(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 769**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.02.2010 E 10710537 (1)**

(97) Fecha y número de publicación de la concesión europea: **12.06.2013 EP 2532134**

(54) Título: **Método para el procesamiento de un mensaje de SOAP dentro de una red y una red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.10.2013

(73) Titular/es:

NEC EUROPE LTD. (100.0%)
Kurfürsten-Anlage 36
69115 Heidelberg, DE

(72) Inventor/es:

GRUSCHKA, NILS y
LO IACONO, LUIGI

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Método para el procesamiento de un mensaje de SOAP dentro de una red y una red.

La presente invención se refiere a un método para procesar un mensaje de SOAP (Protocolo Simple de Acceso a Objetos) dentro de una red, en especial una red de IP (Protocolo de Internet), en el que el mensaje de SOAP basado en XML (Lenguaje de Marcación Extendida) está comprendiendo un fragmento con un contenido binario, en el que el contenido binario se moverá a un elemento adjunto de MTOM (Mecanismo de Optimización de Transmisión de Mensajes) del mensaje de SOAP con una referencia restante al contenido binario dentro del mensaje de SOAP y en el que el elemento adjunto se firmará y/o cifrará por un proceso de firma y de cifrado, respectivamente. Además, la presente invención se refiere a una red, en especial una red de IP (Protocolo de Internet), en la que se procesará un mensaje de SOAP (Protocolo Simple de Acceso a Objetos) basado en XML (Lenguaje de Marcación Extendida), en la que el mensaje de SOAP está comprendiendo un fragmento con un contenido binario, en la que el contenido binario se moverá a un elemento adjunto de MTOM (Mecanismo de Optimización de Transmisión de Mensajes) del mensaje de SOAP con una referencia restante al contenido binario dentro del mensaje de SOAP y en el que el elemento adjunto estará firmado y/o cifrado por un proceso de firma y de cifrado, respectivamente.

El documento WO 2005/030261 A1 desvela un método para el procesamiento de un mensaje de SOAP con todas las características de la parte de preámbulo de la reivindicación 1, en el que se coloca una firma digital en un elemento adjunto adicional al final de una secuencia.

Además, el documento de Xiaoling Lui y otros: "*A novel SOAP Attachment - Oriented Security Model*", *7th International Symposium on Software Reliability Engineering*, 2006 (ISSRE'06) desvela un método en el que una entidad intermedia reconstruye el mensaje de SOAP y valida los elementos adjuntos en un paso único, pero tiene que esperar a que se reciban todos los elementos adjuntos para realizar la validación de seguridad.

Es un hecho bien conocido, que el procesamiento de mensajes XML consume muchos recursos en comparación con los formatos de mensajes binarios. Esta propiedad se ve perjudicada si el mensaje o partes del menaje se firman y se cifran usando medios de seguridad de XML (firma de XML, cifrado de XML). Lo que se indica anteriormente, por supuesto, también es cierto para los mensajes de SOAP ya que SOAP está basado en XML y los medios de seguridad usados - WS-Security (Seguridad de Servicios Web) - se basan en la seguridad de XML. Como consecuencia, los desarrolladores de la estructura del Servicio Web han estado trabajando desde algunos años en la optimización del flujo de procesamiento de mensajes. Un enfoque prometedor es el paradigma de procesamiento de transmisión por secuencias. Para mensajes no seguros ya está adoptado, por ejemplo en la estructura del Servicio Web Apache Axis2 y para mensajes seguros son visibles los primeros resultados.

Documentos adicionales que dan información acerca de la tecnología actual, en especial los procedimientos de cifrado y de firma de XML y el procesamiento de transmisión por secuencias de los mensajes de acuerdo son los que siguen:

1. Bartel, Mark, Boyer, John, Fox, Barb, LaMacchia, Brian y Simon, Ed: *XML Signature Syntax and Processing,* Recomendación de W3C, 2002.

2. Imamura, Takeshi, Dillaway, Blair y Simon, Ed: *XML Encryption Syntax and Processing*, Recomendación de W3C, 2002.

3. Gudgin, Martin, Mendelsohn, Noah, Nottingham, Mark y Ruellan, Herve: *SOAP Message Transmission Optimization Mechanism*, Recomendación de W3C, 2005.

4. Gruschka, Nils, Luttenberger, Norbert y Herkenhöner, Ralph: *Event-based SOAP Message Validation for WS-Security Policy-enriched Web Services*, *Proceedings of the 2006 International Conference on Semantic Web & Web Services*, 2006.

5. Govindaraju, Madhusudhan, Slominski, Aleksander, Chiu, Kenneth, Liu, Pu, van Engelen, Robert y Lewis, Michael J.: *Toward Characterizing the Performance of SOAP Toolkits*, *Proceedings of the Fifth IEEE/ACM International Workshop on Grid Computing* (GRID'04), *IEEE Computer Society*, 365-372, 2004.

6. Lu, Wei, Chiu, Kenneth, Slominski, Aleksander y Gannon, Dennis: *A Streaming Validation Model for SOAP Digital Signature*, *14th IEEE International Symposium on High Performance Distributed Computing* (HPDC- 14), 2005.

7. Imamura, Takeshi, Clark, Andy y Maruyama, Hiroshi: *A stream-based implementation of XML Encryption*, XMLSEC '02: *Proceedings of the 2002 ACM workshop on XML security*, ACM Press, 11-17, 2002.

El problema básico de procesamiento de mensajes de SOAP es su elevado consumo de recursos. El consumo de recursos es incluso mayor cuando partes del mensaje están cifradas o firmadas. El procesamiento de mensajes de transmisión por secuencias es un método para reducir el consumo de recursos. Sin embargo, los elementos adjuntos de MTOM seguros inhiben el procesamiento de transmisión por secuencias de una pasada con respecto a

la secuencia de red.

