MINISTERIO DE LA PRESIDENCIA
ESTADO PLURINACIONAL DE BOLIVIA

AGETIC
agencia de gobierno electrónico y tecnologías de información y comunicación

Ciudadanía Digital

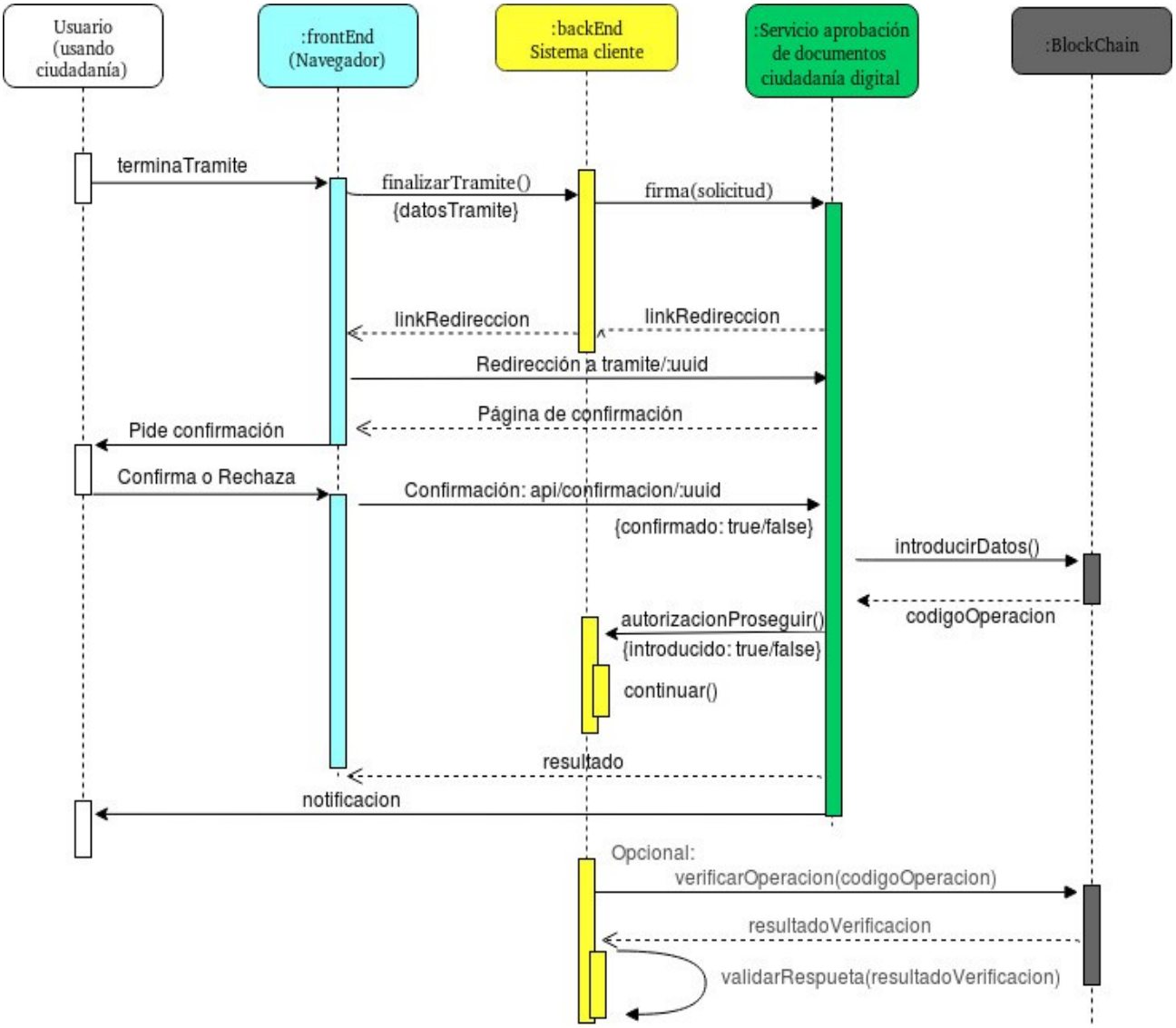
Especificaciones técnicas para el servicio de Aprobación

Versión 1.1

Contenido

1. DESCRIPCIÓN

Este servicio provee un mecanismo para que un ciudadano digital dé su consentimiento para la aprobación de un documento usando su cuenta de ciudadanía digital desde sistemas cliente. También permite verificar la autenticidad, integridad y trazabilidad de los documentos aprobados con este mecanismo. El servicio introduce los datos enviados en el registro de orden cronológico e integridad permitiendo verificar que los documentos enviados no han sido alterados por el sistema cliente, también permite a los sistemas cliente demostrar la autorización y consentimiento del envío de documentos o datos por parte del propietario del recurso.



