Depósito Central
de Valores - DCV

Dirección General de Tecnología

Documento Ténico Para Conectividad de Entidades A Través de Mensajería.

Versión 1.5

2022-12-01

01 de diciembre de 2022

CONTENIDO

1 INTRODUCCIÓN

1.1 PROPÓSITO DEL DOCUMENTO

Presentar la información técnica que deben conocer las entidades/aplicaciones que interactúan con el nuevo sistema de información del Depósito Central de Valores (DCV) del Banco de la República (BR) a través del middleware basado en mensajería.

1.2 ALCANCE

Este documento define los aspectos principales que son necesarios para realizar la implementación de clientes, esto es, productores y consumidores de mensajería exclusivamente dentro del proyecto MIT-DCV.

Este documento está sujeto a modificaciones que se puedan dar durante el desarrollo del proyecto MIT-DCV del BR. Estas modificaciones incluyen ajustes a la información relacionada y/o apartados adicionales que el BR considere necesarios.

1.3 AUDIENCIA

Este documento está dirigido al equipo del proyecto MIT-DCV, al Grupo de Ingeniería del proyecto, área usuaria del Departamento de Fiduciaria y Valores, a la Dirección General de Tecnología y las entidades que se integrarán al nuevo sistema de información del Depósito Central de Valores – DCV a través del middleware de mensajería.

1.4 ORGANIZACIÓN DEL DOCUMENTO

El capítulo 2 presenta la información técnica necesaria para direccionar las implementaciones de productores y consumidores de mensajería. El capítulo 3 presenta anexos de información complementaria. Finalmente, se encuentra el historial de cambios del documento.

1.5 MODIFICACIONES AL DOCUMENTO

Este documento está en permanente actualización a partir del segundo semestre del 2020. Algunos apartados serán complementados o modificados de acuerdo con las circunstancias y definiciones técnicas realizadas por el BR. Los ajustes realizados serán informados oportunamente a todos los interesados.

2 INFORMACIÓN TÉCNICA

2.1 INTRODUCCIÓN

Dentro del programa de proyectos de la Modernización Tecnológica del Departamento de Fiduciaria y Valores (MIT-DFV) del BR, se ha definido que la interoperabilidad entre las entidades y el BR para el caso del Depósito Central de Valores - DCV, se realice a través de mensajería. Para ello, el Banco provee una infraestructura de middleware orientada a mensajería. La Figura 1 presenta a nivel general el mecanismo que ha dispuesto el BR para intercambiar mensajería entre el DCV y las entidades.

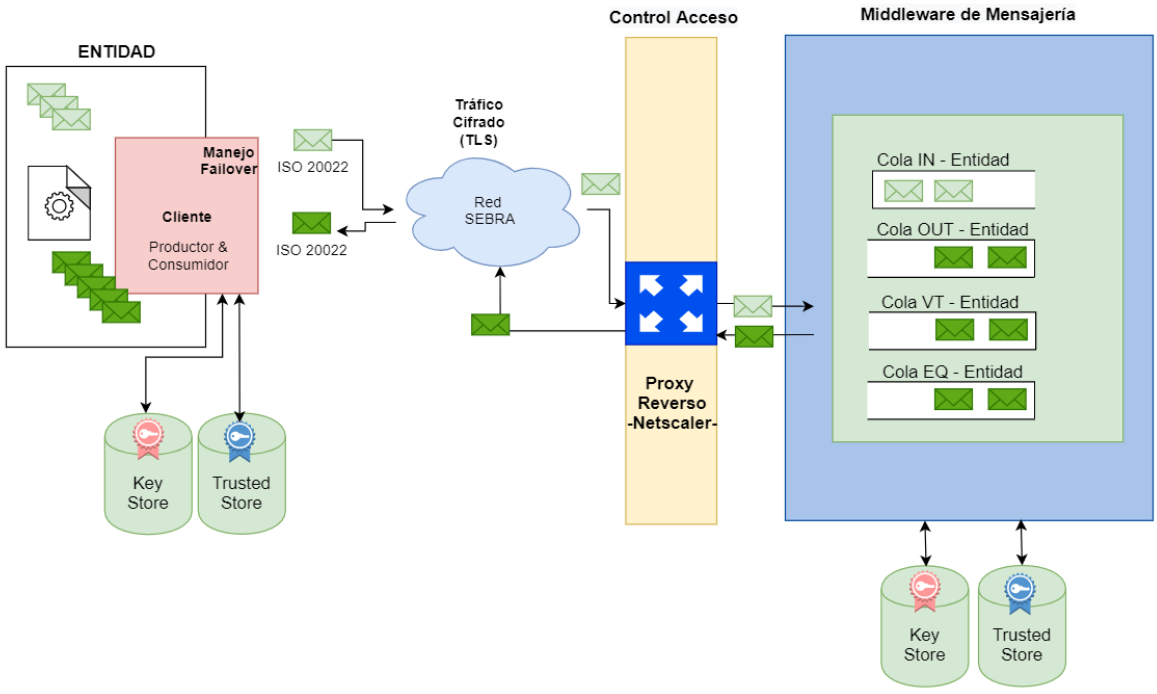


Figura 1- Modelo de Interoperabilidad para el Nuevo DCV

La información técnica que se encuentra a continuación está organizada en los siguientes frentes principales:

- **Conectividad**: Información necesaria para lograr la conexión desde los componentes de software de las entidades hasta la infraestructura de mensajería del BR.
- **Certificados digitales**: Información relacionada con la gestión de certificados digitales requeridos para soportar la interoperabilidad entre las entidades y el BR.
- **Colas de mensajería**: Descripción de los objetos a través de los cuales se intercambiarán mensajes ISO 20022 entre las entidades y el BR.
- **Estructura de los mensajes**[1]: Descripción técnica del formato de los mensajes que serán intercambiados entre las entidades y el BR.
- **Implementación de productores y consumidores**: Descripción de aspectos técnicos a ser tenidos en cuenta en las implementaciones de productores y consumidores de mensajes que deben realizar las entidades.
- **Mensajes de error:** Listado de mensajes de error generados por la infraestructura de mensajería del BR.

2.2 CONECTIVIDAD

2.2.1 Canal de comunicación

Las entidades se conectarán a través del canal dedicado con el que actualmente interactúan con el BR (Red SEBRA).

2.2.2 Endpoints

La dirección y puerto por el cual se realizará la conectividad es la siguiente:

[1] El concepto **mensaje** se refiere al artefacto técnico para interactuar a través del middleware de mensajería. Este artefacto está compuesto de un header (encabezado) y un payload (detalle). El concepto **mensaje ISO 20022** se refiere a un estándar para intercambio electrónico de datos entre instituciones financieras.