Más precisamente, el procesamiento de mensajes de transmisión por secuencias ya no es factible, si el mensaje de SOAP: (1) usa elementos adjuntos de MTOM y (2) uno o más de estos elementos adjuntos se han hecho seguros usando WS-Security. La razón se explica en lo siguiente. La parte binaria del documento de SOAP que va a transportarse como un elemento adjunto se sustituye por una referencia de MTOM. Se envía sobre la red en primer lugar este documento de SOAP y, a continuación, la parte binaria como un elemento adjunto de MTOM. Sin embargo, el elemento adjunto se incorpora virtualmente dentro del mensaje de SOAP en la ubicación de referencia. Para varias operaciones típicas sobre el documento de SOAP - como extraer o mover subárboles de documentos - se puede hacer caso omiso de esta propiedad. Sin embargo, para algunas otras operaciones - incluyendo el cálculo del valor de función de troceo para la verificación de la firma o descifrar contenido cifrado - el elemento adjunto se debe leer completamente en el momento del procesamiento de la referencia dentro del mensaje de SOAP. Por lo tanto, en este caso se rompe el procesamiento de transmisión por secuencias de una pasada del mensaje.

Es un objeto de la presente invención mejorar y desarrollar adicionalmente un método para el procesamiento de un mensaje de SOAP dentro de una red y una red conforme para permitir un procesamiento de transmisión por secuencias de los mensajes de SOAP con elementos adjuntos de MTOM firmados y/o cifrados de una forma simple.

De acuerdo con la invención, el objeto mencionado anteriormente se logra por un método que comprende las características de la reivindicación 1 y una red que comprende las características de la reivindicación 13.

De acuerdo con la reivindicación 1, el método se caracteriza por que durante el proceso de firma además de la aplicación de función de troceo del propio fragmento firmado se aplicará una función de troceo al mismo fragmento excluyendo el contenido binario y/o durante el proceso de cifrado además del cifrado del propio fragmento se cifrará el fragmento incluyendo solo la referencia al contenido binario en lugar del contenido binario.

De acuerdo con la reivindicación 13, la red se caracteriza por unos medios de aplicación de función de troceo, que se adaptan de modo que durante el proceso de firma además de la aplicación de función de troceo del propio fragmento firmado se puede aplicar una función de troceo del mismo fragmento excluyendo el contenido binario y/o por unos medios de cifrado, que se adaptan de modo que durante el proceso de cifrado además del cifrado del propio fragmento se puede cifrar el fragmento incluyendo solo la referencia al contenido binario en lugar del contenido binario.

De acuerdo con la invención, se ha reconocido que es posible permitir un procesamiento de transmisión por secuencias de los mensajes de SOAP con elementos adjuntos de MTOM firmados y/o cifrados simplemente añadiendo información adicional acerca del elemento adjunto firmado y/o cifrado al mensaje de SOAP saliente. En concreto, durante el proceso de firma además de la aplicación de función de troceo del propio fragmento firmado se aplicará una función de troceo del mismo fragmento excluyendo el contenido binario y se puede añadir al mensaje de SOAP de un modo adecuado. Por consiguiente, durante el proceso de cifrado además del cifrado del propio fragmento se cifrará el fragmento incluyendo solo la referencia al contenido binario - en lugar del contenido binario. Esta información adicional también se puede añadir al mensaje de SOAP saliente. Durante el procesamiento de los mensajes de SOAP en un lado de servidor será posible un procesamiento de transmisión por secuencias de una pasada de los mensajes de SOAP con elementos adjuntos de MTOM firmados y/o cifrados en función de las partes adicionales añadidas al mensaje de SOAP saliente.

Preferentemente, durante el proceso de firma y/o de cifrado el contenido binario podría estar presente dentro del fragmento de una forma codificada en texto, codificada preferentemente en base 64. En base a una forma codificada en texto de este tipo, se pueden usar las tecnologías de firma y cifrado habituales durante el proceso de firma y/o de cifrado.

Durante el método inventivo y, en especial, durante el proceso de firma basado en el fragmento al que adicionalmente se ha aplicado función de troceo - excluyendo el contenido binario - se podría crear un bloque adicional para su uso dentro de un protocolo de transporte. Preferentemente, un bloque adicional de este tipo podría ser un bloque de transformación que se podría añadir a un elemento de transformación de la firma respectiva. En base a las etapas mencionadas anteriormente, es posible una extensión simple a los mensajes de SOAP habituales para permitir un procesamiento de transmisión por secuencias de una pasada de los mensajes de SOAP.

Con respecto a una realización preferida adicional de la invención basada en el fragmento cifrado adicionalmente - incluyendo solo la referencia al contenido binario - se podría crear una propiedad de cifrado para su uso dentro de un protocolo de transporte. Una propiedad de cifrado de este tipo podría añadirse simplemente a un bloque de cifrado para una transmisión por secuencias de una pasada en el lado de servidor para el procesamiento de mensajes.

Preferentemente, la propiedad de cifrado podría estar presente de una forma codificada en texto, codificada preferentemente en base 64. De este modo, las tecnologías de cifrado usuales se podrían usar durante el método inventivo.

Con respecto a un método muy simple y efectivo, la referencia al contenido binario podría ser una referencia de XOP

(Empaquetamiento Optimizado binario de XML). Una referencia de XOP de este tipo puede proporcionar la posibilidad de sacar el contenido binario de un mensaje con solo una parte de referencia restante dentro del mensaje original.

Con respecto a un procesamiento de transmisión por secuencias de una pasada muy efectivo, el mensaje de SOAP se podría serializar para un procesamiento de transmisión por secuencias de una pasada de lado de servidor.

