MANUAL DE USUARIO CERTIFICADO POR SOFTWARE

ANDROID - ADSIB

Versión 1.0

Código: ADSIB-INST-MAN-001 UNIDAD DE INNOVACIÓN Y DESARROLLO

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Alberto Daniel Inch Sáinz		Alberto Daniel Inch Sáinz
Cargo:	Jefe de la Unidad de Innovación y Desarrollo		Jefe de la Unidad de Innovación y Desarrollo
Firma:			
Fecha:	27/06/2019		27/06/2019

MANUAL DE CERTIFICADO POR SOFTWARE - ADSIB

1. Certificado por Software....3
2. Conceptos básicos....3
   2.1. Par de claves....3
   2.2. CSR....3
   2.3. Certificado de firma digital....3
   2.4. Entidad Certificadora Autorizada....4
   2.5. Dispositivo criptográfico por software....4
3. Preparando el dispositivo criptográfico por software listo para firmar....4
   3.1. Importar Token....5
   3.2. Abrir dispositivo criptográfico por software....6
   3.3. Generar par de claves....7
   3.4. Generar archivo CSR....8
   3.5. Cargado del certificado....9
4. Firma de documentos PDF....9

1. Certificado por Software

La firma digital en Bolivia nace como una alternativa a la firma manuscrita en el mundo de los documentos digitales el año 2016, para lo cual era necesario hacer uso de dispositivos criptográficos específicamente diseñados para la generación de par de claves. Sin embargo dada la necesidad de utilizar firma digital en sistemas de forma automática, el año 2019 se amplía la posibilidad de utilizar firma digital por software, es decir delegando a un programa la generación de par de claves.

Al eliminar la dependencia de dispositivos criptográficos, surge la necesidad de contar con un programa que se encargue de la generación del par de claves, al cual se lo denominó "Certificado por Software" y que puede ser descargado de playstore. Así mismo es de código abierto por lo que el código fuente está disponible en: https://gitlab.softwarelibre.gob.bo/adsib/fido-android.

2. Conceptos básicos

En términos simples la firma digital es el equivalente a la firma manuscrita en el mundo de los documentos digitales. Sin embargo para poder hacer uso de esta se debe comprender los siguientes conceptos:

2.1. Par de claves

La firma digital se basa en criptografía asimétrica, la cual se compone de un par de claves: "Clave privada" que sirve para firmar y "Clave pública" que sirve para validar la firma.

2.2. CSR

Un CSR (Certificate Signing Request) es un archivo que contiene la clave pública con los datos de identidad y que se envía a la ECA para que emita el certificado en base a la información contenida.

2.3. Certificado de firma digital

El certificado de firma digital viene a ser la "Clave pública" del signatario además de sus datos de identidad, ci, nombre entre otros.

2.4. Entidad Certificadora Autorizada

La Entidad Certificadora Autorizada ECA es la encargada de emitir Certificados de firma digital. Para que una firma digital tenga valor legal, debe contar con un Certificado de firma digital emitido por una ECA autorizada por la ATT.

2.5. Dispositivo criptográfico por software

El dispositivo criptográfico por software es un archivo con extensión p12 o pfx que contiene la clave privada del signatario y el certificado de firma digital cifrados por un algoritmo de criptografía simétrica que protege el contenido por contraseña.

3. Preparando el dispositivo criptográfico por software listo para firmar

Para contar con un dispositivo criptográfico listo para firmar documentos digitales, se debe iniciar el aplicativo “Firmador ADSIB” que desplegará la siguiente interfaz:

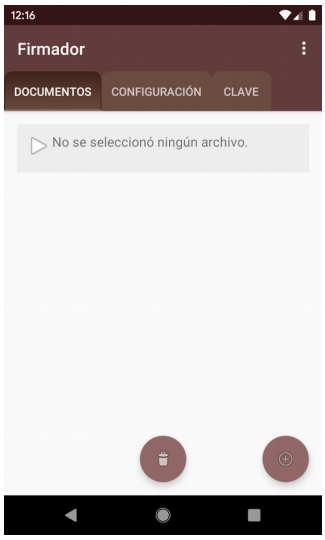

Fig. 1 Inicio aplicativo

En caso de contar con un dispositivo p12 para la firma digital por software puede cargar el mismo como se indica a continuación, en caso de que desee solicitar un nuevo certificado saltar al paso 3.3. Generar par de claves.