Ambiente	Servidor y Puerto
Pruebas	nasa.banrep.gov.co: 5510 nasa.banrep.gov.co: 5515
Producción	totoro.banrep.gov.co: 5510 totoro.banrep.gov.co: 5515

Nota: Debido al cambio de direccionamiento que hace el BR para las entidades que utilizan la red SEBRA, las direcciones IP de los servidores nasa y totoro son 192.168.61.24 y 192.168.61.23 respectivamente. Las entidades pueden configurar la funcionalidad del archivo hosts para registrar la correspondencia entre los servidores nasa y totoro y las direcciones IP relacionadas anteriormente.

2.3 CERTIFICADOS DIGITALES

El BR, a través de su plataforma PKI provee, por demanda, los certificados digitales para las entidades. El proceso de generación de certificados se realiza desde la plataforma tecnológica de la entidad. Los apartados 2.3.4 y 3.4 de este documento, describen el proceso para la generación del certificado en mención.

El cifrado de canal, la autenticación y autorización y la validación de firma digital de mensajes entre la entidad y el BR se realizará a través de certificados digitales.

2.3.1 Cifrado del canal

La conexión entre la entidad y el BR se realiza por el canal dedicado. Para efectos de mensajería, se cifra el canal mediante mutual SSL/TLS. Para lograr este cifrado, se requiere intercambio de llaves públicas entre el BR y la entidad:

- El BR enviará a la entidad la llave pública de la infraestructura de mensajería para que sea configurada en su llavero de confianza.
- La entidad enviará al BR la llave pública de su certificado digital para que sea configurada en el llavero de confianza de la infraestructura de mensajería del BR.

2.3.2 Autenticación y autorización

La autenticación y autorización de la entidad ante la infraestructura de mensajería del BR se realiza a través de la validación del certificado digital de la entidad.

2.3.3 Validación defirma digital de mensajes

Para efectos de validación de firma digital se debe tener en cuenta lo siguiente:

- La entidad firma los mensajes que envía al BR. El BR a su vez, valida esta firma usando la llave pública del certificado de la entidad.
- El BR firma los mensajes que envía a la entidad. El BR enviará a la entidad una llave pública adicional del sistema DCV para la validación de la firma en caso que la entidad decida implementar esta funcionalidad.
- Las secciones 2.5.5 y 2.5.6 de este documento describen el detalle de este procedimiento.

2.3.4 Creación de certificados digitales

Los certificados digitales son emitidos por la Entidad de Certificación Digital Cerrada CA BANREP. El certificado digital para mensajería que debe generar la entidad es exclusivo para este propósito. La documentación para la creación y recuperación de los certificados se encuentra disponible en:

- Instructivo Novedades SEBRA – PKI - GTA
  https://www.banrep.gov.co/sites/default/files/paginas/Instructivo%20Novedades%20SEBRA-PKI-GTA.pdf
- Forma BR-3-986-02
  https://www.banrep.gov.co/sites/default/files/BR-3-986-2.xlsx
- Manual para la Gestión de Instrumentos de Firma Electrónica DSI-GI-128
  https://www.banrep.gov.co/sites/default/files/dsi-gi-128.pdf

2.4 COLAS DE MENSAJERÍA

2.4.1 Cola de entrada

La entidad tendrá asignada una cola de entrada a la cual enviará todos los mensajes que deben ser procesados por el DCV. El nombre de la cola es el siguiente:

CODIGO_BIC + IN

Ejemplo:

ABNABRSPIN

2.4.2 Cola de salida

La entidad tendrá asignada una cola de salida de la cual consumirá todos los mensajes que han sido generados por el DCV para esa entidad en particular. El nombre de la cola es el siguiente:

CODIGO_BIC + OUT

Ejemplo:

ABNABRSPOUT

Los mensajes que genera el BR y que entrega en la cola de salida de cada entidad, permanecerán 120 horas en dicha cola. Si no son consumidos por la entidad después de esta ventana de tiempo, se eliminarán automáticamente de la cola de salida y se moverán copiados a la cola de mensajes expirados.

2.4.3 Cola de validaciones técnicas

Cada entidad cuenta con una cola de validaciones técnicas. El nombre de la cola es el siguiente:

CODIGO_BIC + VT

Ejemplo:

ABNABRSPVT

Los mensajes que llegan a esta cola son aquellos que la entidad ha enviado a su cola de entrada pero que no han cumplido uno o más de los requisitos técnicos solicitados por el BR. Los mensajes que se encuentran en esta cola desaparecen de la cola de entrada, no llegan al DCV y por lo tanto no se procesan. La capa de mensajería del BR valida los requisitos técnicos a través del siguiente filtro:

- Indicador de persistencia: El mensaje debe ser persistente.
- Vigencia del mensaje en la cola: Los mensajes no deben tener fecha de expiración.
- Prioridad del mensaje: La prioridad de los mensajes debe ser igual a 4.
- Estampado de tiempo del mensaje: El cliente debe permitir que el mensaje se cree en el middleware de mensajería del BR con la fecha y hora del sistema.
- Tamaño del mensaje: Los mensajes no deben superar 50kB al sumar el header y el payload.

Los cuatro primeros atributos son parte del header del mensaje se explican con mayor detalle en la sección **¡Error! No se encuentra el origen de la referencia.** de este documento.

Los mensajes de esta cola deben ser consumidos por la entidad para conocer la causa del rechazo por parte del middleware del BR. Así mismo, el BR determinará si aplica un procedimiento operativo de eliminación de mensajes que se encuentren en esta cola, dependiendo del número y vigencia de los mismos.

2.4.4 Cola de mensajes expirados

Cada entidad cuenta con una cola de mensajes expirados. El nombre de la cola es el siguiente:

CODIGO_BIC + EQ

Ejemplo:

ABNABRSPEQ

En esta cola permanecerán los mensajes que fueron movidos desde la cola salida y/o la cola de validaciones técnicas de la entidad hasta el día viernes de cada semana a las 7:00 PM. En ese momento el Banco purgará la cola de mensajes expirados y no será posible recuperar el(los) mensaje(s) a través del middleware de mensajería.

2.5 ESTRUCTURA DE LOS MENSAJES

La estructura de los mensajes se presenta en la Figura 2. Los apartados siguientes explican el contenido de los mensajes tanto de entrada como de salida a nivel de header (encabezado) y payload (detalle).