Con respecto a un procesamiento muy efectivo del mensaje de SOAP durante el procesamiento de lado de servidor, cada uno de los cálculos de los valores de función de troceo se podría realizar en paralelo de un modo de transmisión por secuencias de una pasada.

Para proporcionar un método muy simple y fiable se podría usar WS-Security (Seguridad de Servicios Web) para los procesos de firma y/o de cifrado. De este modo, es posible el uso de las tecnologías conocidas de firma y/o de cifrado para simplificar el método anterior.

El tipo de contenido binario dentro del fragmento no se limita a aplicación específica alguna. Dentro de una realización preferida, el contenido binario podría ser una foto, una imagen médica o números binarios de software.

La presente invención introduce una extensión a las actuales especificaciones de seguridad de Servicios Web y métodos de procesamiento de mensajes para superar el problema mencionado anteriormente y para posibilitar, de este modo, el procesamiento de transmisión por secuencias de los mensajes de SOAP con elementos adjuntos de MTOM cifrados y/o firmados. Para ser más específicos, esta invención define extensiones para las especificaciones de seguridad de los Servicios Web de Firma de XML y de Cifrado de XML. Estas extensiones se añaden por un cliente de Servicios Web - que soporta los mecanismos definidos en la presente invención - al mensaje de SOAP saliente y contienen información adicional acerca del elemento adjunto firmado o cifrado. Un servidor de Servicios Web - que soporta los mecanismos definidos en la presente invención - puede usar estas extensiones para procesar eficientemente este mensaje de un modo de transmisión por secuencias de una pasada. Esto conduce a un mayor rendimiento y a un consumo reducido de recursos en el lado de servidor. Sin embargo, debido a que no se cambia el formato de mensajes convencional, la firma y el cifrado dentro del mensaje de SOAP también se puede procesar aún por servidores de Servicios Web que no soporten los mecanismos definidos en la presente invención.

La presente invención está proporcionando una extensión para la seguridad de SOAP en conjunción con elementos adjuntos de MTOM. Se proporciona un procesamiento de transmisión por secuencias de lado de servidor de una pasada de la totalidad del mensaje de SOAP, incluyendo elementos adjuntos. El resultado es un mayor rendimiento y un consumo reducido de recursos para los servidores de Servicios Web. Se da una compatibilidad total hacia atrás con las normas y estructuras actuales.

Existen varias formas de las que diseñar y desarrollar adicionalmente la enseñanza de la presente invención de un modo ventajoso. Para este fin, ha de hacerse referencia, por una parte, a las reivindicaciones de patente subordinadas a la reivindicación de patente 1 y, por otra parte, a la siguiente explicación de los ejemplos preferidos de realizaciones de la invención, ilustrados por los dibujos. En conexión con la explicación de las realizaciones preferidas de la invención con la ayuda de los dibujos, se explicarán realizaciones generalmente preferidas y desarrollos adicionales de la enseñanza. En los dibujos

la Figura 1 está ilustrando un formato y serialización convencionales de los mensajes de SOAP de MTOM,

la Figura 2 está ilustrando un formato, procesamiento y serialización convencionales de mensajes de SOAP de MTOM firmados,

la Figura 3 está ilustrando un formato, procesamiento y serialización convencionales de mensajes de SOAP de MTOM cifrados,

la Figura 4 está ilustrando una realización para la creación de mensajes de SOAP de MTOM firmados de acuerdo con la invención,

la Figura 5 está ilustrando una realización para la creación de mensajes de SOAP de MTOM cifrados de acuerdo con la invención,

la Figura 6 está ilustrando una realización para el procesamiento de lado de servidor de mensajes de SOAP de MTOM firmados de acuerdo con la invención.

la Figura 7 está ilustrando una realización para el procesamiento de lado de servidor de mensajes de SOAP de MTOM cifrados de acuerdo con la invención.

Las siguientes Figuras 1 a 7 explican la invención y sus realizaciones. Las Figuras 1 a 3 muestran el enfoque convencional para la creación de mensajes de MTOM seguros y cifrados. Las Figuras 4 a 7 muestran el método de la presente invención.

La Figura 1 está ilustrando un formato y serialización convencionales de los mensajes de SOAP de MTOM. Esta

Figura 1 ilustra cómo se crean los elementos adjuntos de MTOM. En el lado izquierdo, se puede ver un fragmento de mensaje de SOAP con contenido binario - en este caso: una foto. Debido a que XML es un formato de texto, el contenido binario solo se puede transportar de una forma codificada en texto. La forma más común para esto es la codificación en base 64. Este tipo de manejo de contenido binario - especialmente grande - crea algunos problemas. Principalmente, el uso de base 64 aumenta el consumo de espacio en memoria y sobre la red (33 %). Adicionalmente, el manejo de un gran documento de SOAP es más difícil y consume más recursos. Para superar estos problemas, en el pasado se han publicado varias posibilidades para eliminar estas “partes de documento externas” lógicas del mensaje de SOAP y transportarlas como un elemento adjunto. De entre estos, MTOM se considera como el mejor enfoque ya que elimina algunos inconvenientes de, por ejemplo, SwA (SOAP con Elementos adjuntos).

Como se muestra en la Figura 1, MTOM usa el llamado conjunto de información de XOP para almacenar mensajes en la memoria. Mediante este, los datos binarios - en este caso: una foto - se mantienen en su forma original fuera del mensaje de SOAP que solamente incluye una referencia (<xop:Include>) al fichero binario.

