



## Resolución Administrativa Homologación

**ANEXO**  
**CERTIFICADO DE HOMOLOGACIÓN**

- a) **CÓDIGO:** ATT-DJ-RA-H-TL LP 516/2020
- b) **EMISIÓN Y VENCIMIENTO:** 03 de noviembre del 2020, vence el 02 de noviembre del 2025
- c) **CONDICIONES DE OTORGACIÓN DE LA HOMOLOGACIÓN:** Reconocimiento y verificación de una certificación internacional
- d) **CATEGORÍA Y SUBCATEGORÍA DENTRO DE LAS CUALES EL EQUIPO FUE HOMOLOGADO**

<b>CATEGORIA</b>	Dispositivo de Hardware de Seguridad
<b>SUBCATEGORIA</b>	HSM (Hardware Security Module)

- e) **NOMBRE Y DIRECCIÓN DEL FABRICANTE:**

**THALES**  
225 W Park Loop NW  
Huntsville, Alabama 35806  
USA

- f) **DATOS TÉCNICOS:**

Producto	Luna Network HSM
Marca	Safenet
Modelo	A750

- g) **ESPECIFICACIONES TÉCNICAS PRINCIPALES:**

<b>ESPECIFICACIONES TÉCNICAS PRINCIPALES</b>	
Sistemas Operativos Compatibles para Administración	- Windows, Linux, Solaris, AIX. - Virtual: VMware, Hyper-V, Xen, KVM.
Soporte API	- PKCS # 11, Java (JCA / JCE), Microsoft CAPI y CNG, OpenSSL. - API REST.
Criptografía	- Soporte completo de Suite B. - Asimétrico: RSA, DSA, Diffie-Hellman, curva elíptica Criptografía (ECDSA, ECDH, Ed25519, ECIES) con nombre, curvas definidas por el usuario y de Brainpool, KCDSA. - Simétrico: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST. - Hash / Message Digest / HMAC: SHA-1, SHA-2, SM3.



E-LP-5769



## Resolución Administrativa Homologación

Criptografía (Cont.)	- Derivación de claves: modo de contador SP800-108. - Envoltura de llaves: SP800-38F. - Generación de números aleatorios: diseñado para cumplir con AIS 20/31 a DRG.4 utilizando una fuente de ruido real basada en HW junto con CTR-DRBG compatible con NIST 800-90A. - Cifrado de billetera digital: BIP32. - Mecanismos criptográficos 5G para la autenticación de suscriptores: Milenage, Tuak y Comp128.
Certificaciones de Seguridad	- FIPS 140-2 Nivel 3 - Contraseña y multifactor (PED) - eIDAS CC EAL4 + (AVA_VAN.5 y ALC_FLR.2) contra el Perfil de protección 419221-5
Interfaz de Host	- 2 opciones: 4 puertos Ethernet Gigabit con enlace de puertos, o Conectividad de red de fibra 2 x 10G y 2 x 1G con conexión de puertos - IPv4/IPv6
Memoria	16MB
Particiones	5
Particiones Máximas	20
<b>OTRAS CARACTERÍSTICAS IMPORTANTES</b>	
Cumplimiento de seguridad y medioambiente	- UL, CSA, CE - Marca FCC, CE, VCCI, C-TICK, KC - RoHS2, WEEE - TAA

## h) CERTIFICACIÓN INTERNACIONAL:

<b>ORGANISMO QUE EMITIO CERTIFICACIÓN:</b>	The National Institute of Standards and Technology
<b>NÚMERO DE CERTIFICACIÓN:</b>	3205

**Nota.-**

- i) El presente certificado no constituye título habilitante para la prestación de servicios de telecomunicaciones, ni autoriza el uso de frecuencias del espectro radioeléctrico.
- ii) En caso de difusión de publicidad **escrita o audiovisual** acerca del equipo, se deberá incluir el logo de la ATT y señalar que el equipo fue homologado por esta Autoridad.



E-LP-5769

LA PAZ: Calle 13 de Calacoto  
Nº 8260 entre Av. Los Saucos  
y Av. Custanera  
Telf.: 2772266 - Fax: 2772299  
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián  
Nº 683, Esq. España y La Paz  
(El Prado)  
Telf./Fax: 4-4581182 - 4-4581184  
4-4581185

SANTA CRUZ: Avenida Beni,  
entre 4º y 5º anillo, calle 3,  
Edificio Gardenia, Condominio  
Club Torre Sur, Planta Baja Of. 2,  
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Méndez Nº 311  
esq. Alejandro del Carpio  
Barrio Las Panosas  
Telf.: 6644136 - 6112611

Línea Gratuita de Protección al  
Usuario  
4 de 4  
800-10-6000  
www.att.gob.bo