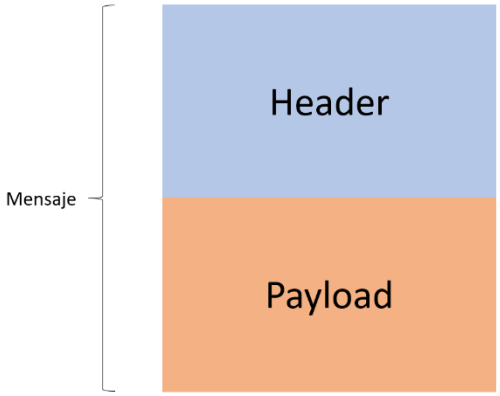


Figura 2- Estructura del Mensaje

2.5.1 Header de mensajes enviados por la entidad

El encabezado (header) del mensaje que envía la entidad al BR debe contener los siguientes campos y valores:

#	Campo	Descripción	Valor establecido por la Entidad
1	JMSDestination	Cola destino (Cola de entrada)	Ver numeral 2.4.1 de este documento.

#	Campo	Descripción	Valor establecido por la Entidad
2	JMSPriority	Prioridad del mensaje	4 (prioridad por defecto)
3	JMSRedelivered	Posibilidad de re-entregas	FALSE
4	JMSReplyTo	Cola de respuesta	Vacío
5	JMSTimestamp	Estampa de tiempo de creación del mensaje en el Broker	Atributo habilitado por defecto en JMS
6	JMSDeliveryMode	Indicador de persistencia	2 (persiste el mensaje)
7	JMSExpiration	Vigencia del mensaje en la cola	0 (no expira)
8	JMSCorrelationID	Correlación de mensajes	Vacío
9	JMSMessageID	Identificador del mensaje asignado por el Broker	No Aplica. Asignado por el Broker
10	MSG_SENDER	Nit del productor del mensaje. Nit Entidad Originadora	NIT de la entidad que envía el mensaje. Sin dígito de verificación.
11	MSG_TYPE	Código de mensaje ISO 20022: BusinessArea+MessageID+Variant+Version	Código del mensaje ISO 20022 incluyendo: BusinessArea+MessageID+Variant+Version
12	REF	IdentificadorMensaje	Identificador alfanumérico único que asigna la entidad para efectos de trazabilidad.
13	RELREF	Correlación de mensaje	Vacío
14	SIGN	Firma digital del mensaje ISO 20022	Ver numeral 2.5.5 para asignar este valor

Nota 1: La especificación JMS contiene campos de encabezados adicionales los cuales no serán tenidos en cuenta por la infraestructura tecnológica del BR.

Nota 2: Se deben respetar los valores requeridos por el BR por cuanto el sistema de mensajería ejecuta filtros de completitud y correctitud de los valores definidos en el header del mensaje.

Nota 3: Todos los campos del encabezado, incluyendo el campo “SIGN” (Firma digital del mensaje ISO 20022) deben cumplir con el formato de codificación caracteres UTF-8.

2.5.2 Header de mensajes recibidos por la entidad

El encabezado (header) del mensaje que envía el BR a las entidades tiene los siguientes campos y valores:

#	Campo	Descripción	Valor establecido por el BR
1	JMSDestination	Cola destino (cola de salida)	Ver numeral 2.4.2 de este documento.
2	JMSPriority	Prioridad del mensaje	Valor asignado por el DCV
3	JMSRedelivered	Posibilidad de re-entregas	FALSE
4	JMSReplyTo	Cola de respuesta	Vacío
5	JMSTimestamp	Estampa de tiempo de creación del mensaje en el Broker	Atributo habilitado por defecto en JMS
6	JMSDeliveryMode	Indicador de persistencia	2 (persiste el mensaje)
7	JMSExpiration	Vigencia del mensaje en la cola	0 (no expira)
8	JMSCorrelationID	Correlación de mensajes	ID del mensaje de entrada que generó el mensaje de salida
9	JMSMessageID	Identificador del mensaje asignado por el Broker	No Aplica. Asignado por el Broker
10	MSG_SENDER	Nit del productor del mensaje. Nit Entidad Originadora	NIT del BR sin dígito de verificación
11	MSG_TYPE	Código de mensaje ISO 20022: BusinessArea+MessageID+Variant+Version	Código del mensaje ISO 20022 incluyendo: BusinessArea+MessageID+Variant+Version
12	REF	IdentificadorMensaje	Identificador único asignado por el DCV.
13	RELREF	Correlación de mensaje	REF del mensaje que dio origen al mensaje de salida
14	SIGN	Firma digital del mensaje ISO 20022	Firma realizada por el BR sobre el mensaje ISO 20022

Nota 1: La especificación JMS contiene campos de encabezados adicionales los cuales no serán tenidos en cuenta por la infraestructura tecnológica del BR.

Nota 2: Todos los campos del encabezado, incluyendo el campo "SIGN" (Firma digital del mensaje ISO 20022) deben cumplir con el formato de codificación caracteres UTF-8.

2.5.3 Payload de mensajes enviados por laentidad

Consideraciones a tener en cuenta sobre el payload del mensaje:

- La entidad deberá enviar en el payload, el mensaje ISO 20022 de acuerdo con la especificación de mensajes de negocio que entregará el BR.
- El payload debe ser en todos los casos un mensaje ISO 20022 en formato XML.
- El mensaje JMS (Header + Payload) no podrá tener un tamaño mayor a 50kB.
- El payload del mensaje ISO 20022 debe cumplir con el formato de codificación caracteres UTF-8.

2.5.4 Payload de mensajes enviados por BR

El BR enviará en el payload, el mensaje ISO 20022 de acuerdo con la especificación de mensajes de negocio que entregará el BR. El payload es en todos los casos un mensaje ISO 20022 en formato XML.

2.5.5 Firma de mensajes ISO 20022

Los mensajes incluyen en el encabezado un campo/propiedad de firma. Esta firma corresponde a la firma digital del mensaje ISO 20022.

El DCV estará en la capacidad de realizar la validación de la firma recibida en cada uno de los mensajes, como también la generación e inclusión de la misma, en los mensajes que sean generados por el DCV hacia las entidades.

La firma de mensajes con certificados digitales garantiza los principios básicos de seguridad de integridad y no repudio. Los certificados digitales para firma de esta

mensajería serán provistos, por demanda, por la infraestructura PKI del BR. En este sentido, la firma de mensajes producidos por las Entidades es de carácter obligatorio.

