Seguridad en el móvil Formiik

Versión 1.0

Autores:	David Cruz
Fecha de creación:	24/05/2017
Fecha de última actualización:	

Seguridad Móvil

El presente documento describe las diferentes estrategias que se siguen en el dispositivo para garantizar la seguridad de la aplicación móvil Formiik.

Existen diferentes vulnerabilidades en una aplicación móvil, como son:

1. Autenticación y validación de identidad de operaciones en la aplicación

Es muy importante que solo las personas indicadas puedan acceder a la aplicación y ejecutar las operaciones que su trabajo requieren, como pueden ser consultas o modificaciones de datos sensibles. En aplicaciones como Formiik donde se está jugando un papel de proveedor, es necesario que las credenciales del usuario no sean almacenadas para evitar malos usos.

2. Seguridad del canal de comunicaciones.

Mediante determinadas técnicas es posible conocer lo que se transmite en las llamadas de la aplicación móvil a la nube, por lo que es importante que estas comunicaciones viajen seguras y no sea posible conocer la información que se envía. No toda la información que se envía es sensible, pero la información sensible debe estar asegurada.

3. Base de datos en el dispositivo.

La base de datos que vive dentro del dispositivo, y que puede contener información sensible, es un archivo binario que pudiera abrirse para conocer su contenido. Es muy importante que esta información no pueda ser observada por personas no autorizadas.

4. Ingeniería inversa en la aplicación empaquetada

Una aplicación móvil como Formiik, se empaqueta en un archivo APK, que mediante técnicas de ingeniería inversa, es posible obtener el código fuente con el que fue creado. Es posible así modificar el código fuente y distribuir una versión malintencionada que pudiera estar observando los datos que se están utilizando. También existe el riesgo que si existiera información de la aplicación (credenciales para acceder a un recurso por ejemplo) en el código, podría también ser observado.

5. Robo del dispositivo

Los dispositivos móviles son muchas veces robados a las personas que están en campo, y la información que se tiene en ellos es sensible (información personal de los clientes) por lo que se debe proteger.

Para cada una de estas amenazas, se han desarrollado estrategias para que Formiik mantenga la información segura.

Soluciones para cada vulnerabilidad

1. Autenticación vía OAuth

Con el objetivo primordial de permitir a nuestros clientes manejar su propia seguridad y políticas, es posible utilizar Formiik para que la autenticación sea vía OAuth. Esto permite que Formiik no conoce nunca las credenciales de los usuarios que se firman, no sea necesario guardarlas, y al mismo tiempo, el Banco sea capaz de controlar sus propios accesos utilizando las políticas y tecnologías que mejor se acomoden a sus necesidades.

Formiik maneja una sesión, mediante la cual garantiza que las operaciones son ejecutadas por la persona que se autenticó.

Sesión

Una sesión es el permiso que se le otorga a un usuario en un dispositivo, después de que sus credenciales fueron validadas, para poder hacer operaciones en Formiik. Esta sesión tiene una vigencia, que es un momento en que ya no es válida esta sesión y es necesario renovar la sesión.

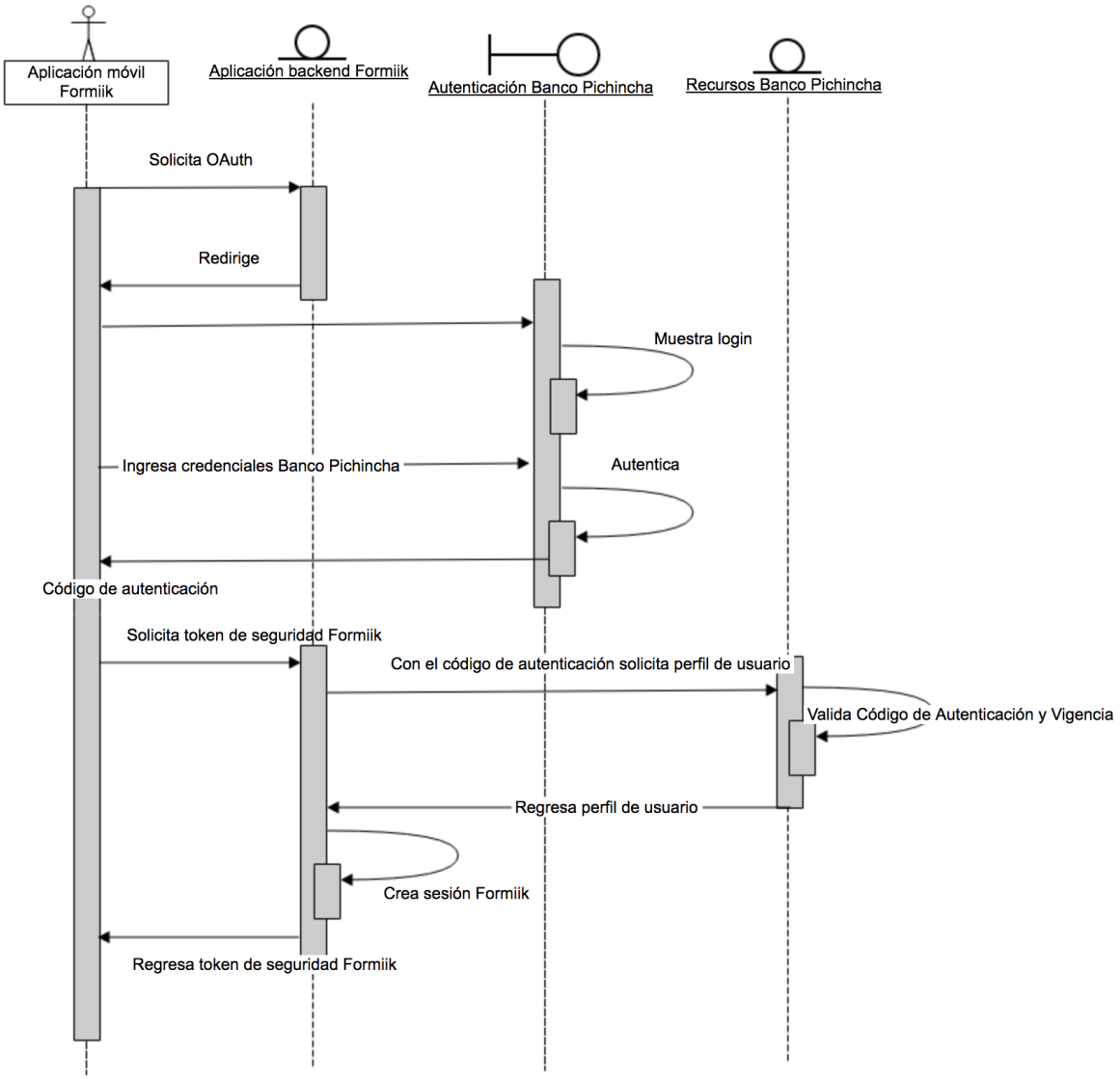
La vigencia de la sesión es configurable por usuario, y se maneja un valor default de 12 horas desde iniciada.

