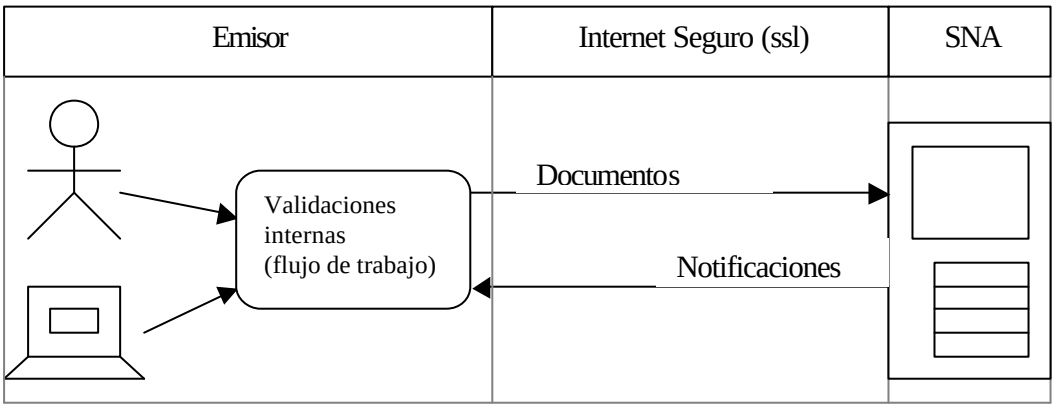
Introducción a la Firma Electrónica en MIDAS

Firma Digital

Introducción.

El Módulo para la Integración de Documentos y Acceso a los Sistemas(MIDAS) emplea la firma digital como método de aseguramiento de la integridad de los datos que se envían y como certificación del emisor de estos datos.

Este módulo permite la creación de documentos, ya sea digitándolos o importando sus datos desde otros sistemas. Estos documentos pueden entrar a un ciclo de validaciones por personas de la misma organización y finalmente son enviados hacia un servidor. Esto se resume en el siguiente esquema:



El firmado de documentos por MIDAS ocurre en dos instancias. En la primera, los documentos son firmados internamente (en la misma organización del emisor) y en la segunda, durante los procesos de envío de documentos hacia el servidor y de notificaciones desde el servidor.

En el primer caso, la utilidad de la firma es sólo para la organización que actúa de emisor, ya que le permite certificar la validación de documentos por personas naturales de la misma organización y asegura que estos datos no son luego modificados (antes de enviarse al servidor).

En el caso del servidor, el firmado de los documentos ocurre al momento de éstos ser enviados. En este caso, la firma es una certificación del emisor como organización, no como una persona natural dentro de esta organización. Al mismo tiempo, las notificaciones que se envían desde el servidor, se firman antes de ser enviadas.

Firma digital

La firma digital es un proceso mediante el cual es posible técnicamente asegurar que un conjunto de datos (documento) no ha sido modificado desde el momento en que éste es firmado y el momento en que es consultado.

La basa de la firma digital se centra en algoritmos asimétricos o de clave pública, el concepto de clave pública se sustenta en el uso de un par de llaves (una es privada y la otra pública). Cuando hablamos de llave pública nos referimos a los certificados digitales y cuando hablamos de llave privada se trata de una clave que sólo el dueño del certificado conoce y fue generada en el momento de obtener su certificado digital. Esta clave puede estar protegida por otra, para evitar confusiones , a esta otra clave la denominaremos “clave del contenedor”, con esta última se puede obtener la llave privada desde un contenedor de claves protegido.

Tanto la llave privada como el certificado digital (Contiene la clave pública) deben ser entregados a cada persona por las organizaciones autorizadas para la emisión de certificados. El uso del par de claves es el siguiente: la llave pública se usa para asegurar que un documento ha sido firmado usando su correspondiente llave privada.

Por lo general, la llave privada se encuentra encriptada dentro de un contenedor (un archivo encriptado que puede encontrarse en un medio magnético o dispositivo externo al PC). Usando la clave del contenedor , que sólo debe conocer el firmante, se abre el contenedor , se obtiene la clave privada y se procede al proceso de firma.

