desarrollo que sea fácil de expandir y mantener.

REFERENCIAS

[1] Sergio Talens-Oliag: "Introducción a los certificados digitales". Universidad de Valencia, España. https://www.uv.es/sto/articulos/BEI-2003-11/certificados_digitales.html. [Accessed: 28-Enero-2018]

[2] Suárez, Ibérico: "Mejoramiento de la gestión de trámite documentario utilizando firma digital en el Proyecto Especial Alto Mayo-Moyobamba.", Tesis de maestría, Universidad Nacional de San Martín, Perú, 2013.

[3] Carrera, Xavier, and Jordi L. Coiduras Rodríguez: "Identificación de la competencia digital del profesor universitario: un estudio exploratorio en el ámbito de las Ciencias Sociales." Red-U: Revista de docencia universitaria, 2012, vol. 10, num. 2, pp. 273-298. 2012.

[4] UCI. Universidad de las Ciencias Informática, Historia. (Sitio oficial). 2018.

[5] Martínez, Norbert Said: "Módulo de integración de la Infraestructura de Clave Pública con el Sistema de Administración de Identidades del Ministerio del Interior", Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas, UCI, 2010.

[6] DSI: Manual para la solicitud y obtención de Certificados Digitales, Dirección de Seguridad Informática (DSI), Vicerrectoría de Producción UCI, 2016.

[7] NAVARRO MARTIN, Adrià: "Estudio e implementación de un framework de desarrollo de aplicaciones con funciones de seguridad y privacidad para móviles". Tesis de Ingeniería Informática, Universitat Politècnica de Catalunya (UPC), BarcelonaTech 2013.

[8] Watson, Gray: "ORMLite Package." Versión 5.0, 2016.