Por cada operación que se desee realizar, se valida dicha sesión y su caducidad. En caso de que caduque, se solicita que el usuario vuelva a autenticarse para crear una nueva sesión.

Abriendo una sesión

Un dispositivo móvil sin sesión vigente, muestra en el teléfono la pantalla de login. Al ser una autenticación vía OAuth, se despliega una página web de la entidad que solicita credenciales del usuario para verificarlas.

Una vez que el dispositivo móvil recibe una autorización de esta página, se envía desde esta entidad un código de autenticación. Con este código, el dispositivo, se solicita a la nube de Formiik que acceda a un recurso de la entidad, para obtener el perfil del usuario. Si es posible acceder al recurso del perfil, se crea un token de seguridad Formiik, el cual se envía al dispositivo junto con una vigencia. Esta es la sesión que el dispositivo móvil va a utilizar.
Como funciona se describe brevemente en el siguiente diagrama:



2. Uso de certificados en los canales de comunicación

Entre el dispositivo móvil y la nube de Formiik existen certificados SSL que demuestran la identidad de los servicios, al mismo tiempo que la información viaja cifrada mediante TLS 1.2 a 256 bits.

3. Encripción de Base de Datos

La base de datos de Formiik en el móvil, SQLite, es el repositorio donde se guarda la información sensible de los clientes. Esta base de datos es configurable para poder utilizar encripción. Mediante SQLCipher contamos con una encripción 256-bit AES. La llave para encriptar se encuentra en una librería escrita en C para evitar problemas de ingeniería inversa, y se construye leyendo el IMEI del dispositivo, así que cada llave de encripción es diferente para cada dispositivo.

4. Ofuscación del APK

Se utilizan técnicas para ofuscar el código en la creación del APK de Formiik. Así evitamos que se intente hacer una ingeniería inversa y se pueda hacer malos usos.

Por otro lado, para cada APK que se libera, se obtiene un hash del archivo generado, y se mantiene en un listado en la nube para validar que solo las versiones que generamos pueden hacer operaciones contra la nube de Formiik.

Adicionalmente es configurable por cliente, qué versiones de Formiik móvil pueden entrar, para así también garantizar que los usuarios están actualizados y normalizados.

5. Uso de MDM

Dentro del uso de Formiik se incluye el uso de un software de MDM (Mobile Device Management) que permite, aparte de monitorear los dispositivos e instalar versiones de aplicaciones, también el poder asegurar estos dispositivos en caso de robo.

De manera central, el MDM puede borrar el contenido de un dispositivo que haya sido reportado como robado, para evitar que quieran hacer mal uso de este.

Auditorías constantes

En Formiik estamos constantemente haciendo esfuerzos para detectar posibles huecos de seguridad. Sabemos que la información que se maneja por nuestros clientes es sensible y muy importante.

Es por eso que cada año solicitamos una asesoría de Ethical Hacking que nos ayuda a revisar, y con ojos externos, si existen vulnerabilidades que necesitamos atacar y solventar.

También fomentamos que nuestros clientes hagan sus propios estudios de ser necesario y así garantizar su seguridad. Formiik es un producto en constante evolución, y no solo estamos preocupados por las necesidades funcionales sino también de seguridad.