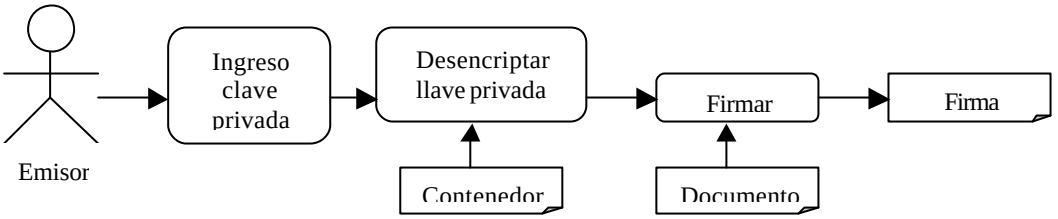
El proceso de firma emplea algoritmos que permiten obtener una secuencia de números a partir de los datos originales que se desean firmar. Esta serie de número es lo que se denomina "firma digital".

La validación de la firma; es decir, asegurar que efectivamente el documento no fue adulterado y corresponde al emisor que firma, ocurre de la siguiente forma: usando el certificado digital del emisor, se obtiene la llave pública, luego utilizando la llave pública se desencripta el valor codificado con la llave privada del emisor. Este valor tiene que ser igual a un valor Hash (Valor obtenido con el mismo algoritmo Hash que utilizó el emisor) calculado sobre el documento que se está validando. Si lo anterior es correcto , la firma fue validada satisfactoriamente.

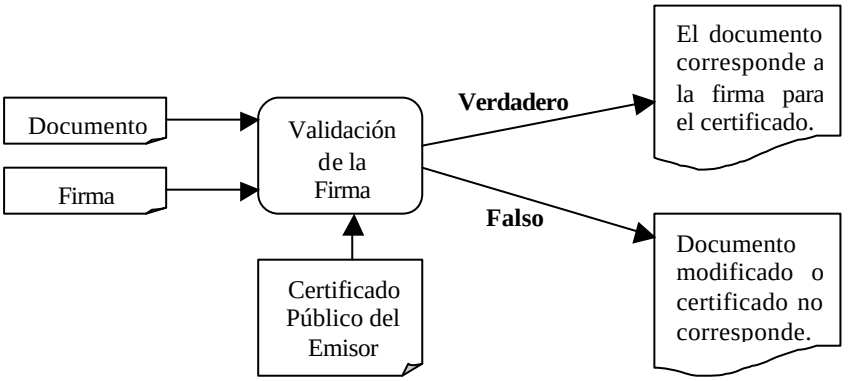
De esta forma, para firmar un documento se requiere una llave privada y la clave del contenedor, mientras que para asegurar que la firma corresponde a una persona, basta con tener acceso al certificado público de la misma persona.

En los siguiente esquemas se explican los procesos de firmado y validación de la firma digital.

Firmado de un documento



Validación de la firma



Documentos XML

La comunicación entre MIDAS y el servidor se basa en documentos XML, por lo que acá se presenta una pequeña introducción a este tipo de documentos.

Un documento en formato XML es la representación de un conjunto de datos y de su estructura en un medio electrónico (archivo de computador). La diferencia principal de este tipo de archivos es que tanto los datos como su estructura se encuentran en un mismo archivo, lo que permite que éstos sean leídos tanto por aplicaciones computacionales como por personas.

Otra ventaja de estos archivos es que se escriben en formato de texto estándar por lo que pueden ser interpretados por personas y por diferentes plataformas de sistemas computacionales.

Dentro de un documento xml, los datos se separan en estructuras delimitadas por marcadores o "tags". Por ejemplo, el siguiente texto puede ser parte de un documento XML:

```
<participantes>
  <exportador>
    <rut>999999</rut>
    <nombres>Nombre del exportador</nombre>
  </exportador>
  <agente>
    <rut>000000</rut>
    <nombres>Nombre del agente</nombre>
  </agente>
</participantes>
```

Como se observa en el ejemplo, cada campo de datos comienza con un nombre de tag y termina con el caracter "/" y luego el mismo nombre de tag como "<rut>000000</rut>".