3.1. Importar Token

Para importar un dispositivo p12, se debe seleccionar la pestaña “CLAVE” y en el menú de la esquina superior derecha seleccionar “Importar Token”:

Fig. 2 Importar token

Seguidamente se abrirá el gestor de archivos para seleccionar el dispositivo p12.

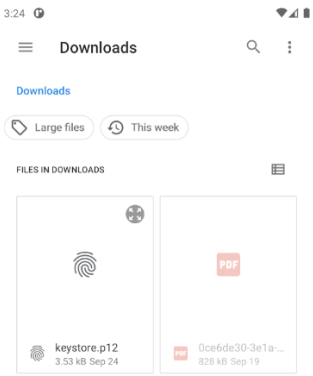

Fig. 3 Seleccionar archivo .p12

En la imagen de ejemplo se puede ver que ya se tiene descargado el archivo keystore.p12, el cual contiene el par de claves y el certificado ya emitido. Bastará con seleccionarlo y el programa pedirá la contraseña para concluir la importación.

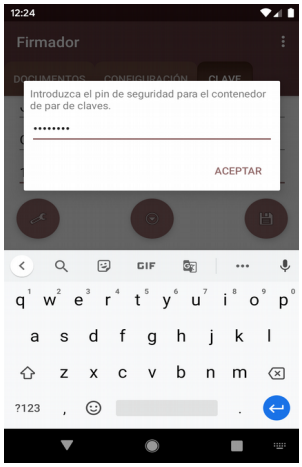

Fig. 4 Ingresar contraseña

3.2. Abrir dispositivo criptográfico por software

Una vez se ha guardado la clave privada en el dispositivo criptográfico p12, se podrá recuperar en cualquier momento a través de la pestaña “CLAVE”:

Fig. 5 Recuperar p12

Y una vez introducida, se abrirá mostrando los datos de identidad introducidos antes de guardar el archivo p12.

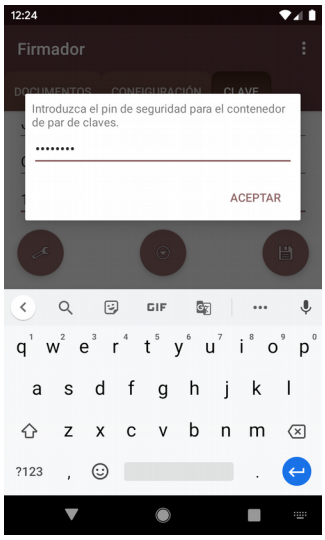

Fig. 6 Ingresar contraseña del archivo .p12

3.3. Generar par de claves

La generación de par de claves se la realiza a través de la pestaña “CLAVE”:

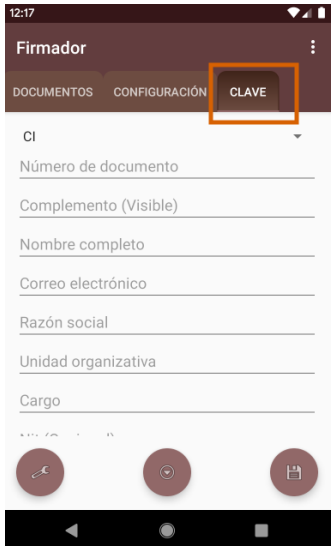

Fig. 7 Generar par de claves

En la cual se debe llenar los datos que serán utilizados para solicitar el certificado. Una vez hecho esto se pulsa el botón guardar que solicitará la contraseña para el dispositivo p12.

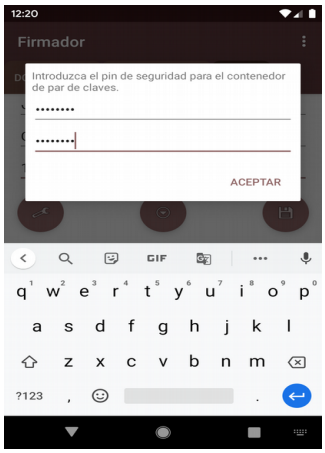

Fig. 8 Ingresar y confirmar contraseña

Con esto se crea el par de claves y se tiene todo listo para comenzar a trabajar. Los campos para llenar la identidad del signatario se habilitan para que puedan ser llenados.

El archivo p12 se crea en la memoria interna del celular en un espacio restringido para el resto de aplicaciones de manera que no sea de fácil acceso.