El flujo para la aprobación de documentos se muestra en el diagrama, donde hay cuatro actores; El ciudadano que mediante un navegador interactúa con el servicio , el sistema cliente que envía la solicitud de aprobación, el servicio de aprobación de ciudadanía digital y el registro de orden cronológico e integridad (blockchain).

1.1 DESCRIPCIÓN DE ACTORES

- Cliente (Client)
  Es el Sistema Cliente, el cual hace peticiones de aprobación de documentos en nombre del usuario (el usuario debe haber iniciado sesión en el sistema cliente con su cuenta de ciudadanía digital).
- Servidor de aprobación de documentos (signature-service)
  El Sistema de aprobación de documentos es el responsable de validar y registrar la operación en el registro de orden cronológico e integridad los datos que envía el sistema cliente para la confirmación del ciudadano.
- Registro de orden cronológico e integridad (cadena de bloques o blockchain)
  Es un registro de documentos y datos digitales que permite verificar posteriormente con grado de certeza la existencia y orden cronológico del registro de un documento o dato y la integridad del mismo.
- Propietario del recurso
  Ciudadano identificado en el sistema cliente con su cuenta de ciudadanía digital.

El proceso de aprobación comienza con el sistema cliente enviando una solicitud al servicio de aprobación de ciudadanía digital, luego de comprobar sesión este servicio le responde con un enlace donde el propietario del recurso puede ver el documento y confirmar o rechazar su aprobación. Dependiendo de la decisión el servicio lo registra en la cadena de bloques (blockchain) y notifica al sistema cliente y al ciudadano de la conclusión de la operación de aprobación.

1.2 CONSIDERACIONES REGISTRO DE SISTEMA CLIENTE A CIUDADANÍA DIGITAL

Para poder usar este servicio, el sistema cliente debe haber registrado los siguientes campos en el registro de ciudadanía digital del servicio de autenticación con ciudadanía digital:

- **redirect_uris_signature**: Que es el arreglo de urls que este servicio usa para notificar al sistema cliente sobre el resultado del proceso de aprobación de documentos. El primer elemento es la url del backend del sistema cliente al que hace la notificación para proseguir, el segundo elemento es la ruta del frontend para redireccionar al ciudadano a la página del sistema cliente donde puede ver resultados del proceso.
- **authorization_token**: El servicio de aprobación adjuntará este token a la cabecera “Authorization” de la petición al backend del sistema cliente que le informa de la conclusión del proceso de aprobación por parte del propietario del recurso.

2. FLUJO DE APROBACIÓN

2.1 SOLICITUD DE APROBACIÓN DE DOCUMENTOS

Para la solicitud de aprobación de documentos, el sistema cliente debe enviar una petición al servicio de ciudadanía digital, el cual se describe a continuación:

TIPO: POST

```
https://<url-base-servicio-interoperabilidad-aprobacion-firma>
```

Header

Campo	Tipo	Descripción
authorization	String	Bearer + *token_interoperabilidad* Token de autorización para consumir la ruta en la plataforma de interoperabildiad.
content-type	String	Contenido enviado en la solicitud (application/json)

Parámetros

campo	Tipo	Descripción
tipoDocumento	String	Tipo de Objeto a aprobar, los valores que se puede enviar PDF ó JSON
documento	string	Cadena con el valor del objeto, el PDF o JSON deben enviarse como string, en caso de objetos se deben enviar siguiendo el estándar JSON descrito en http://json.org/ para strings.
hashDocumento	String	Hash (sha256) del campo documento
descripcion	String	Operación que el ciudadano está realizando en el sistema cliente
idTramite	String	Identificador único de trámite generado por el sistema cliente, se espera un campo del tipo uuidv4.
token	string	El token es obtenido en el inicio de sesión del ciudadano mediante ciudadanía digital, el sistema cliente debe definir el mecanismo para guardar este *access_token* que tiene validez igual al tiempo de la sesión de ciudadanía digital. Si este caduca es necesario que el ciudadano vuelva a iniciar sesión en ciudadanía.