Además de esos campos finales, en el documento XML pueden incluirse campos compuestos. En el ejemplo anterior, el campo "participantes" se compone de "exportador" y "agente" y cada uno de ellos a su vez se compone de "rut" y "nombres".

Uso de la Firma Digital en MIDAS en comunicaciones hacia y desde el Servidor.

La aplicación MIDAS usa firmas digitales para asegurar la integridad de los documentos que circulan dentro de la organización, en sus flujos de validaciones y para la comunicación (envío final) de estos documentos hacia el servidor. Las notificaciones que el servidor envía a la aplicación cliente también son firmadas.

En esta sección se explica el uso de la firma en la comunicación desde y hacia el servidor.

En los procesos de comunicación entre la aplicación cliente (MIDAS) y el servidor (SNA) los firmantes corresponden a las personas naturales que representan a la organización que envía los documentos y al Servicio Natural de Aduanas en el caso de las Notificaciones. Esto significa que tanto cada organización cliente que envíe documentos hacia el servidor, como el propio servidor deben poseer los pares de llaves públicos y privados.

Para la validación de la firma, es necesario contar con el certificado digital del firmante. Esto significa que los clientes deben enviar (una vez) sus certificados digitales hacia el servidor y deben descargar el certificado digital del servidor. El servidor validará los documentos enviados por el cliente usando los certificados públicos que éste le envió y el

cliente validará las notificaciones recibidas desde el servidor usando el certificado descargado.

La aplicación MIDAS mantiene los documentos en estructuras de directorios o carpetas dependiendo del estado en que estos documentos se encuentran. Los documentos que están listos para ser enviados hacia el servidor se depositan en una carpeta llamada "Salida".

Los documentos pueden tener un comportamiento diferente dependiendo de su tipo. Algunos de ellos son enviados hacia el servidor y no necesitan de ninguna aprobación por personas, por lo que, en el momento en que son enviados y aceptados por el servidor, pueden darse por recibidos y son movidos a la carpeta en el cliente para este efecto.

Existen otros documentos que pueden requerir de algún proceso de aprobación manual. Estos documentos se mantienen en una carpeta del cliente llamada "Esperando Notificación" hasta que se recibe una notificación desde el servidor que indique su cambio de estado y son movidos a las carpetas finales para cada estado.

La aplicación MIDAS contiene un proceso automático y periódico denominado "monitor". Este proceso es el encargado de revisar periódicamente la carpeta de salida hacia el servidor, de firmar y luego de buscar las notificaciones.

Firma en el Proceso de Envío.

Un documento XML manejado por MIDAS contiene varias secciones, delimitadas por tags dentro de su estructura. Estas secciones son:

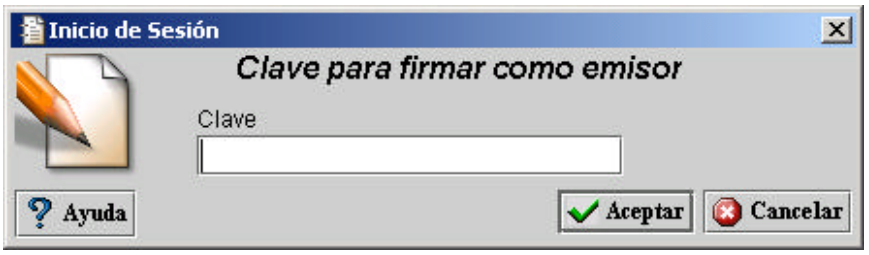
- ?? Área de datos del documento que contiene los datos de cada formulario.
- ?? Área de información de flujos de trabajo y validaciones internas que contiene la información de los diferentes estados por los que ha pasado el documento desde su creación, al interior de la organización emisora.
- ?? Área de control de versiones que mantiene información de todos los cambios que se le han realizado al documento desde su creación, con las firmas digitales de las personas que realizaron estos cambios.
- ?? Área de control de envíos. Un documento puede ser enviado y reenviado varias veces si éste es rechazado por el servidor por problemas de datos (códigos inválidos por ejemplo) o estructura (faltan campos obligatorios). En esta sección se almacena la información de cada envío y las respuestas dadas por el servidor para que se tomen acciones correctivas.