3.4. Generar archivo CSR

Para generar este archivo, bastará con hacer clic sobre el botón Generar CSR, el botón del medio. Se preguntará por la contraseña para almacenar los datos actualizados tal cual se exportan al CSR. Se guardará el archivo p12 actualizado y se creará un archivo solicitud.csr en la memoria del dispositivo móvil dentro de la carpeta adsib.

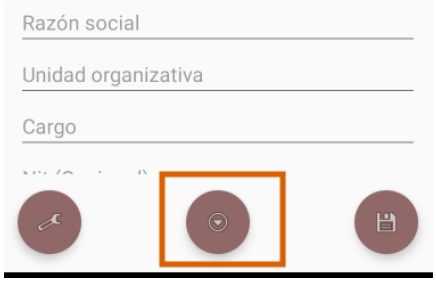

Fig. 9 Opción generar CSR

3.5. Cargado del certificado

Una vez se tiene disponible el certificado emitido por la ECA, el mismo deberá ser guardado juntamente con la clave privada en el archivo p12. Para lo cual se utiliza el botón de la izquierda.

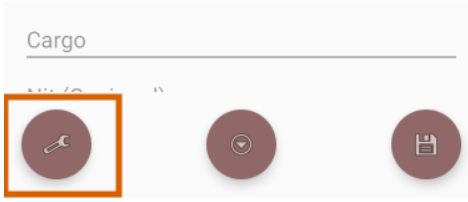

Fig. 10 Opción importar certificado

Para cargar el certificado, simplemente seleccionar el el archivo.

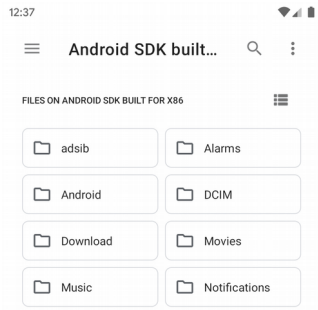

Fig. 11 Búsqueda del certificado

Una vez cargado se muestra un mensaje de confirmación con lo que el dispositivo criptográfico por software se encuentra listo para firmar.

4. Firma de documentos PDF

Con el dispositivo criptográfico por software listo como se indica en la anterior sección, es posible firmar documentos PDF desde esta misma aplicación a través de la pestaña “Documentos”. El botón agregar permite agregar documentos a la lista y en el menú se encuentra la opción firmar todo, que firmará todos los documentos.

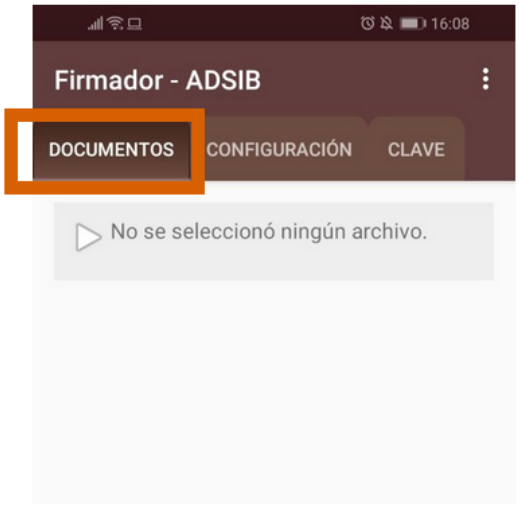

Fig. 12 Opción para firmar documentos

Al momento de abrir los archivos en caso de contar con firmas digitales, las mismas se validarán y se mostrará el nombre de los signatarios:

Fig. 13 Cargar documentos para firmar

Finalmente para firmar bastará con seleccionar del menú de la esquina superior derecha la opción “Firmar Todo” e introducir la contraseña del dispositivo p12.

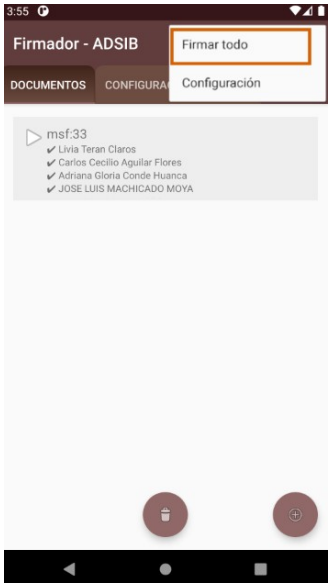

Fig. 14 Firmar documentos