Ejemplo solicitud de aprobación de documentos PDF (curl):

```
curl -X POST \
     'https://<url-base-servicio-interoperabilidad-aprobacion-firma> \
     -H 'Authorization: Bearer <token-interoperabilidad>'
     -d '{
           "tipoDocumento": "PDF",
           "documento": "UIOJLKJJKKkdfsdfseeeoooe ....",
           "hashDocumento": "c1f246612c",
           "idTramite": "fdc5b6cd-5e54-45d9-a319-1977ee73d925",
           "descripcion": "Trámite de prueba PDF",
           "token": "0UCOcFmVx5REpbeOHzpgf_z4jaduw7gQJWltcLB8Gdk"
     }'
```

Ejemplo solicitud de aprobación de documentos JSON (curl):

```
curl -X POST \
  https://<url-base-servicio-interoperabilidad-aprobación-firma> \
  -H 'Authorization: Bearer <token_interoperabilidad>' \
  -H 'Content-Type: application/json' \
  -d '{
         "tipoDocumento": "JSON",
         "documento": "[{\"clave\":\"PARA\",\"tipo\":\"texto\",\"valor\":\"Juan
Perez\"},{\"clave\":\"ASUNTO\",\"tipo\":\"texto\",\"valor\":\"Adquisición de
accesoriosGSM-IP 16 canales\"}]",
       "hashDocumento": "d1f2853as902a45...",
       "idTramite": "9dd95700-cb0d-11e8-a9c0-29fb28bbb654"
       "descripcion": "Tramite de prueba JSON",
       "token": "0UCOcFmVx5REpbeOHzpgf_z4jaduw7gQJWltcLB8Gdk"
}'
```

Ejemplo de respuesta exitosa (para PDF y JSON):

HTTP status code: 200

```
{
  "finalizado": true,
  “estadoProceso”: “exito”,
  "link": "https://<base-url-servicio-aprobación>/tramite/9dd95700-cb0d-11e8-a9c0-
29fb28bbb654"
}
```

Ejemplo de respuesta errónea:

HTTP status code: 400

```
{
  "finalizado": false,
  “estadoProceso”: “Ya existe una solicitud con uuid 5c6c608cc2dfaa06efa5f396”,
  "link": ""
}
```

Estructura objeto a aprobar (`documento`)

Tipo del Documento [JSON|PDF]

documento	Esquema del documento: En caso de tipo PDF el campo data recibe un string en base64 del documento. (tamaño máximo 5 MB) En caso de tipo JSON el campo data recibe un arreglo con los valores del formulario. El array debe estar representado como una cadena JSON siguiendo el estándar JSON descrito en http://json.org/ para strings. (tamaño máximo 5 MB)

Ejemplos de Estructura de Documento de tipo PDF

```
"documento": "JVBeRi0..."
```

Luego de completar la solicitud de aprobación de trámite, el servicio de aprobación mostrará una pantalla con el documento siendo aprobado y dos botones, uno para confirmar y otro para rechazar el proceso de aprobación. Esta pantalla posteriormente de acuerdo a la decisión del usuario realizará la notificación al sistema cliente.

Estructura de un documento de tipo JSON

El servicio acepta un objeto JSON representado como cadena JSON siguiendo el estándar descrito en http://json.org/ para strings.

Ejemplos de Estructura de Documento de tipo JSON

```
“documento": “{\"documento\":\"Aprobación de documento de declaración\",\"nro-
documento\":90032,\"codigo-documento\":\"AC78-90032-2019\",\"remitentes\":
[{\"item\":\"cuid-56\",\"fecha-firma\":\"2019/11/01 14:00:32\"},{\"item\":\"cuid-
56\",\"fecha-firma\":\"2019/10/18 18:10:20\"}],\"contenido\":\"Meidante la presente se
aprueba el documento AC78-90032-2019 y se confirma la
revisión\",\"observacion\":\"\",\"revisor\":{\"item\":\"atru-12\",\"fecha-
firma\":\"2019/11/03 14:11:20\"}}"
```

2.2 NOTIFICACIÓN SOLICITUD DE APROBACIÓN DE DOCUMENTOS.

El sistema cliente debe exponer un servicio REST con formato JSON para que se pueda notificar si el ciudadano acepto o rechazo la aprobación del documento. El servicio de aprobación utilizará los campos *redirect_uris_signature* ([0] backend, [1] frontend) que el sistema cliente ha registrado anteriormente en la integración con la autenticación de ciudadanía digital.