Desde la aplicación MIDAS es posible editar o modificar e imprimir el contenido de datos del documento. El Área de datos es la que contiene la información del formulario. El resto de las áreas son de información de control.

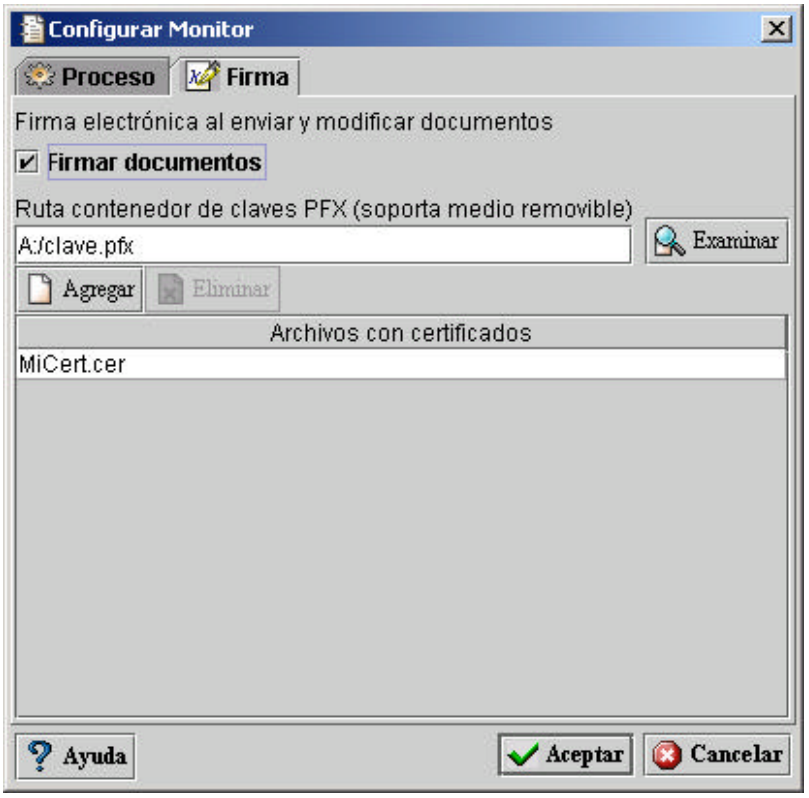
El proceso monitor recorre la carpeta de salida con una cierta frecuencia. Al encontrar un nuevo documento en esta carpeta, significa que debe firmarse y enviarse hacia el servidor.

Hacia el servidor sólo se envía el área de datos; es decir, se envía el equivalente al formulario, con la firma del emisor. Esto significa que el monitor obtiene un documento XML que contiene sólo el área de datos del documento original. Sobre esta área de datos aplica el algoritmo de firmado y obtiene un firma digital, la que es anexada al documento como un nuevo tag "Signature".

Todo lo anterior ocurre solicitando explícitamente la clave del contenedor (necesaria para obtener la llave privada) al usuario administrador encargado del equipo que actúa como monitor (el único PC que envía los documentos hacia el servidor) en la organización.



Usando la configuración del monitor, sólo los usuarios que tengan permisos de administrador pueden indicar la ruta del contenedor con la llave privada. Además debe indicar la ruta de los certificados que se desea luego cargar hacia un servidor.



Desde la ventana de configuración del servidor se debe indicar que se desea verificar la firma del emisor en cada documento enviado, se debe indicar que se desea recibir notificaciones firmadas por el servidor y se deben descargar el certificado X509 (certificado digital) del servidor para poder comprobar las firmas que el servidor envíe en sus notificaciones.