Finalmente, en el lado derecho de la figura se puede ver cómo el conjunto de información de XOP se transporta sobre la red: la parte de XML serializada y la parte binaria se transportan como bloques de MIME (Extensiones de Correo Electrónico de Internet Multipropósito) separados dentro del protocolo de transporte, típicamente HTTP (Protocolo de Transferencia de HiperTexto). De este modo, la parte binaria se puede transportar tal y como está - sin codificación - como un elemento adjunto al mensaje de SOAP.

La Figura 2 está ilustrando un formato, procesamiento y serialización convencionales de los mensajes de SOAP de MTOM firmados. La Figura 2 muestra el proceso de creación de firma para un mensaje de SOAP con MTOM habilitado. Una propiedad importante del conjunto de información de XOP es que la referencia <xop:Include> es una referencia “por valor”, es decir, todas las operaciones deben tratar los documentos de XML así como el contenido binario que se incorpora dentro del documento. Para varias operaciones, por ejemplo, el movimiento del nodo <m:photo>, no se necesita considerar esto, ya que el funcionamiento es equivalente sobre el conjunto de información de XOP o sobre el conjunto de información original. Sin embargo, para una operación de firma que requiere leer y aplicar una función de troceo a la totalidad del contenido de un nodo firmado, se debe cumplir con esta propiedad.

De este modo, como se muestra en la Figura 2 antes de firmar un nodo que incluye un elemento adjunto de MTOM, el elemento adjunto se debe incorporar al documento de XML, lo que realmente reconstruye el conjunto de información original. A continuación, el nodo se puede firmar, incluyendo la aplicación de función de troceo al elemento adjunto binario codificado en base 64. Después del cálculo de la firma, se puede restaurar la parte de XOP - lo que no se muestra en la Figura 2 - y la parte binaria se puede transportar de nuevo como un elemento adjunto.

Si una serialización de este tipo se procesa en el lado de servidor, esto no se puede hacer de un modo de transmisión por secuencias de una pasada. Después de procesar el nodo <m:photo>, el cálculo de función de troceo se debe pausar hasta que se haya recibido completamente el elemento adjunto de modo que se pueda realizar el cálculo de función de troceo, lo que causa un comportamiento de bloqueo para el procesamiento de SOAP.

La Figura 3 está ilustrando un formato, procesamiento y serialización convencionales de mensajes de SOAP de MTOM cifrados. Esta figura ilustra el modo de cifrar un fragmento de mensaje de SOAP que contiene un elemento adjunto de MTOM. De nuevo, antes de aplicar la operación de cifrado, se debe volver a incorporar el elemento adjunto - y codificarse en base 64 - dentro del documento de XML. Después del cifrado, el bloque de cifrado de XML sustituye al bloque cifrado, en el ejemplo anterior el elemento <:m:photo>. Este bloque de cifrado incluye de nuevo un nodo de contenido binario - codificado en base 64: el contenido del elemento <xenc:CipherData>. Este contenido binario se puede extraer a continuación del documento de XML y serializarse como un elemento adjunto de MTOM. Debe observarse que, - en contraste con la creación de firma - el elemento adjunto del mensaje cifrado no es el mismo que en el mensaje sin cifrar.

Debido a que las partes del documento de XML sin cifrar - en este caso: el contenedor de <m:photo> - se han movido por el proceso de cifrado al elemento adjunto, de nuevo el procesamiento, es decir el descifrado, en el lado de servidor no se puede realizar de un modo de transmisión por secuencias de una pasada.

La Figura 4 está ilustrando una realización de un método para la creación de mensajes de SOAP de MTOM firmados de acuerdo con la invención. Esta Figura 4 muestra el enfoque inventivo para la creación de una firma de XML para un fragmento que contiene un elemento adjunto de MTOM. El mensaje resultante permite un procesamiento de transmisión por secuencias de una pasada en el lado de servidor, véase la Figura 6 a continuación. Los detalles del proceso de firma son como sigue: además de la aplicación de función de troceo del propio fragmento firmado - <m:photo> en el ejemplo anterior - se aplica una función de troceo al mismo fragmento - excluyendo el contenido binario. Por lo tanto, se añade el siguiente bloque de transformación al elemento <ds:Transforms> de la firma respectiva:

<ds:Transform Algorithm=“http://www.w3.org/2002/06/xmldsig-filter2”>

  <dsf:XPath Filter=“intersect”>

```
  xpath-of-signed-element
 </dsf:XPath>
 <dsf:XPath Filter="subtract">
  xpath-of-wrapping-element/*
 </dsf:XPath>
</ds:Transform>
```

Prefijo	Espacio de nombres
dsf	http://www.w3.org/2002/06/xmldsig-filter2
ds	http://www.w3.org/2000/09/xmldsig#

Los valores xpath-of-signed-element (xpath del elemento firmado) y xpath-of-wrapping-element (xpath del elemento contenedor) se deben sustituir por unas expresiones XPath que hacen referencia a los elementos que han de firmarse y el elemento primario del contenido binario ("elemento contenedor"). En el ejemplo usado en la Figura 4, ambas expresiones son //m:photo.