Información adicional relacionada con este asunto:

- El algoritmo que debe utilizar la entidad para la firma digital de los mensajes es SHA256withRSA.
- La librería de código abierto java.security debe ser utilizada para la generación y validación de firmas
- La firma debe ser almacenada en el campo SIGN del header del mensaje. Esto aplica tanto para los mensajes enviados por la entidad como para los enviados por el BR.

A continuación se muestra un ejemplo de una implementación para realizar la firma de mensajes:

```
public static byte[] generateSimpleSignature(byte[] data, String alias, boolean encode) {
   try {
      KeyStore keystore = findKeystore();
      String signingAlgorithm = "SHA256withRSA";
      Signature sign = Signature.getInstance(signingAlgorithm);
      PrivateKey privateKey = (PrivateKey) keystore.getKey("firma",
                                                           "KeystorePassword".toCharArray());
      sign.initSign(privateKey);
      sign.update(data);
      byte[] rez = sign.sign();
      return encode ? Base64.getEncoder().encode(rez) : rez;
       } catch (Exception e) {
        log.error("Failed to generate simple signature ", e);
     }
        return null;
    }
```

Nota 1: Información detallada sobre la librería java.security se encuentra en el siguiente enlace: https://docs.oracle.com/javase/8/docs/api/java/security/Signature.html

2.5.6 Validación de firma de mensajes ISO 20022

Las Entidades podrán validar los mensajes de respuesta producidos por el DCV toda vez que esta mensajería será generada con firma en sus encabezados. El BR enviará su llave pública a las entidades para que estas puedan realizar la respectiva validación (la cual se entiende discrecional por parte de la Entidad).

A continuación, se muestra un ejemplo de una implementación para realizar la verificación de firma de los mensajes.

```
public static boolean validateSimpleSignature(byte[] data, byte[] signature, String
                                              alias, boolean encoded) {
        try {
            KeyStore keystore = findKeystore();
            byte[] toVerify = signature;
            String signingAlgorithm = "SHA256withRSA";
            Signature sign = Signature.getInstance(signingAlgorithm);
            /*
              extra error check to catch library call exceptions
            */
            java.security.cert.Certificate cert = keystore.getCertificate("firma");
            if (cert == null) {
                log.error("Failed to validate simple signature, no certificate found in
                           server keystore for alias " + alias);
                return false;
            }
            sign.initVerify(keystore.getCertificate("firma"));
            sign.update(data);
            if (encoded) {
                toVerify = Base64.getDecoder().decode(toVerify);
            }
          return sign.verify(toVerify);
        } catch (Exception e) {
            log.error("Failed to validate simple signature ", e);
        }
        return false;
    }
```

2.6 IMPLEMENTACIÓN DE PRODUCTORES Y CONSUMIDORES

2.6.1 Lenguaje de programación soportados

El lenguaje de programación en el cual se debe realizar la implementación del productor y consumidor de mensajes es JAVA utilizando Java 1.8 o superior.

2.6.2 Protocolos de mensajería

Los protocolos de mensajería que pueden ser utilizados son:

- API JMS 2.0 (CORE)
- AMQP 1.0 sobre JMS 2.0

A continuación, se describen las librerías que deben ser utilizadas para la implementación de los clientes productores y consumidores de mensajes.

2.6.2.1 Librería JMS API

Librería JAVA que debe ser utilizada en todos los casos. Esta librería se utiliza para crear la conexión con un sistema de mensajería tipo JMS. Puede ser descargada de https://mvnrepository.com/artifact/javax.jms/javax.jms-api. En este repositorio se encuentra la librería y/o la configuración del proyecto Maven en caso que la entidad utilice esta herramienta de construcción de proyectos Java. La Figura 3 presenta una imagen del repositorio donde se encuentra la librería. El BR recomienda utilizar la versión 2.0.1 o superior.

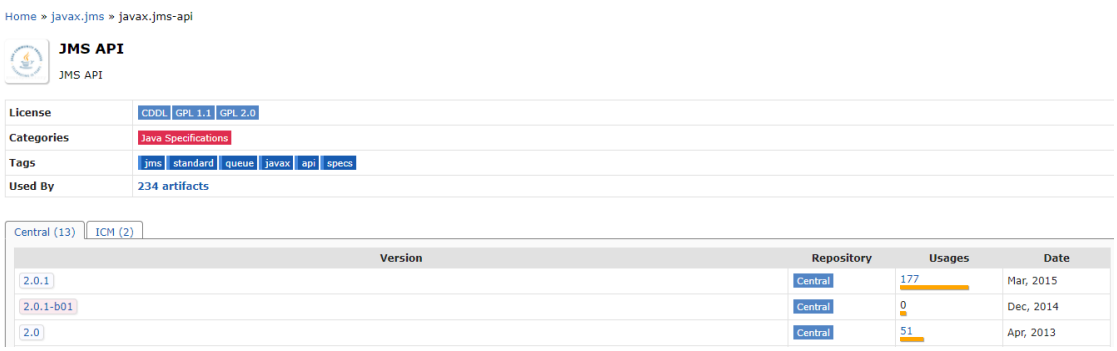


Figura 3- Repositorio de librería JMS API

2.6.2.2 Librería ActiveMQ Artemis – protocolo CORE

La librería JAVA que debe ser utilizada para realizar la implementación de los clientes JMS 2.0, productores y consumidores que hacen uso del protocolo CORE puede ser descargada de https://mvnrepository.com/artifact/org.apache.activemq/artemis-jms-client-all. En este repositorio se encuentra la librería y/o la configuración del proyecto Maven en caso que la entidad utilice esta herramienta de construcción de proyectos Java. La Figura 4 presenta una imagen del repositorio donde se encuentra la librería. El BR recomienda que la versión utilizada por la entidad sea igual o superior a la 2.13.0.

Figura 4- Repositorio de librería ActiveMQ Artemis – Protocolo CORE

2.6.2.3 Librerías Java – protocolo AMQP

La librería JAVA que debe ser utilizada para realizar la implementación de los clientes JMS 2.0, productores y consumidores que hacen uso del protocolo AMQP puede ser descargada de https://mvnrepository.com/artifact/org.apache.qpid/qpid-jms-client. En este repositorio se encuentra la librería y/o la configuración del proyecto Maven en caso que la entidad utilice esta herramienta de construcción de proyectos Java. La Figura 5 presenta una imagen del repositorio donde se encuentra la librería. El BR recomienda que la versión utilizada por la entidad sea igual o superior a la 0.54.0.

