Política de privacidad TuID móvil

TuID

Versión 1.0

19/8/2019

POLÍTICA DE PRIVACIDAD

El objetivo de la aplicación móvil de TuID (en adelante, TuID móvil) es brindar el servicio de Identidad Digital y Firma Electrónica Avanzada a través de dispositivos móviles.
TuID móvil cuenta con todos los requisitos de seguridad necesarios para garantizar la protección de los datos personales y la seguridad en las transacciones.

1. Activación de TuID móvil

TuID móvil requiere de un proceso de activación que se inicia desde el portal de TuID www.tuid.uy por el titular de una Identidad Digital.

Para poder activar TuID móvil, el titular deberá autenticarse con un nivel alto (nivel 2 de registro) y seguir las instrucciones de activación disponibles en la sección de Aplicación Móvil.

2. Datos personales y su tratamiento

TuID móvil no solicita, almacena, ni trafica en ningún momento información sensible; solicita datos personales a los solos efectos de la autenticación e ingreso en la aplicación: usuario y contraseña. Estos datos personales tampoco quedan almacenados en la aplicación.

Los datos personales ingresados son utilizados únicamente para los propósitos especificados en esta política de privacidad, así como también para mejorar la usabilidad de la aplicación.

Para operaciones de autenticación, firma y confirmación de transacción, no se intercambia información personal, solo se recupera del servidor la información de la operación.

Durante el proceso de activación de TuID móvil se intercambia información personal durante el proceso de autenticación OAuth, pero esta información no se almacena.

3. Usos de TuID móvil.

Los titulares de TuID móvil podrán utilizar la app para autorizar operaciones de autenticación, firma o confirmar transacciones, todo esto es posible porque TuID móvil proporciona un mecanismo de autenticación de doble factor basado en criptografía de clave pública y protección mediante un PIN propio.

4. Permisos de la aplicación móvil

- **Retrieve running apps, Read phone status and identity** (Recuperar listado de apps que están corriendo, Leer estado de teléfono e identidad).
  Necesario para versiones antiguas de Android donde los permisos de acceso no estaban tan refinados como actualmente.
- **Read/ Modify/ delete the contents of your USB storage** (Leer/modificar/borrar el contenido del almacenamiento)
  Necesario para la descarga/lectura de PDF en operaciones de firma de documentos.
- **Take pictures and videos** (tomar fotografías y videos).
  Necesario para escanear códigos QR para activar la aplicación. No se sacarán fotos, ni grabarán videos no autorizados en ninguna circunstancia.
- **Receive data from Internet, View network connections, Full network Access** (recibir datos de internet, Ver configuraciones de red, Acceso completo a la red)

Necesario para acceder a internet.

- **Control vibration, Prevent device from sleeping** (control de vibración, Mantener el dispositivo despierto)
  Necesario para permitir la vibración al recibir notificaciones.

5. Condiciones de seguridad del servicio

a) Autorización de operaciones

El usuario cuenta con un PIN de seguridad que define al momento de realizar la activación de TuID móvil y el mismo le será solicitado en cada operación que se desee realizar.

Si el usuario durante la activación decide utilizar su huella dactilar (y el dispositivo lo permite) la aplicación utilizará este método como primera opción para autorizar una operación. En estos casos TuID móvil no almacenará la huella dactilar, sino que quedará almacenada en el equipo móvil, según las buenas prácticas dispuestas por el sistema operativo correspondiente android o iOS

Si el usuario introduce una huella dactilar no válida, a continuación, la aplicación le permitirá escoger entre autenticación usando la huella dactilar o usando el PIN de seguridad.

Si el usuario insiste en usar la huella y la introduce incorrectamente más de 5 veces consecutivas, el sistema operativo bloqueará el conjunto de huellas del dispositivo. Cuando esto ocurre, la aplicación en iOS solo le permitirá autenticación usando el PIN hasta que el usuario desbloquee el conjunto de huellas, y en Android el sistema insertará retardos crecientes hasta que la huella sea correcta.

Si el usuario usa el PIN para confirmar la operación, dispondrá de 3 intentos para poner el PIN correctamente, si falla 3 veces consecutivas, la aplicación se desvinculará de la Identidad de TuID.

b) Bloqueo Remoto

El servicio está provisto con la posibilidad de realizar una desactivación remota que puede ser iniciada por el titular de TuID desde el dispositivo donde está activada la app o desde el portal www.tuid.uy. Esta desactivación también podrá ser realizada por Antel en caso de detectarse un uso indebido del servicio.

Si el usuario desea volver a activar el servicio deberá seguir los mismos pasos que realizó en la primera activación.

6. Uso de cookies

Las únicas cookies presentes en esta app son las que intercambia con el servidor a través del WebView como cualquier otra aplicación cliente OAuth.

7. Cambios en la Política de Privacidad.

TuID móvil puede modificar esta Política de privacidad cuando lo considere necesario. Los cambios se informarán a través de nuestros servicios, o por otros medios fehacientes, para ofrecerte la oportunidad de revisar los cambios.

8. Documentación relacionada

Este documento complementa la Declaración de Prácticas de Certificación de TuID, así como los Términos y Condiciones de TuID.