La Figura 5 está ilustrando una realización de un método para la creación de mensajes de SOAP de MTOM cifrados de acuerdo con la invención. Esta Figura 5 muestra el enfoque inventivo para cifrar un fragmento que contiene un elemento adjunto de MTOM. El mensaje resultante permite un procesamiento de transmisión por secuencias de una pasada en el lado de servidor, véase la Figura 7 a continuación. Los detalles del proceso de cifrado son como sigue: se cifra, además del fragmento procedente del "conjunto de información original" - en el ejemplo anterior el elemento <m:photo> incluyendo el contenido binario -, el mismo fragmento del "conjunto de información de XOP" - en el ejemplo anterior el elemento <m:photo> incluyendo la referencia XOP. El resultado de la segunda operación de cifrado se añade - codificado en base 64 - como una propiedad de cifrado al bloque de cifrado. Para ser más precisos, se añade el siguiente elemento al bloque <xenc:EncryptionProperties>:

```
<xenc: EncryptionProperty>
 <nec: EncrytedBinaryWrapper>
  encrypted-xop-infoset-fragment
 </nec:EncrytedBinaryWrapper>
</xenc: EncryptionProperty>
```

Prefijo	Espacio de nombres
xenc	http://www.w3.org/2001/04/xmlenc#
Nec	http://www.w3.neclab.eu/2010/10/secmtom

Finalmente, mientras que se serializa el mensaje de SOAP, el contenido de <xenc:CipherValue> se extrae como un elemento adjunto de MTOM, mientras que el contenido de <nec:EncrytedBinaryWrapper> permanece dentro del documento de XML. Debido a que los elementos adjuntos se prevén para grandes elementos adjuntos binarios y se supone que el contenedor es bastante pequeño, esto es conforme a los principios de los elementos adjuntos.

La Figura 6 está ilustrando una realización para el procesamiento de lado de servidor de los mensajes de SOAP de MTOM firmados de acuerdo con la invención. Esta Figura 6 muestra el procesamiento de lado de servidor propuesto de los mensajes firmados creados usando el enfoque que se presenta anteriormente, véase la Figura 4. Se puede ver que los cálculos de los dos valores de función de troceo - dig1 y dig2 - se realizan en paralelo, cada uno de un modo de transmisión por secuencias de una pasada. Durante la transmisión por secuencias de una pasada se realizará el almacenamiento en memoria caché de los elementos contenedores de cierre - en el ejemplo anterior el

elemento </m:photo>. Sin embargo, en base a la suposición de que el elemento contenedor es bastante pequeño, esto implica solo un pequeño consumo de memoria.

Se puede ver que, después de leer el último elemento de mensaje de SOAP, se puede verificar la versión del conjunto de información de XOP del mensaje.

La Figura está ilustrando una realización para el procesamiento de lado de servidor de los mensajes de SOAP de MTOM cifrados. Esta Figura 7 muestra el procesamiento de lado de servidor propuesto de los mensajes cifrados creados usando el enfoque que se presenta anteriormente, véase la Figura 5. Se puede ver que los elementos cifrados del conjunto de información de XOP se crean y se retransmiten a la aplicación del servicio de un modo de transmisión por secuencias. Durante la transmisión por secuencias de una pasada se realizará el almacenamiento en memoria caché de los elementos contenedores, lo que es necesario para eliminar el contenedor durante el descifrado del elemento adjunto.

Como se puede ver, después de la lectura del último elemento de mensaje de SOAP, la versión del conjunto de información de XOP del mensaje se descifra completamente.

Los enfoques inventivos presentados anteriormente para la firma y el cifrado, por supuesto, se pueden combinar de forma ininterrumpida para proporcionar diversas aplicaciones. De este modo, se soportan completamente mecanismos de seguridad anidados.

Las ventajas de la presente invención son: en primer lugar, el método posibilita el procesamiento de mensajes de lado de servidor de un modo de transmisión por secuencias totalmente, lo que en general conduce a una gran reducción de recursos en comparación con los métodos basados en documentos. Adicionalmente, debido a que el mensaje de SOAP se descifra y se verifica completamente después de leer el último elemento de SOAP - es decir, antes de leer el elemento adjunto - el método posibilita un “preprocesamiento temprano” para comenzar, por ejemplo, tareas de dispositivo, que no requieren el elemento adjunto, o posibilita la detección y el rechazo de las llamadas de mensajes inválidos sin malgastar recursos en el procesamiento de elementos adjuntos.

La presente invención está proporcionando una extensión del formato de mensajes de SOAP y el procesamiento en el contexto de elementos adjuntos de MTOM seguros. Este uso novedoso del formato de los mensajes de SOAP / MTOM seguros está proporcionando un procesamiento de transmisión por secuencias de una pasada de lado de servidor de mensajes de SOAP de MTOM firmados y/o cifrados.

El resultado del método inventivo es una reducción del consumo de memoria y de los costes de computación para el procesamiento de mensajes de lado de servidor (*green computing*, tecnologías verdes). El método inventivo está proporcionando una compatibilidad total con las normas implicadas y con las estructuras de Servicio Web existentes.

Muchas modificaciones y otras realizaciones de la invención expuesta en el presente documento vendrán a la mente de un experto en la materia a la que se refiere la invención que tenga el beneficio de las enseñanzas presentadas en la descripción anterior y los dibujos asociados. Por lo tanto, ha de entenderse que la invención no ha de limitarse a las realizaciones específicas desveladas y que se pretende que las modificaciones y otras realizaciones estén incluidas dentro del alcance de las reivindicaciones adjuntas. Aunque se emplean términos específicos en el presente documento, se usan solo en un sentido genérico y descriptivo y no con fines de limitación.

REIVINDICACIONES

1. Un método para el procesamiento de un mensaje de SOAP (Protocolo Simple de Acceso a Objetos) dentro de una red, en especial una red de IP (Protocolo de Internet), en el que el mensaje de SOAP basado en XML (Lenguaje de Marcación Extendida) está comprendiendo un fragmento con un contenido binario, en el que el contenido binario se moverá a un elemento adjunto de MTOM (Mecanismo de Optimización de Transmisión de Mensajes) del mensaje de SOAP con una referencia restante al contenido binario dentro del mensaje de SOAP y en el que el elemento adjunto se firmará y/o se cifrará por un proceso de firma y de cifrado, respectivamente,

caracterizado por que durante el proceso de firma además de la aplicación de función de troceo del propio fragmento firmado, se aplicará una función de troceo del mismo fragmento excluyendo el contenido binario y/o durante el proceso de cifrado además del cifrado del propio fragmento se cifrará el fragmento incluyendo solo la referencia al contenido binario en lugar del contenido binario.