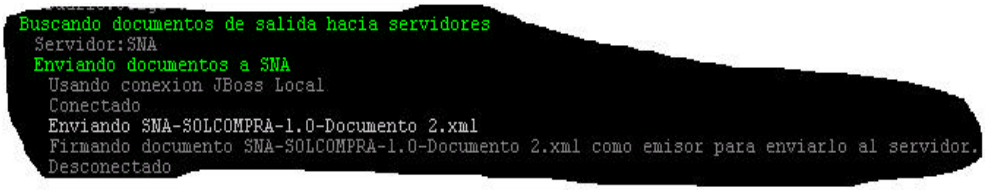
Usando esta información de configuración, el proceso de envío y recepción funciona de la siguiente forma:

1. Al iniciarse la aplicación en el PC que se indique como monitor, se solicita la clave para abrir el contenedor y se debe insertar el medio removible que contiene al archivo con este contenedor.
2. El proceso monitor encuentra un nuevo documento en la bandeja de salida para ser enviado al servidor.
    a. Se obtiene el área de datos del documento
    b. Se obtiene la firma digital de estos datos usando la clave y la ruta hacia el contenedor de la llave privada.
    c. Se anexa la firma digital al documento XML como un nuevo tag identificado como sigue:

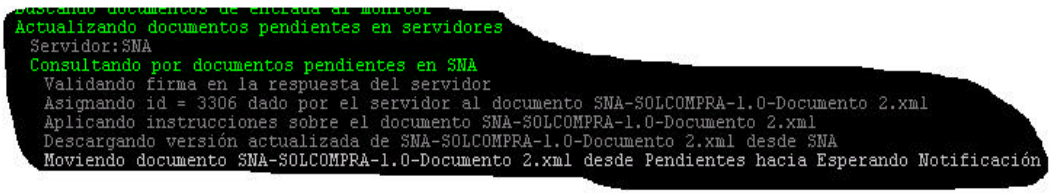
```
<Documento>
  <numero-referencia>BL456</numero-referencia>
  <fecha-emision>2002-09-06</fecha-emision>
  {Otros datos del formulario}
```

```
  <Signature>
      ....
  </Signature >
</Documento>
```

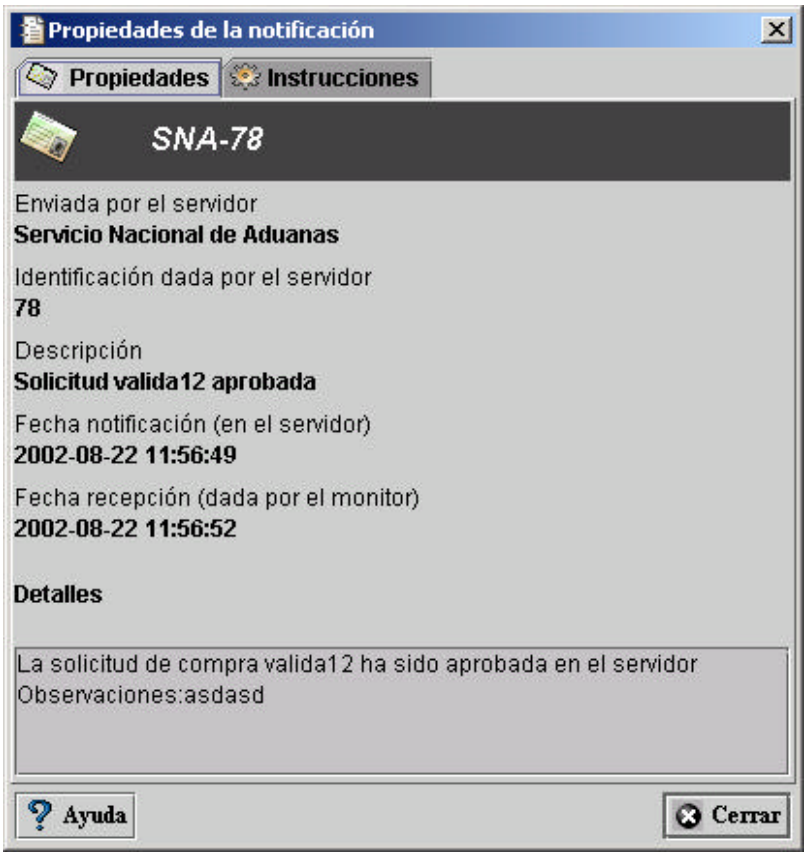
d. El proceso monitor se conecta al sistema de mensajería del servidor y envía el documento firmado. Este documento se mueve (en el cliente) hacia una carpeta de "Pendientes" que contiene los documentos que se han enviado, pero que aún no han sido notificados como recibidos por el servidor.

