ANEXO

FECHA DE EMISION:	**25 de Enero del 2021**	**CÓDIGO:**	**ATT-DJ-RA-H-TL LP 5/2021**
FECHA DE VENCIMIENTO:	**24 de Enero del 2026**		

CERTIFICADO DE HOMOLOGACIÓN

1	**CATEGORÍA (S)**	Software de aplicación o aplicativo de la Infraestructura Nacional de Certificado Digital
2	**SUBCATEGORIA (S)**	Software de aplicación para la generación de par de claves
3	**NOMBRE Y DIRECCIÓN DEL FABRICANTE**	AGENCIA PARA EL DESARROLLO DE LA SOCIDAD DE LA INFORMACIÓN EN BOLIVIA – ADSIB Calle Jaime Mendoza No 981, Zona San Miguel La Paz – Bolivia

	APLICACIÓN	**DESARROLADOR**	**VERSIÓN**
4	Certificado por Software - Android	ADSIB	1.0

5	**ORGANISMO AUDITOR**	AGETIC	**REPORTE O INFORME DE LA AUDITORIA INFORMATICA**
			AGETIC-UCGII/IT/0098/2020 AGETIC-UCGII/IT/0308/2020

	TECNOLOGÍA	***Software de Aplicación para la Generación de Par de Claves***
6	**SISTEMA OPERATIVO**	Debian 9 "Stretch"
7	**COMPATIBILIDAD DE SISTEMAS OPERATIVOS**	Android KitKat – Android 10
8	**LENGUAJE PARA EL DESARROLLO**	Java
9	**TIPO DE AUTENTICACIÓN Y CONTROL DE ACCESO**	Cifrado simétrico por contraseña mediante el algoritmo pbeWithSHAAnd3-KeyTripleDESCBC aplicado a la clave privada y el certificado.
10	**SOPORTE API DEL CLIENTE Y ESTÁNDARES**	PKCS#12
11	**ALGORITMOS CRIPTOGRÁFICOS**	pbeWithSHAAnd3-KeyTripleDES-CBC RSAES-PKCS1-v1_5
12	**ALGORITMO DE HASH**	SHA-256
13	**LONGITUD DE CLAVE RSA**	2048

I-LP-2906

14	**NIVEL DE SEGURIDAD FIPS140-2**	Nivel 1
15	**TIPO DE GENERACIÓN DE NÚMEROS ALEATORIOS**	Pseudo-Aleatorios (PRNG)
16	**CRIPTOGRAFÍA BASE**	BouncyCastle
	Sobre el Software	
17	**VERSIONES (REVISIONES)**	URL: https://gitlab.softwarelibre.gob.bo/adsib/fido-android
18	**PROGRAMA FUENTE (ÚLTIMA VERSIÓN)**	URL: https://gitlab.softwarelibre.gob.bo/adsib/fido-android/-/archive/final/fido-androidfinal.tar.gz.
19	**Código o Programa Ejecutable**	URL: https://firmadigital.bo/android/
	Versión Final de Software de Aplicación MS5 o SHA1	
20	https://gitlab.softwarelibre.gob.bo/adsib/fidoandroid/-/archive/final/fido-android-final.tar.gz	4d0d17ff5c1d04910a49aca2ae8400df89e0f217
21	**CONDICIÓN DE LA HOMOLOGACIÓN**	Reconocimiento y verificación mediante un Organismo Auditor

Nota. -

i) El desarrollador del software de aplicación o aplicativo para la generación de claves, es responsable de la correcta generación del par de calves para los propósitos del servicio de Certificación Digital.

ii) Toda entidad Certificadora, debe hacer uso de un software de aplicación o aplicativo registrado en la ATT.

iii) El Informe Técnico Jurídico es parte integrante de la Resolución Administrativa como documento que respalda la información en el presente Certificado.

V°B° A.T.T.

ANALISTA LEGAL V°B° L.F.P.L. A.T.T.

1-LP-2996