2. Un método de acuerdo con la reivindicación 1, en el que durante el proceso de firma y/o de cifrado está presente el contenido binario dentro del fragmento de una forma codificada en texto, codificada preferentemente en base 64.

3. Un método de acuerdo con la reivindicación 1 o 2, en el que se creará un bloque adicional en base al fragmento al que adicionalmente se ha aplicado función de troceo excluyendo el contenido binario para su uso dentro de un protocolo de transporte.

4. Un método de acuerdo con la reivindicación 3, en el que el bloque adicional es un bloque de transformación que se añadirá a un elemento de transformación de la firma respectiva.

5. Un método de acuerdo con una de las reivindicaciones 1 a 4, en el que en base al fragmento cifrado adicionalmente que incluye solo la referencia al contenido binario se creará una propiedad de cifrado para su uso dentro de un protocolo de transporte.

6. Un método de acuerdo con la reivindicación 5, en el que la propiedad de cifrado se añadirá a un bloque de cifrado.

7. Un método de acuerdo con la reivindicación 5 o 6, en el que la propiedad de cifrado está presente de una forma codificada en texto, codificada preferentemente en base 64.

8. Un método de acuerdo con una de las reivindicaciones 1 a 7, en el que la referencia al contenido binario es una referencia de XOP (Empaquetamiento Optimizado binario de XML).

9. Un método de acuerdo con una de las reivindicaciones 1 a 8, en el que el mensaje de SOAP se serializará para un procesamiento de transmisión por secuencias de una pasada de lado de servidor.

10. Un método de acuerdo con la reivindicación 9, en el que durante el procesamiento de lado de servidor los cálculos de los valores de función de troceo se realizarán en paralelo.

11. Un método de acuerdo con una de las reivindicaciones 1 a 10, en el que se usará la función WS-Security (Seguridad de Servicios Web) para los procesos de firma y/o de cifrado.

12. Un método de acuerdo con una de las reivindicaciones 1 a 11, en el que el contenido binario es una foto, una imagen médica o números binarios de software.

13. Una red, en especial una red de IP (Protocolo de Internet), que comprende un medio para el procesamiento de un mensaje de SOAP (Protocolo Simple de Acceso a Objetos) basado en XML (Lenguaje de Marcación Extendida), en el que el mensaje de SOAP comprende un fragmento con un contenido binario, en el que dichos medios de procesamiento están adaptados para mover el contenido binario a un elemento adjunto de MTOM (Mecanismo de Optimización de Transmisión de Mensajes) del mensaje de SOAP con una referencia restante al contenido binario dentro del mensaje de SOAP y para firmar y/o cifrar el elemento adjunto por un proceso de firma y de cifrado, respectivamente,

caracterizada por unos medios de aplicación de función de troceo, que están adaptados para generar, durante el proceso de firma además de un valor de función de troceo del propio fragmento firmado, un valor de función de troceo del mismo fragmento excluyendo el contenido binario y/o **por** unos medios de cifrado que están adaptados para cifrar durante el proceso de cifrado el propio fragmento, y para cifrar el fragmento incluyendo solo la referencia al contenido binario en lugar del contenido binario.

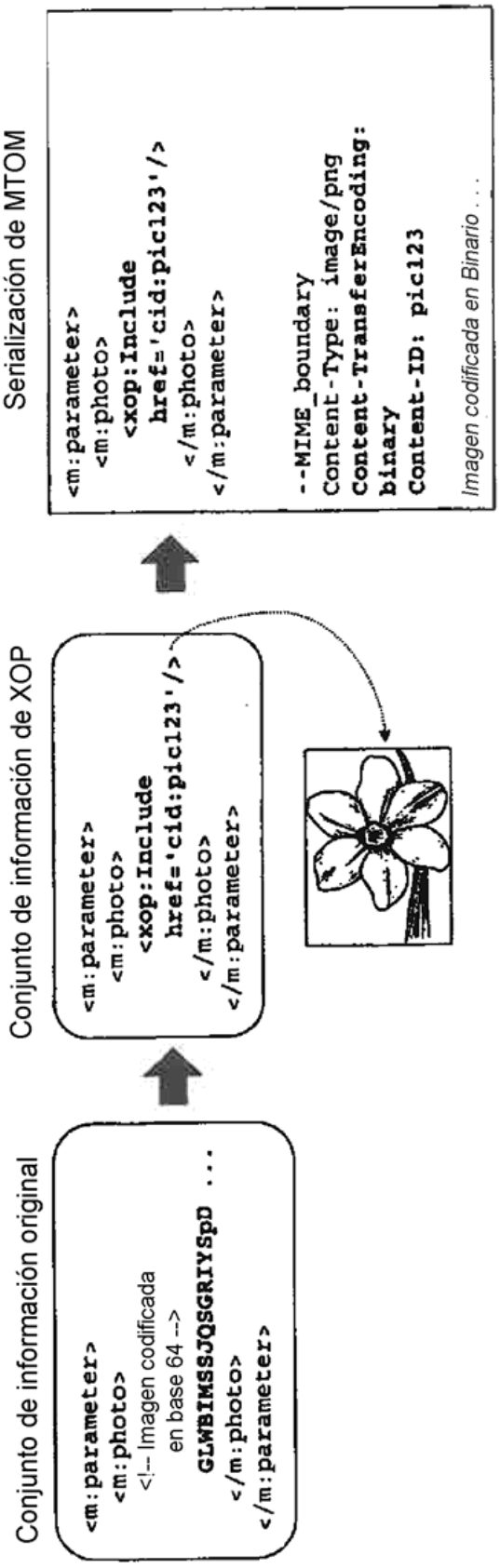
Conjunto de información original
<m:parameter>
<m:photo>
<!-- Imagen codificada en base 64 -->
GlWBIMSSJQSGRIYSpD ...
</m:photo>
</m:parameter>
Conjunto de información de XOP
<m:parameter>
<m:photo>
<xop:Include
href='cid:pic123'/>
</m:photo>
</m:parameter>
Serialización de MTOM
<m:parameter>
<m:photo>
<xop:Include
href='cid:pic123'/>
</m:photo>
</m:parameter>
--MIME_boundary
Content-Type: image/png
Content-TransferEncoding:
binary
Content-ID: pic123
Imagen codificada en Binario . . .