- Se envía esta notificación directamente al backend del sistema cliente.

URL: redirect_uris_signature[0] (backend, este es el paso “autorizaciónProseguir()”)

MÉTODO: POST
Header

Campo	Tipo	Descripción
authorization	String	Token de autorización *authorization_token* que el sistema cliente ha registrado para la autenticación con ciudadanía digital.
content-type	String	Contenido enviado en la solicitud (JSON)

El cuerpo del mensaje enviado por el servicio de aprobación con ciudadanía digital es el siguiente:

campo	Tipo	Descripción
aceptado	boolean	Parámetro que indica si el ciudadano acepto/rechazó los datos del trámite. El trámite se registra en la cadena de bloques sólo si *aceptado* es *true*
introducido	boolean	Parámetro que indica si se ha conseguido introducir el registro en la cadena de bloques exitosamente. En caso de error este campo es *false* y el sistema deberá volver a enviar la solicitud de aprobación (con campo *idTramite* distinto) si require volver a pedir la aprobación del ciudadano.
requestUuid	string	Identificador de la solicitud del trámite (el mismo que el sistema cliente envío como *idTramite* al iniciar el flujo).
codigoOperacion	string	Identificador adicional de solicitud de aprobación. Se envía una cadena vacía en caso de que el campo *introducido* sea *false.*
mensaje	string	Mensaje del resultado de la operación, cuando el campo *introducido* es *false* en este campo se especifica el error.
transaction_id	string	Código de transacción para comprobaciones en la blockchain. Se envía cadena vacía en caso de que el campo *introducido* sea *false.*
fechaHoraSolicitud	string	Fecha y hora en que se ha realizado la solicitud de firma en formato DD/MM/YYYY HH:mm:ss.SSS

hashDatos	String	Digesto del algoritmo hash aplicado al contenido del trámite a aprobar.
ci	string	Número de documento del ciudadano que usa el servicio.

Respuesta que se espera del sistema cliente

HTTP Status Code: 200

campo	Tipo	Descripción
finalizado	boolean	Resultado de la operación en el sistema cliente, debería ser *true*. (proceso del trámite)
mensaje	string	Mensaje del resultado de la operación (opcional)

Luego de realizar esta notificación de solicitud de aprobación de documentos, desde la pantalla con el diálogo de aprobación y rechazo se redireccionará al ciudadano a la URI *redirect_uris_signature[1]* para mostrar una pantalla de notificación con el resultado del trámite realizado, se envían parámetros para que el sistema cliente muestre detalles de la operación realizada.

Los parámetros enviados son los siguientes:

campo	Tipo	Descripción
finalizado	boolean	Resultado de la aprobación o rechazo del trámite realizado, *true* si se confirmó y realizó, *false* si no se realizó la aprobación.
estado	boolean	Indica si el usuario ha confirmado o rechazado la aprobación del trámite.
mensaje	string	Mensaje del resultado de la operación, con valores posibles: - Caso 1: (usuario rechaza la aprobación): “La persona interesada ha rechazado la aprobación del trámite o documento ”. - Caso 2: (usuario acepta la aprobación pero se produce un error introduciendo el registro en la cadena de bloques): “El-servicio-de-orden-cronológico-no-está-disponible-en-este-momento.” - Caso 3: (usuario acepta la aprobación y se ha introducido el registro exitosamente en la cadena de bloques): “Completado”
linkVerificacion	string	Enlace de verificación general.
linkVerificacionUnico	string	Enlace de verificación exclusivo para este documento.
transactionCode	string	Identificador único del trámite en la blockchain, se puede utilizar para hacer la verificación única del documento en cualquier servicio de verificación de documentos en la blockchain.

requestUuid	string	Campo *requestUuid* enviado al iniciar el flujo de aprobación
rediurectUri	string	URL de redirección con los parámetros: *finalizado*, *estado, mensaje, linkVerificacionUnico, linkVerificacion, transactionCode, requestUuid*