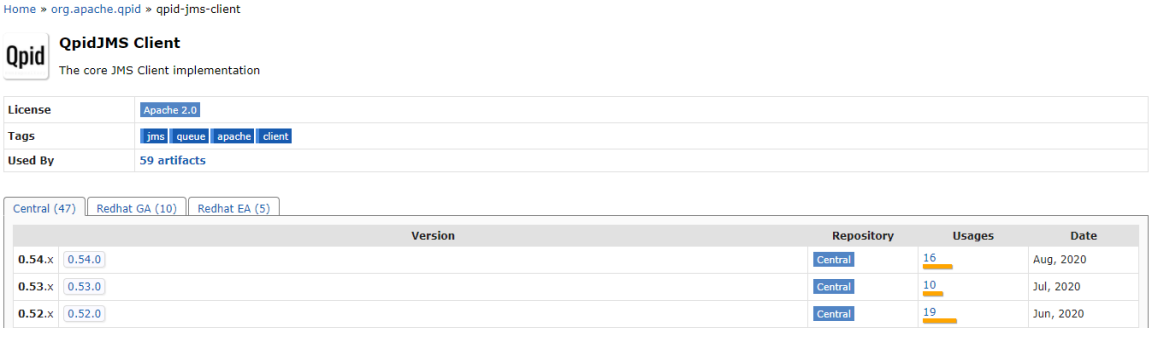


Figura 5- Repositorio de librerías para JMS 2.0 con AMQP

2.6.3 Protocolos de transporte

El protocolo de transporte que debe ser utilizado es:

- TCP

2.6.4 Manejo de JNDI[2]

Los clientes productor y consumidor de mensajes podrían utilizar un Java Naming and Directory Interface (JNDI) para permitir al cliente descubrir y buscar objetos y datos a través de nombres. El Anexo 3.1- Ejemplo de archivo JNDI, presenta la estructura general de un archivo JNDI.

Dentro del archivo JNDI se manejará la cadena de conexión hacia la infraestructura del BR. Esta cadena tiene la siguiente estructura:

```
NombreVariable = (Protocolo1:Servidor1:Puerto1, Protocolo2:Servidor2:Puerto2)?
                 ha=true&
                 retryInterval=1000&
                 retryIntervalMultiplier=1.0&
                 reconnectAttempts=10&
                 sslEnabled=true&
                 trustStorePath= NombreAlmacen1.jks &
                 trustStorePassword=PasswordAlmacen1&
                 keyStorePath= NombreAlmacen2.jks&
                 keyStorePassword= PasswordAlmacen1
```

A continuación una descripción de cada elemento de la cadena de conexión:

[2] https://en.wikipedia.org/wiki/Java_Naming_and_Directory_Interface

Variable	Descripción
Protocolo1:Servidor1:Puerto1	Conexión al servidor principal.
Protocolo2:Servidor2:Puerto2	Conexión al servidor secundario.
ha=true	Parámetro usado para configurar alta disponibilidad entre 2 o más nodos.
retryInterval=1000	Determina el periodo en milisegundos entre los intentos de reconexión si la conexión principal falló.
retryIntervalMultiplier=1.0	Multiplicador usado para calcular el tiempo desde el último hasta el próximo reintento.
reconnectAttempts	Define el número de intentos de reconexión antes de terminar la conexión.
sslEnabled=true	Establece la conexión haciendo uso de SSL.
trustStorePath= NombreAlmacen1.jks	Ruta del truststore usado para autenticar la conexión con el servidor.
trustStorePassword=PasswordAlmacen1	Contraseña del truststore.
keyStorePath= NombreAlmacen2.jks	Ruta del keystore usado para establecer la conexión con el servidor.
keyStorePassword= PasswordAlmacen1	Contraseña del keystore.

Nota: Si bien no es requerido el uso de un archivo JNDI, el BR recomienda su uso para dar flexibilidad a la implementación de clientes de la entidad.

2.6.5 Recomendaciones y buenas prácticas

A continuación, se presentan algunas prácticas sugeridas por el BR para la implementación de los clientes productores y consumidores de mensajes:

- Manejar cierre de conexiones una vez se hayan enviado o consumido mensajes de las colas de la entidad.
- Manejar excepciones para cerrar las conexiones en eventos de falla del cliente. El sistema de mensajería del BR cerrará automáticamente las conexiones que hayan superado un tiempo de inactividad de **2 horas**. Se entiende como inactividad en este caso, conexiones donde el broker de mensajería no recibe un ping del cliente.
- Por ser un modelo asincrónico de comunicación, se recomienda la implementación del productor de mensajes independiente del consumidor de mensajes.

Nota: Esta sección se complementará en la medida en que aparezcan nuevos escenarios de implementación por parte de los clientes de la entidades.

2.7 MENSAJES DE ERROR

A continuación, se encuentra la relación de los mensajes de error identificados por el BR y las posibles explicaciones para cada uno de ellos.

Error	Explicación
AMQ229200	Maximum Consumer Limit Reached on Queue. Se ha alcanzado el número máximo de consumidores para la cola de salida de la entidad.
AMQ219007	Cannot connect to server(s). Tried with all available servers. No es possible conectarse al servidor por parte del cliente. En la mayoría de los casos es un asunto de configuración del cliente.
AMQ214016	Failed to create netty connection. Problemas con la autenticación a través de certificados digitales entre el cliente de la entidad y el sistema de mensajería
AMQ229031	Unable to validate user from /10.201.2.10:XXXX. Username: null. El usuario no está definido correctamente en el sistema de mensajería del BR.
AMQ229032	User: USER does not have permission='SEND' on address ADDRESS. El usuario intenta enviar un mensaje a una cola a la cual no tiene permisos.
AMQ214016	Failed to create netty connection. Problemas con los certificados para lograr autenticación con el middleware de mensajería del BR

Nota 1: Solamente se relacionan los errores que se pueden llegar a presentar al interactuar con el sistema de mensajería del BR. Los errores JAVA son propios de cada implementación.

Nota 2: En el enlace https://access.redhat.com/solutions/4418991 se encuentra una lista de errores AMQ.Para acceder a ella se requiere un registro gratuito en el sitio de Red Hat.