Fig. 1

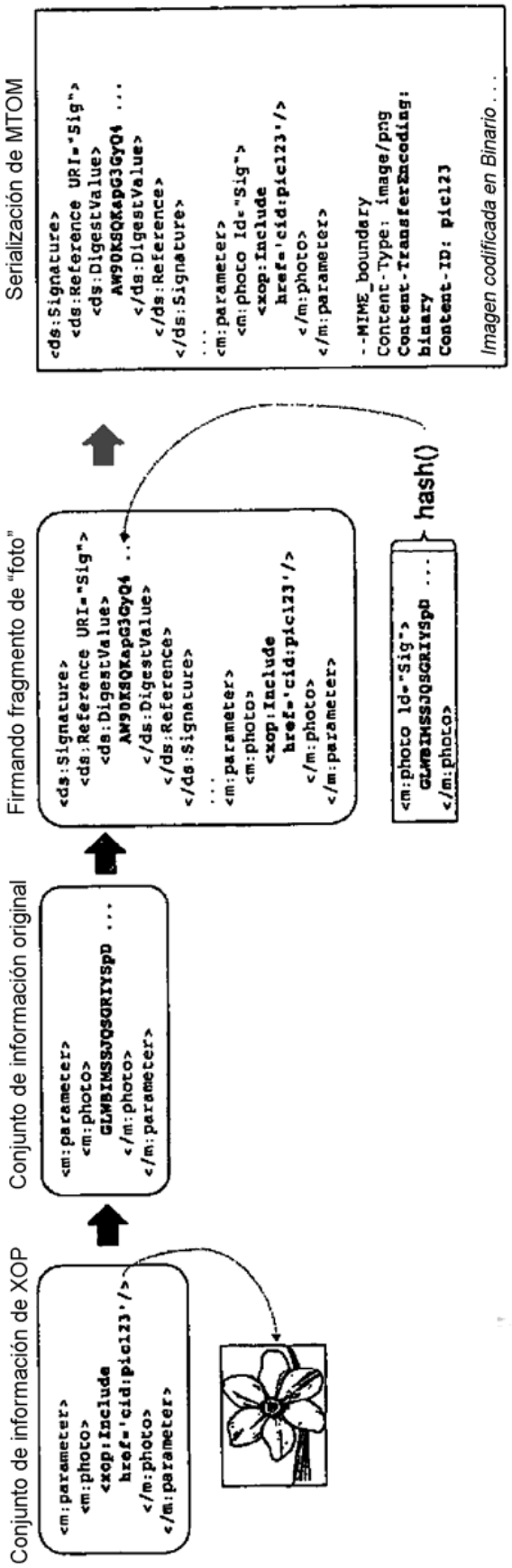
Conjunto de información de XOP
Conjunto de información original
Firmando fragmento de "foto"
Serialización de MTOM
hash()
Imagen codificada en Binario . . .

Fig. 2

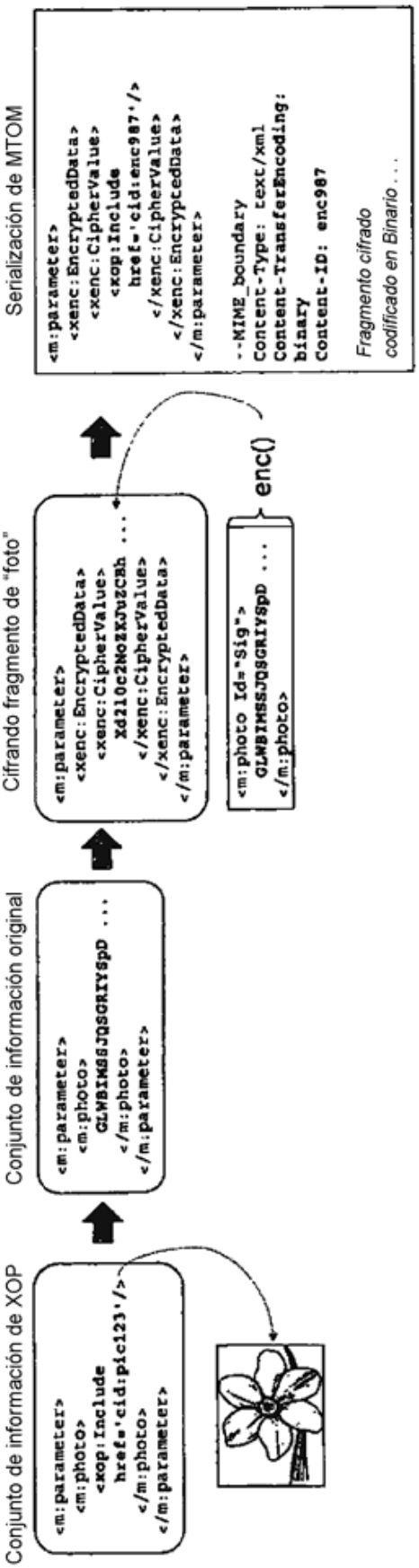
Conjunto de información de XOP
<m:parameter>
<m:photo>
<xop:Include
href='cid:pic123'/>
</m:photo>
</m:parameter>
Conjunto de información original
<m:parameter>
<m:photo>
GLMBIMSSJQSGRIYSpD ...
</m:photo>
</m:parameter>
Cifrando fragmento de "foto"
<m:parameter>
<xenc:EncryptedData>
<xenc:CipherValue>
Xd210c2NoZXJvZCBh ...
</xenc:CipherValue>
</xenc:EncryptedData>
</m:parameter>
<m:photo Id="Sig">
GLMBIMSSJQSGRIYSpD ...
</m:photo>
enc()
Serialización de MTOM
<m:parameter>
<xenc:EncryptedData>
<xenc:CipherValue>
<xop:Include
href='cid:enc987'/>
</xenc:CipherValue>
</xenc:EncryptedData>
</m:parameter>
--MIME_boundary
Content-Type: text/xml
Content-TransferEncoding:
binary
Content-ID: enc987
Fragmento cifrado
codificado en Binario ...