Ejemplo de respuesta redirección:


```
{
  "finalizado": true,
  "estado": true,
  "mensaje": "Completado",
  "linkVerificacion": "<url-verificacion>",
  "linkVerificacionUnico" "<url-verifcacion-
unica>8e1f761ae9f33545925fd6ed73fa26606a7f0be52cc81a439381b6565de716ea",
  "redirectUri":  "<redirect_uris_signature[1]>?
estado=true&finalizado=true&mensaje=&linkVerificacion=<url-
verificacion>&linkVerificacionUnico=<url-verificacion-
unica>8e1f761ae9f33545925fd6ed73fa26606a7f0be52cc81a439381b6565de716ea&transactionCode=8e1f
761ae9f33545925fd6ed73fa26606a7f0be52cc81a439381b6565de716ea&requestUuid=fdc5b6cd-5e54-
45d9-a319-1977ee73d925",
  "transactionCode": "8e1f761ae9f33545925fd6ed73fa26606a7f0be52cc81a439381b6565de716ea",
  "requestUuid": "fdc5b6cd-5e54-45d9-a319-1977ee73d925"
}
```


Una vez que se termina el proceso de aprobación, el sistema cliente puede continuar con el flujo normal del procesamiento del trámite del usuario.

3. SERVICIO DE VERIFICACIÓN

Este servicio permite verificar si se ha registrado la aprobación de un documento consultando la cadena de bloques.

3.1 VERIFICACIÓN POR HASH

TIPO: POST

```
https://<url-base-servicio-interoperabilidad-aprobacion-verificar>
```

Header

Campo	Tipo	Descripción
authorization	String	Bearer + *token_interoperabilidad* Token de autorización para consumir la ruta en la plataforma de interoperabildiad.
content-type	String	Contenido enviado en la solicitud (JSON)

Parámetros

campo	Tipo	Descripción
archivo	String	Cadena con el contenido siendo verificado. En caso de tipo PDF el campo es una cadena en base64 del documento.

El servicio recibirá el contenido del archivo enviado en el campo *archivo* y calculará el hash (sha256) de esta cadena, hace una consulta a la cadena de bloques si existen registros asociados a ese hash calculado y retorna los registros encontrados con el siguiente formato.

campo		Tipo	Descripción
verificacionCorrecta		boolean	Si se han encontrado registros asociados a el hash calculado del campo *archivo* enviado. Retorna **true** en caso de encontrar al menos un registro y **false** en caso de no encontrar registros.
registros		array	Un arreglo con los registros encontrados, será un array vacio en caso de no encontrar registros
cada objeto en el array	descripcion	string	Nombre del trámite enviado
	hashDatos	string	hash calculado de la cadena enviada

registros contiene los campos:	fechaSolicitud	string	Fecha y hora en que se hizo la solcitud de aprobación en formato: DD/MM/AAAA HH:mm:ss.SSS por ejemplo: 23/10/2019 09:33:13.000
	ci	string	Documento de identidad del ciudadano que realizó la acción de aprobación de este contenido.
	nombres	string	Nombres del ciudadano
	primer_apellido	string	Primer apellido del ciudadano
	segundo_apellido	string	Segundo apellido del ciudadano
	codigoOperacion	string	Identificador de la transacción realizada en la cadena de bloques.
	uuidBlockchain	string	campo de verificación adicional.

Ejemplo cuerpo de verificación:

```
{
  "archivo":
“JVBERi0xLjQNCjEgMCBvYmoNCjw8IA0KL0xlbmd0aCA4MjQ4DQovRmlsdGVyIC9GbGF0ZURlY29kZQ0KPj...”
}
```

Ejemplo cuerpo de respuesta verificación:

```
{
  "verificacionCorrecta": true,
  "registros": [
    {
      "timestamp": "2019-10-23 13:34:22.503 +0000 UTC",
      "codigoOperacion":
"04b20ea95e6fee207eeec5f29a6f01cde8ba5ec44165fd65831ff5a6cd8af48b",
      "segundo_apellido": "MACUAPA",
      "primer_apellido": "ROCHA",
      "nombres": "MARIANA",
      "ci": "4206088",
      "fechaSolicitud": "23\/10\/2019 09:33:13.000",
      "hashDatos": "1db05053051c5f73e6938fef1c60d2f3e6c22291a088dc07191e1b0f85c0aecc",
      "descripcion": "Tramite de prueba PDF",
      "uuidBlockchain": "80b22c6f-0fc9-4439-9888-06555e11d265"
    }
  ]
}
```

3.1 VERIFICACIÓN POR TRANSACTION_ID

TIPO: POST

```
https://<url-base-servicio-interoperabilidad-aprobacion-verificar>/
<transaction_id>
```

Header

Campo	Tipo	Descripción
authorization	String	Bearer + *token_interoperabilidad* Token de autorización para consumir la ruta en la plataforma de interoperabildiad.
content-type	String	Contenido enviado en la solicitud (JSON)

Parámetros

campo	Tipo	Descripción
archivo	String	Cadena con el contenido siendo verificado. En caso de tipo PDF el campo es una cadena en base64 del documento.