3 ANEXOS

3.1 EJEMPLO DE ARCHIVO JNDI

```
java.naming.factory.initial=org.apache.activemq.artemis.jndi.ActiveMQInitialContextFactory
ConnectionFactory.SslConnectionFactory=(tcp://nasa.banrep.gov.co:5500,
                                       tcp:// nasa.banrep.gov.co:5515)?
                                       ha=true&retryInterval=1000&
                                       retryIntervalMultiplier=1.0&
                                       reconnectAttempts=10&
                                       sslEnabled=true&
                                       trustStorePath=DCVTrusKeytstore.jks&
                                       trustStorePassword=passwordtruststore&
                                       keyStorePath=DCVKeystore.jks&
                                       keyStorePassword= passwordkeystore
queue.queue0/QueueIn=BANCO123456IN
queue.queue1/QueueOut=BANCO123456OUT
queue.queue2/QueueExp=BANCO123456EQ
```

Nota: Este es un ejemplo proporcionado por el BR y se comparte como guía para las implementaciones de las entidades.

3.2 EJEMPLO DE CÓDIGO JMS 2.0 PARA CREACIÓN DE PRODUCTOR

```
public static String Productor() {
    try {
        Context context = new InitialContext();
        ConnectionFactory cf = (ConnectionFactory) context.lookup("SslConnectionFactory");
        Destination queue = (Destination) context.lookup("queue0/queueIn");
        JMSContext jmsContext = cf.createContext();
        JMSProducer productor = jmsContext.createProducer();

        productor.setPriority(4);
        productor.setDeliveryMode(2);
        productor.setTimeToLive(0);
        productor.setJMSCorrelationID("ABC123");
        productor.setProperty("MSG_SENDER", "111.222.333");
        productor.setProperty("MSG_TYPE", "sese.021.002.03");
        productor.setProperty("REF", "ID123");
        productor.setProperty("RELREF", ""); //se debe enviar vacío
        productor.setProperty("SIGN", getFirma());
        String mensaje = "Mensaje XML";
        productor.send(queue, mensaje);
        jmsContext.close();

    } catch (NamingException e) {
        e.printStackTrace();
    }
}
```

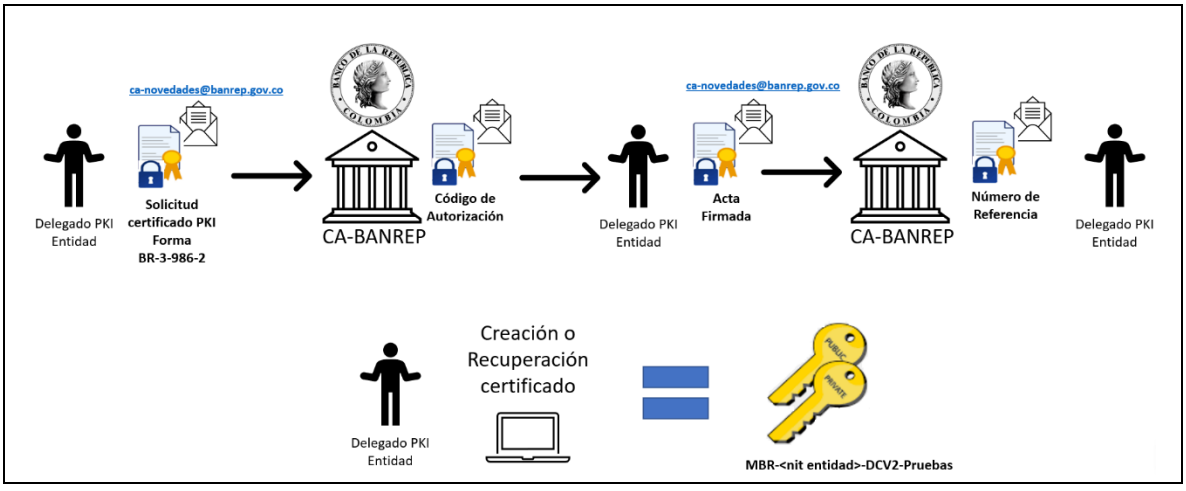
Nota: Este es un ejemplo proporcionado por el BR y se comparte como guía para las implementaciones de productores de mensajes de las entidades.

3.3 EJEMPLO DE CÓDIGO JMS 2.0 PARA CREACIÓN DE CONSUMIDOR

```
public static String Consumidor() {
    try {
        Context context = new InitialContext ();
        ConnectionFactory cf = (ConnectionFactory) context.lookup("SslConnectionFactory");
        Destination queue = (Destination) context.lookup("queue1/queueOut");
        JMSContext jmsContext = cf.createContext();
        JMSConsumer message = jmsContext.createConsumer(queue);
        Message mensaje = message.receive();
        jmsContext.close();
    } catch (NamingException e) {
        e.printStackTrace();
    }
}
```

Nota: Este es un ejemplo proporcionado por el BR y se comparte como guía para las implementaciones de consumidores de mensajes de las entidades.

3.4 PROCEDIMIENTO DE GENERACIÓN DE CERTIFICADO DIGITAL



3.5 EJEMPLO FORMATO BR-3-986-02 AMBIENTE DE PRUEBAS

BR-3-986-2

NOVEDADES DEL SUSCRIPTOR - IDENTIDAD ELECTRÓNICA
BANCO DE LA REPÚBLICA

Fecha: 2022-11-15

Marque con X la opción deseada (Renglón gris: creación identidad electrónica para Persona Jurídica - Renglón blanco: usuario suscriptor)

Mensajería MBR	X	B2B[1]		Procesos automáticos		Pruebas	X	Producción	
Actualizar datos		Incluir	X	Recuperar		Revocar (certificado PKI)		**Retirar Delegado	

Nombres y apellidos del Delegado PKI: **Nombre(s) Apellido(s)**
Número de teléfono del Delegado PKI: **000-000-0000**
Nombre y NIT de la Entidad Usuaria: **Nombre Entidad - 123456789-0**

DATOS DEL SUSCRIPTOR / ENTIDAD

Nombre completo: **Nombre Entidad** No. Cédula/NIT: **Nit Entidad**
Correo electrónico: email@entidadnotificaciones.com Ciudad: **CiudadEntidad**

Nombre de la entidad abierta que emite el certificado[2]:
DN[3]:
Nota: Por favor adjuntar al mensaje el certificado digital (Archivo con extension .cer o .crt)

Observaciones: (Si la solicitud es para incluir, recuerde escribir la dirección del suscriptor , si no lo hace, la solicitud será devuelta)

