



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

BCB-DGD-VUC

2016 AGO 11 PM 3:44

CORRESPONDENCIA
GENERAL
DESPACHADA

CIRCULAR EXTERNA

La Paz, 10 de agosto de 2016
SGDB N° 035/2016

DE: GERENCIA GENERAL
GERENCIA DE ENTIDADES FINANCIERAS
A: ENTIDADES FINANCIERAS PARTICIPANTES DEL SISTEMA DE
LIQUIDACION INTEGRADA DE PAGOS (LIP)
ASUNTO: **NUEVO CERTIFICADO DIGITAL DEL BCB PARA EL SISTEMA DE
PAGOS**

Señoras y señores:

El Banco Central de Bolivia (BCB) comunica a todos los participantes del Sistema de Liquidación Integrada de Pagos (LIP), la emisión de un nuevo certificado digital que entrará en vigencia el miércoles 17 de agosto de 2016, que se encuentra disponible en la siguiente dirección:

➤ Portal del Sistema LIP : <http://portallip.bcb.gob.bo>

De acuerdo con los procedimientos establecidos en la Guía Operativa e Informática del Sistema de Liquidación Integrada de Pagos GOISLIP (v.1.0) y las características descritas en el documento adjunto, las entidades que utilicen Web Services para su operativa en el Sistema LIP, deberán programar el intercambio de certificados digitales en presencia de Notario de Fe Pública.

La programación de horarios será atendida por la Mesa de Ayuda, a partir de la fecha; para tal efecto, favor comunicarse a los teléfonos 2407262, 2147077, 2661623, 2661645 o al correo institucional ayudalip@bcb.gob.bo

Atentamente,

RONALD O. PINTO RIBERA
GERENTE DE ENTIDADES
FINANCIERAS a.i.
BANCO CENTRAL DE BOLIVIA

CARLOS A. COLODRO LÓPEZ
GERENTE GENERAL a.i.
BANCO CENTRAL DE BOLIVIA

CCL/RPR/APM/PCS



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

**Características que deben cumplir los certificados Digitales para
Operar en el Sistema LIP**

Los Certificados Digitales deberán cumplir con las características descritas a continuación:

1. Características Técnicas:

- a. **Clave Pública:** El algoritmo de la Clave pública al momento de su generación deberá ser RSA y su Longitud debe ser de **2048 bits**.
- b. **Vigencia.-** La vigencia de los Certificados Digitales deberá ser de 2 años.
- c. **Algoritmo de Firma.-** Al momento de su generación deberá utilizarse el algoritmo de firma (signatureAlgorithm) SHA256withRSA

2. Formato de Datos para el Sujeto

a. Certificados Utilizados para Web Services

i. Certificados para Transacciones.

- 1. **Sujeto:** En el Certificado Digital, dentro de los Atributos del Sujeto, los campos que deberán ser llenados de manera Obligatoria son **Common Name (CN), Organization (O) y Country (C)** , de acuerdo al siguiente formato.

a. **Campo Common Name (CN).** El Campo "Common Name" tiene como objetivo identificar al propietario del Certificado, deberá contener el o los nombres de los representantes legales de la entidad y el propósito del certificado. Para el Sistema LIP, debe cumplir con el siguiente formato CN= "Nombre(s) del(os) Representante(s) Legal(es)" – Transacciones LIP

b. **Campo Organization (O).** El campo "Organization", tiene como objetivo identificar la Organización a la que pertenece el titular del certificado, deberá incluir el Nombre de la Entidad.

c. **Campo Country (C).** El campo "Country" tiene como objetivo identificar el País correspondiente al Certificado y deberá contener el valor "BO".

ii. Certificados para Revocatoria.

- 1. **Sujeto:** En el Certificado Digital, dentro de los Atributos del Sujeto, los campos que deberán ser llenados de manera obligatoria son Common Name (CN), Organization (O) y Country (C) , de acuerdo a la siguiente formato.



BANCO CENTRAL DE BOLIVIA

ESTADO PLURINACIONAL DE BOLIVIA

- a. **Campo Common Name (CN).** El Campo "Common Name" tiene como objetivo identificar al propietario del Certificado, deberá incluir el o los nombres de los representantes legales de la entidad y el propósito del certificado. Para el Sistema LIP, debe cumplir con el siguiente formato CN= "Nombre(s) del(os) Representante(s) Legal(es)" – Revocatoria LIP
- b. **Campo Organization (O).** El campo "Organization", tiene como objetivo identificar la Organización a la que pertenece el titular del certificado, deberá Incluir el Nombre de la Entidad.
- c. **Campo Country (C).** El campo "Country" tiene como objetivo identificar el País correspondiente al Certificado y deberá contener el valor "BO".

b. Certificados Utilizados por la Aplicación WEB

i. Certificados para Transacciones.

1. **Sujeto:** En el Certificado Digital, dentro de los Atributos del Sujeto, los campos que deberán ser llenados de manera Obligatoria son: **Common Name (CN)**, **Organization (O)** y **Country (C)**, de acuerdo a la siguiente formato.
 - a. **Campo Common Name (CN).** El Campo "Common Name" tiene como objetivo identificar al propietario del Certificado, deberá contener el o los nombres de los representantes legales de la entidad y el propósito del certificado. Para el Sistema LIP, debe cumplir con el siguiente formato CN= "Nombre(s) del(os) Representante(s) Legal(es)" – Transacciones LIP
 - b. **Campo Organization (O).** El campo "Organization", tiene como objetivo identificar la Organización a la que pertenece el titular del certificado, deberá Incluir el Nombre de la Entidad.
 - c. **Campo Country (C).** El campo "Country" tiene como objetivo identificar el País correspondiente al Certificado y deberá contener el valor "BO".

3. Ejemplo de Generación de Certificados con las Características técnicas utilizando java Keytool

```
keytool -genkey -alias1 test -keyalg rsa -keysize 2048 -sigalg sha256withrsa -  
validity 730 -keystore test.jks2
```

¹ El alias es definido por el participante el momento de generar el Certificado Digital. En el ejemplo se utiliza el nombre de alias test, sin embargo este debe ser elegido por el participante

² El nombre del archivo que servirá de contenedor es elegido por el participante. Es importante asignar la extensión ".jks" para su identificación.



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

4. Ejemplo de Valores Generados en el Campo Sujeto y Características Técnicas

Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Algoritmo de firma	sha256RSA
Algoritmo hash de firma	sha256
Emisor	Ronald Omar Pinto Ribera - Tr...
Válido desde	miércoles, 17 de agosto de 20...
Válido hasta	viernes, 17 de agosto de 2018...
Clave pública	RSA (2048 Bits)
Identificador de clave del bit	8b 36 8c 56 00 8a ac e3 8d 1f

GN = Ronald Omar Pinto Ribera - Transacciones LIP
OU = Gerencia de Entidades Financieras
O = Banco Central de Bolivia
L = La Paz
S = La Paz
C = BO

Editar propiedades... Copiar en archivo...

Más información acerca de los [detalles del certificado](#)

El presente documento forma parte de la Guía Operativa e Informática del Sistema LIP.