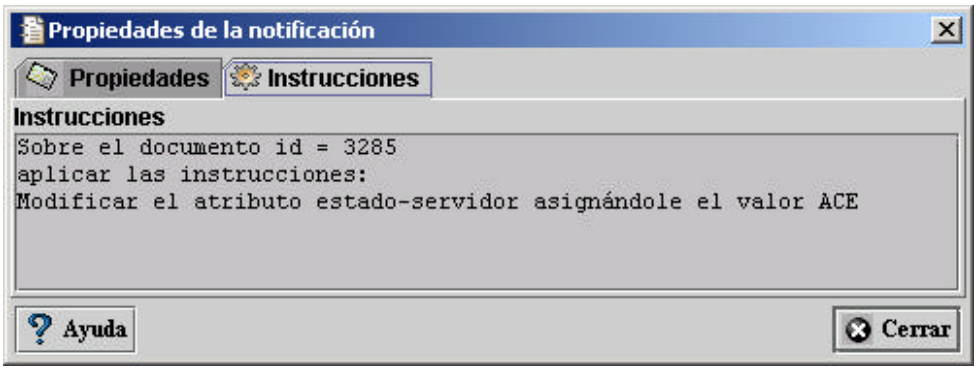


3. El servidor recibe el documento y se asegura que éste se encuentre firmado. Valida la firma de el área de datos usando el tag "Signature" del emisor y los certificados que el emisor antes cargó en el servidor. Se almacena el resultado de esta validación para ser enviada al cliente la próxima vez que éste se conecte.
4. Durante la siguiente ejecución del proceso monitor se consulta al servidor por el estado de cada uno de los documentos que se tienen en "Pendientes". El servidor responde al cliente con una notificación. Esta notificación es otro documento XML que contiene un número único asignado por el servidor al documento original y puede contener algunas instrucciones como cambio de estado del documento o solicitarle al cliente que descargue una nueva versión del documento desde el servidor. Estas notificaciones son firmadas y la firma se valida en el cliente antes de aplicar cualquier instrucción sobre el documento.



a. Si el tipo de documento indica que al aceptarse el envío se da por recibido, el proceso termina moviendo el documento a una carpeta de terminados.
b. Si el tipo de documento define que se debe esperar por alguna otra notificación de cambio de estado, el documento de mantiene en una carpeta de "Esperando Notificación" hasta que se reciba una nueva notificación firmada con instrucciones de cambio de estado y con un aviso a los responsables indicando la aceptación o rechazo del documento.