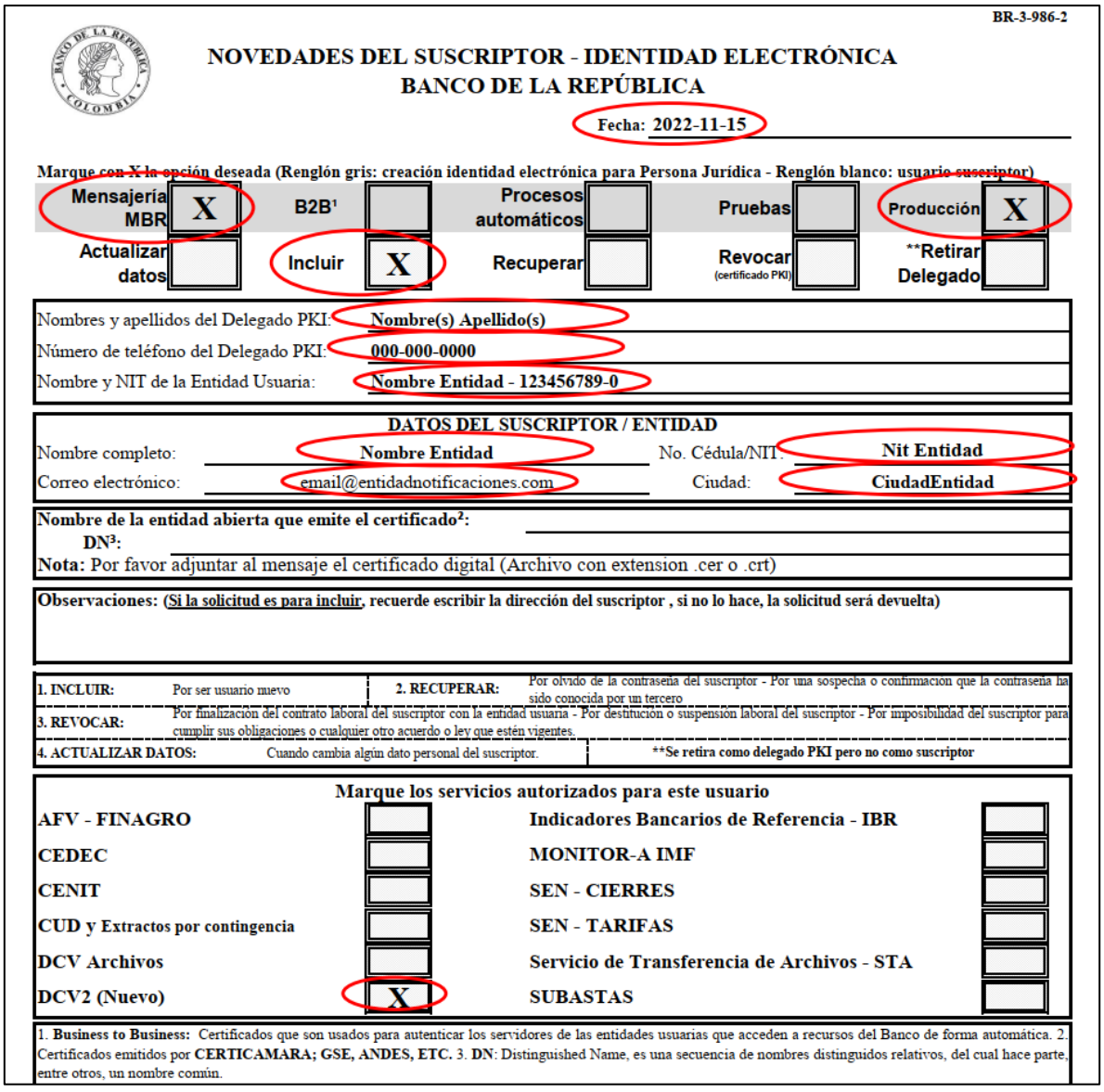
1. INCLUIR:	Por ser usuario nuevo	2. RECUPERAR:	Por olvido de la contraseña del suscriptor - Por una sospecha o confirmacion que la contraseña ha sido conocida por un tercero
3. REVOCAR:	Por finalizacion del contrato laboral del suscriptor con la entidad usuaria - Por destitucion o suspension laboral del suscriptor - Por imposibilidad del suscriptor para cumplir sus obligaciones o cualquier otro acuerdo o ley que estén vigentes.		
4. ACTUALIZAR DATOS:	Cuando cambia algún dato personal del suscriptor.	**Se retira como delegado PKI pero no como suscriptor	

Marque los servicios autorizados para este usuario

AFV - FINAGRO		Indicadores Bancarios de Referencia - IBR	
CEDEC		MONITOR-A IMF	
CENIT		SEN - CIERRES	
CUD y Extractos por contingencia		SEN - TARIFAS	
DCV Archivos		Servicio de Transferencia de Archivos - STA	
DCV2 (Nuevo)	X	SUBASTAS	

1. **Business to Business**: Certificados que son usados para autenticar los servidores de las entidades usuarias que acceden a recursos del Banco de forma automática. 2. Certificados emitidos por **CERTICAMARA; GSE, ANDES, ETC**. 3. **DN**: Distinguished Name, es una secuencia de nombres distinguidos relativos, del cual hace parte, entre otros, un nombre común.

3.6 EJEMPLO FORMATO BR-3-986-02 AMBIENTE DE PRODUCCIÓN



BR-3-986-2

NOVEDADES DEL SUSCRIPTOR - IDENTIDAD ELECTRÓNICA
BANCO DE LA REPÚBLICA

Fecha: 2022-11-15

Marque con X la opción deseada (Renglón gris: creación identidad electrónica para Persona Jurídica - Renglón blanco: usuario suscriptor)

Mensajería MBR	X	B2B[1]		Procesos automáticos		Pruebas		Producción	X
Actualizar datos		Incluir	X	Recuperar		Revocar (certificado PKI)		**Retirar Delegado	

Nombres y apellidos del Delegado PKI: **Nombre(s) Apellido(s)**
Número de teléfono del Delegado PKI: **000-000-0000**
Nombre y NIT de la Entidad Usuaria: **Nombre Entidad - 123456789-0**

DATOS DEL SUSCRIPTOR / ENTIDAD

Nombre completo: **Nombre Entidad** No. Cédula/NIT: **Nit Entidad**
Correo electrónico: email@entidadnotificaciones.com Ciudad: **CiudadEntidad**

Nombre de la entidad abierta que emite el certificado[2]:
DN[3]:
Nota: Por favor adjuntar al mensaje el certificado digital (Archivo con extension .cer o .crt)

Observaciones: (Si la solicitud es para incluir, recuerde escribir la dirección del suscriptor , si no lo hace, la solicitud será devuelta)

