· Gestor Transaccional genera y envía el mensaje de correo electrónico informativo sobre la operación realizada a todos los destinatarios especificados en el mensaje de solicitud (opcional).

Cuando se envía una petición de fechado al servidor de TSA, es obligatorio enviar el hash del documento. En el caso de solicitud de fechado, el servidor no dispone del documento, es por eso que el hash lo tiene generar el Cliente, pero en el caso de custodia, el Cliente envía el documento a la aplicación por lo tanto se puede generar el hash en los servidores, quitando de esta forma carga de proceso a la aplicación Cliente.

Es por eso que para el caso de custodia, el mensaje que sale del API Cliente no incluye el hash del documento y será la aplicación de Custodia quien al recibir el mensaje generará el hash utilizando el documento contenido en el mensaje y construirá el mensaje com-pleto para el servidor de fechado.

De igual forma que en el punto anterior, este fechado digital se tendrá que guardar auto-máticamente en una ruta de la máquina definida para tal efecto cambiando el nombre del token de manera adecuada para que sea fácil reconocerlo y poderlo asociar al documento original (nombre_ del_ documento_ origen.fecha_de_la_petición.token.der).

Descripción de los mensajes.

Contenido del mensaje de petición de custodia de un documento requestTimeStampWi-thCustody:

- Identificador de Contrato
- Tipo de operación
- Nombre del documento
- Huella digital del documento (hash del documento) calculado en el Cliente
- Campo libre
- Documento cifrado con la clave simétrica
- Clave simétrica cifrada con la clave pública
- Lista con los destinatarios de e-recibo
- Tipo de identificador para cada destinatario
- Identificación para cada componente de la lista con los destinatarios de e-recibo
- Certificado digital del cliente
- Firma digital del cliente sobre el mensaje

Contenido del mensaje de respuesta returnTimeStampWithCustody:

- Información sobre el resultado de la petición y posibles causas del problema si éste aparece
- Fechado digital
- Referencia de custodia
- Firma digital del mensaje

Recuperación de un documento en custodia

Un documento bajo custodia podrá ser consultado o recuperado posteriormente por parte del cliente que lo entregó en custodia.

· El cliente solicita la recuperación de un documento en custodia enviando el men-saje getDocument.

· El servicio de custodia realiza la autenticación y autorización de la solicitud.

· El Gestor Transaccional obtiene de la base de datos el fechado digital y el docu-mento custodiado

· El Gestor Transaccional verifica si el fechado digital recibido en el mensaje de so-licitud getDocument corresponde al documento y el fechado digital recuperado de la base de datos de Custodia. Esta verificación consta de las siguientes fases:

o Verificación la firma digital del fechado digital recibido

o Validación del fechado digital con el documento recuperado de la base de datos

o Validación que la fecha de expiración de la custodia no haya sido superada

· En caso de una verificación correcta el Gestor Transaccional descifra el documento custodiado.

· Gestor Transaccional genera y envía al cliente el mensaje de respuesta returnDo-cument.

-

Descripción de los mensajes.

Contenido del mensaje de petición de recuperación de documento bajo custodia getDo-cument:

- Identificador de Contrato
- Tipo de operación
- Fechado digital