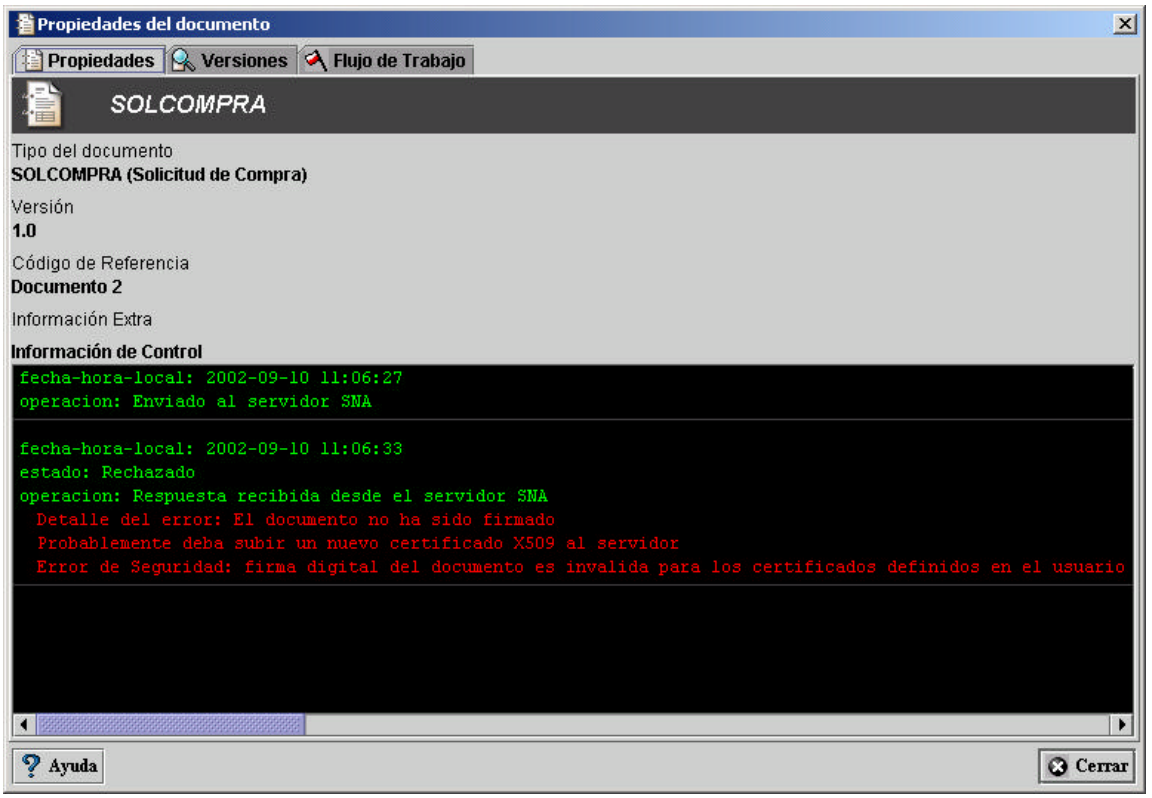
La descripción anterior del proceso supone que todas las firmas son válidas. Si alguna de las firmas es inválida, ya sea porque los datos fueron modificados o la firma no corresponde a los certificados declarados (cargados en el servidor) por el emisor, el proceso se aborta y se generan mensajes de error.

Los siguientes ejemplo muestran cómo se comportaría el sistema al ocurrir excepciones relativas a la validación de las firmas.

Para el primer ejemplo, se indicará en la configuración que se debe validar la firma en cada documento enviado, pero se enviará un documento no firmado hacia el servidor:

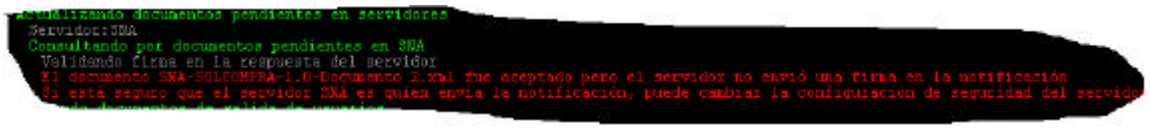
Al consultar por el estado del documento pendiente, el proceso monitor obtiene la siguiente respuesta.

Las propiedades del documento muestran la siguiente información.



Si el documento se modifica entre el momento en que se firma y el momento en que se envía, se obtendría un error similar. Cabe destacar que esto es altamente improbable si se usa la aplicación MIDAS para el envío de los documentos, ya que ambas operaciones (firmado y envío) ocurren como parte de un mismo proceso y dentro de la memoria del computador.

Para el siguiente ejemplo se ha configurado el servidor para que no firme las notificaciones o respuestas hacia el cliente. El cliente se mantiene configurado para exigir respuestas firmadas.



En este caso, la respuesta recibida no está firmada, por lo que es rechazada y marcada como un error.

Lo mismo ocurre en el caso de las notificaciones (con instrucciones o con información de texto para el emisor). Si una notificación no contiene la firma o los datos que se reciben no corresponden a la firma, es rechazada y se da aviso del error.

Resumen final

El proceso de firma y validaciones en la transmisión de mensajes entre el Módulo para la Integración de Documentos y Acceso a los Sistemas y el servidor SNA asegura la integridad de los datos y el origen del emisor de los mensajes.

Si se considera además que todos los mensajes viajan por canales seguros a través de internet (canales de comunicación encriptados), se restringe al máximo la posibilidad de intervención sobre la información que se envía, de acuerdo a las últimas tecnologías de firma digital y encriptación de datos.

Toda la información relativa al envío y recepción de documentos y al envío de notificaciones se firma en el lugar en que se emite y se valida en el lugar en que se recibe.