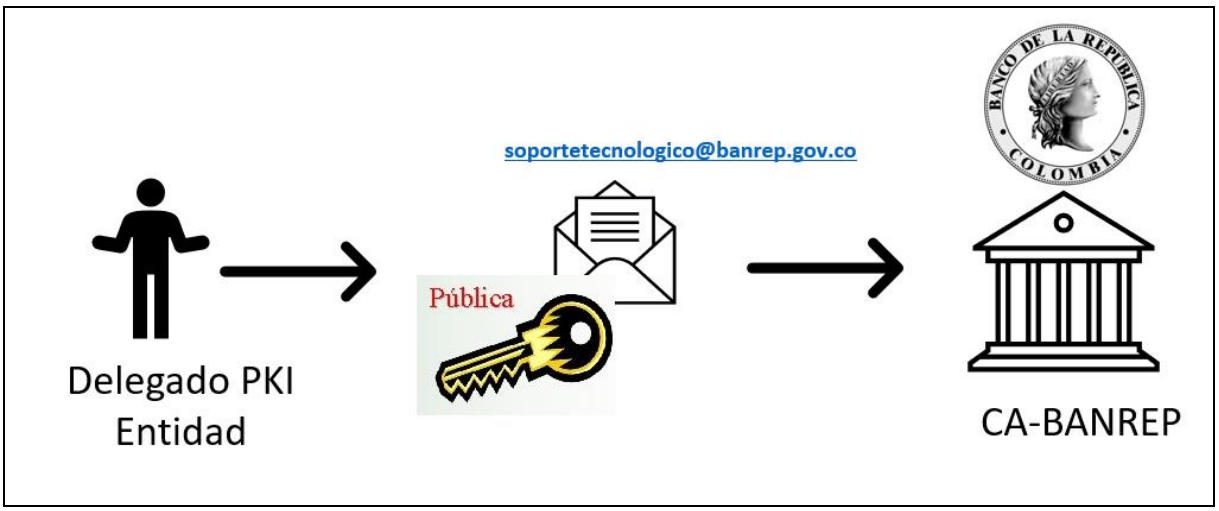
1. INCLUIR:	Por ser usuario nuevo	**2. RECUPERAR:**	Por olvido de la contraseña del suscriptor - Por una sospecha o confirmacion que la contraseña ha sido conocida por un tercero
3. REVOCAR:	Por finalizacion del contrato laboral del suscriptor con la entidad usuaria - Por destitucion o suspension laboral del suscriptor - Por imposibilidad del suscriptor para cumplir sus obligaciones o cualquier otro acuerdo o ley que estén vigentes.		
4. ACTUALIZAR DATOS:	Cuando cambia algún dato personal del suscriptor.	****Se retira como delegado PKI pero no como suscriptor**	

Marque los servicios autorizados para este usuario

AFV - FINAGRO		**Indicadores Bancarios de Referencia - IBR**	
CEDEC		**MONITOR-A IMF**	
CENIT		**SEN - CIERRES**	
CUD y Extractos por contingencia		**SEN - TARIFAS**	
DCV Archivos		**Servicio de Transferencia de Archivos - STA**	
DCV2 (Nuevo)	X	**SUBASTAS**	

1. **Business to Business:** Certificados que son usados para autenticar los servidores de las entidades usuarias que acceden a recursos del Banco de forma automática. 2. Certificados emitidos por **CERTICAMARA; GSE, ANDES, ETC.** 3. **DN**: Distinguished Name, es una secuencia de nombres distinguidos relativos, del cual hace parte, entre otros, un nombre común.

3.7 PROCEDIMIENTO PARA LA ENTREGA DE LA LLAVE PÚBLICA DE LA ENTIDAD



HISTORIAL DE CAMBIOS

Versión 1.0

Fecha 2020-09-24

Responsable Juan Manuel Cubillos.

Descripción: Liberación versión 1.0 del documento

Versión 1.1

Fecha 2020-10-21

Responsables: Carlos Mario Paredes, Alejandro Rodríguez y Juan Manuel Cubillos.

Descripción:

- Ajuste de información técnica de firma de mensajes ISO20022.
- Sección 2.5.5 Firma de Mensajes ISO 20022.
- Se cambian las librerías Bouncy Castle por librerías nativas Java.security Inclusión de ejemplos de firma y validación de firma de mensajes ISO 20022.

Versión 1.2

Fecha 2021-02-12

Responsables:

Descripción:

- Actualización de la nota 1 de la sección 2.2.4.
- Eliminación del Tercer Nodo Tecnológico para el diagrama de despliegue.
- Inclusión del formato UTF-8 para los mensajes ISO-20022.
- Inclusión del formato UTF-8 para la propiedad “sign”.
- Inclusión de la Nueva cola Verificaciones Técnicas.
- Actualización de las librerías de JAVA Inclusión de sección Creación de Certificados Digitales.
- Inclusión nota 3 Conexión ambiente de pruebas a través de Nasa.

- Actualización de diagrama Modelo de Interoperabilidad para el Nuevo DCV Ajuste a las reglas de juego de mensajes expirados.

Versión 1.3

Fecha 2022-03-28

Responsables:

Descripción:

- Actualización de la versión del protocolo AMQP 1.0 – Sección 2.6.2.
- Eliminación de notas de la sección 2.2.2.
- Los ambientes de pruebas y producción ya se encuentran configurados.
- Creación de sección 2.3 de Certificados Digitales Organización de la sección 2.2
- Conectividad Eliminación de la Sección 2.7
- Creación de certificados digitales Estadanzarización de tamaño máximo de mensajes JMS (Header + Payload) Inclusión de explicaciones de expiración de mensajes de las colas de salida y validaciones técnicas. Inclusión del Anexo 3.4. Diagrama del procedimiento para solicitar certificados digitales.
- Aclaración de atributo Timestamp del header del mensaje JMS (Inclusión en filtro de validaciones técnicas y definición en el encabezado).

Versión 1.4

Fecha 2022-11-15

Responsables: Carlos Mario Paredes, Alejandro Rodríguez y Andrés Tangarife.

Descripción:

- Inclusión de dos (2) anexos explicativos de la forma como debe ser diligenciado el formato BR-3-986-2.
- Reemplazo del formato BR-3-598-02 por el BR-3-986-2.
- Ajustar los enlaces para descargar el formulario BR-3-986-2.

Versión 1.5

Fecha 2022-12-01

Responsables: Carlos Mario Paredes y Andrés Tangarife.

Descripción:

- Inclusión de un (1) anexo que explica la forma como se envían las llaves públicas al Banco.
- Ajuste gráfica Anexo 3.4.