El servicio recibirá el contenido del archivo enviado en el campo *archivo* y calculará el hash (sha256) de esta cadena, hace una consulta a la cadena de bloques si existe un registro asociado al *transaction_id* enviado (URI) y si ese registro coincide con el *hash* calculado. Se devuelve el registro de la forma:

campo		Tipo	Descripción
verificacionCorrecta		boolean	Si se han encontrado registros asociados a el hash calculado del campo *archivo* enviado. Retorna **true** en caso de encontrar al menos un registro y **false** en caso de no encontrar registros.
registros		array	Un arreglo con los registros encontrados, será un array vacio en caso de no encontrar registros
cada objeto en el array del registro contiene los campos:	descripcion	string	Nombre del trámite enviado
	hashDatos	string	hash calculado de la cadena enviada
	fechaSolicitud	string	Fecha y hora en que se hizo la solcitud de aprobación en formato: DD/MM/AAAA HH:mm:ss.SSS por ejemplo: 23/10/2019 09:33:13.000
	ci	string	Documento de identidad del ciudadano que realizó la acción de aprobación de este contenido.

	nombres	string	Nombres del ciudadano
	primer_apellido	string	Primer apellido del ciudadano
	segundo_apellido	string	Segundo apellido del ciudadano
	codigoOperacion	string	Identificador de la transacción realizada en la cadena de bloques.
	uuidBlockchain	string	campo de verificación adicional.

4. INFORMACIÓN ADICIONAL

4.1 URLs AMBIENTE DE PRUEBAS

Existe un ambiente para pruebas de integración del servicio:

Nombre	URL test
`<url-base-servicio-interoperabilidad-aprobacion-firma>`	`https://interoperabilidad.agetic.gob.bo/fake/aprobacion-documentos/v1/aprobaciones`
`<url-base-servicio-interoperabilidad-aprobacion-verificar>`	`https://interoperabilidad.agetic.gob.bo/fake/aprobacion-documentos/v1/verificaciones`

4.2 SOBRE GUARDADO DE DATOS EN LA CADENA DE BLOQUES

El servicio de aprobación guarda en la cadena de bloques un registro de la acción de aprobación y no el documento PDF o JSON enviado. Una vez se registra la acción de aprobación en la cadena de bloques y se notifica al ciudadano, se elimina el documento enviado en la base de datos temporal del servicio y también se elimina cuando el ciudadano rechaza la acción de aprobación.

Por cada solicitud de aprobación se guarda la siguiente información en la cadena de bloques de acuerdo a un contrato inteligente con la siguiente estructura, donde todos los campos son del tipo cadena de texto:

Campo	Descripción
transaction_id	Identificador único de la transacción una vez realizada
uuidBlockchain	Identificador adicional de la transacción
uuid	Identificador del trámite (campo *tramiteId* enviado al inicio del flujo)
sub	Código *sub* devuelto por el proveedor de identidad de ciudadanía digital
hashFingerprint	*Hashfingerprint* devuelto por el proveedor de identidad de ciudadanía digital
hashDatos	Hash del documento (sha256). Este campo se usa como identificador para verificar si

	un documento existe en la cadena de bloques
fechaSolicitud	Fecha hora de solicitud
fechaInicioSesion	Fecha y hora de inicio de sesión devuelto por el proveedor de identidad
clienteId	Id del sistema cliente que hace la petición devuelto por el proveedor de identidad de ciudadanía digital.
grantId	*grantId* devuelto por el proveedor de identidad
ci	Número de documento de identidad del ciudadano (Devuelto por el proveedor de identidad de ciudadanía digital)
nombres	Nombres del ciudadano realizando la acción de aprobación
primer_apellido	Primer apellido del ciudadano realizando la acción de aprobación
segundo_apellido	Segundo apellido del ciudadano realizando la acción de aprobación
descripcion	Descripción del trámite enviado por el sistema cliente