



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

CIRCULAR EXTERNA

La Paz, 19 de junio de 2017
SGDB N° 030/2017

BCB-DGD-VUC

2017 JUN 22 AM 9:55

N°
TRAMITE GENERAL
CERRADO

DE: GERENCIA GENERAL
GERENCIA DE ENTIDADES FINANCIERAS
A: ENTIDADES FINANCIERAS PARTICIPANTES DEL SISTEMA DE
LIQUIDACIÓN INTEGRADA DE PAGOS (LIP)
ASUNTO: GENERACIÓN DE CERTIFICADOS DIGITALES PARA EL
SISTEMA DE PAGOS

Señoras y señores:

El Banco Central de Bolivia (BCB) comunica a los participantes del Sistema de Liquidación Integrada de Pagos (LIP), que de acuerdo con los procedimientos establecidos en la Guía Operativa e Informática del Sistema de Liquidación Integrada de Pagos GOISLIP (v.1.0), para la generación de certificados digitales que permiten su operativa en el Sistema LIP deberán considerar las características descritas en el documento adjunto.

Cualquier consulta favor comunicarse con la Mesa de Ayuda del LIP a los Teléfonos 2662154, 2661117, 2661623, 2661645, 2407262, 2147077 y/o correo electrónico ayudalip@bcb.gob.bo.

Atentamente,

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

ABEL F. SANJINÉS ÁLVAREZ
GERENTE GENERAL a.i.
BANCO CENTRAL DE BOLIVIA

ASA/RPR/JDM/APM/CCD/OAU/jkt
Adj. lo citado



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

Características que deben cumplir los certificados digitales para operar en el Sistema LIP

Para la generación de certificados digitales se deberá considerar el estándar X.509 obligatoriamente en los siguientes aspectos: (sin ser estos limitativos)

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 Organización (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 al 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 Organización (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 al siguiente formato".
 - 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)" –Transacciones Aplicativo Web LIP.
 - b. **Campo Organización (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.



BANCO CENTRAL DE BOLIVIA

ESTADO PLURINACIONAL DE BOLIVIA

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

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	Luis Alberto Machicao Tamayo ...
Válido desde	martes, 27 de septiembre de 2...
Válido hasta	jueves, 27 de septiembre de 2...
Sujeto	Luis Alberto Machicao Tamayo ...
Clave pública	RSA (2048 Bits)
Identificador de clave del tit	52 a8 hd 63 d0 74 a6 9b r2 1a

CN = Luis Alberto Machicao Tamayo - Transacciones LIP
OU = Departamento de Servicios Financieros
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

Aceptar

Web Services

Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Versión	V3
Número de serie	0c 94 27 dd
Algoritmo de firma	sha256RSA
Algoritmo hash de firma	sha256
Emisor	Perico Perez Perez - Transacci...
Válido desde	martes, 20 de junio de 2017 1...
Válido hasta	jueves, 20 de junio de 2019 1...
Sujeto	Perico Perez Perez - Transacci...

CN = Perico Perez Perez - Transacciones Aplicativo Web LIP
OU = Gerencia General
O = Cooperativa de Ahorro Central
L = La Paz
S = La Paz
C = BO

Editar propiedades... Copiar en archivo...

Más información acerca de los detalles del certificado

Aceptar

Aplicación Web

JOSE S. DELGADO MACHICADO
GERENTE DE SISTEMAS
BANCO CENTRAL DE BOLIVIA

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 deber 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.