Fig. 3

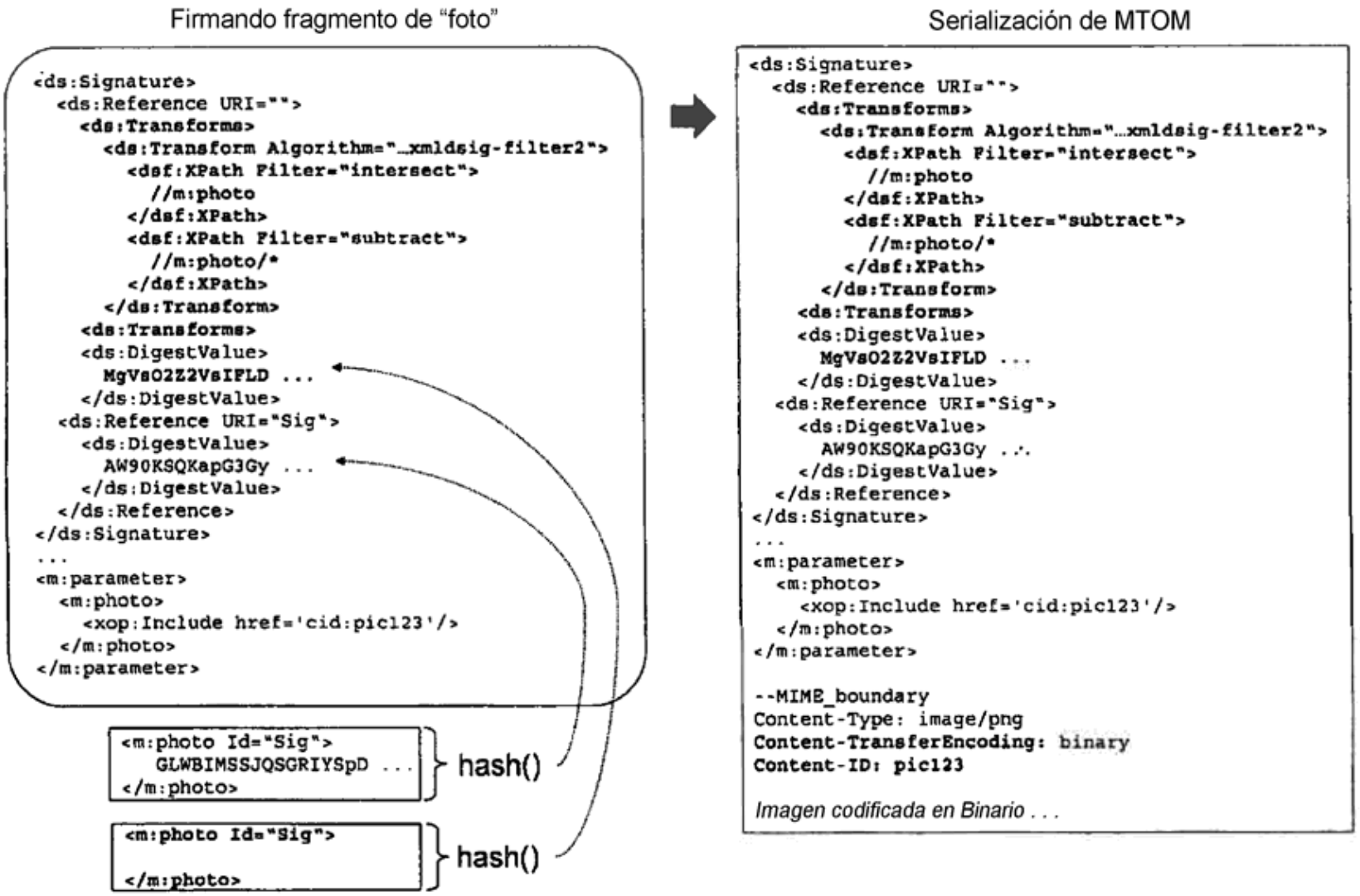
Firmando fragmento de “foto”
Serialización de MTOM
<ds:Signature>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="…xmldsig-filter2">
<dsf:XPath Filter="intersect">
//m:photo
</dsf:XPath>
<dsf:XPath Filter="subtract">
//m:photo/*
</dsf:XPath>
</ds:Transform>
<ds:Transforms>
<ds:DigestValue>
MgVsO2Z2VsIFLD ...
</ds:DigestValue>
<ds:Reference URI="Sig">
<ds:DigestValue>
AW90KSQKapG3Gy ...
</ds:DigestValue>
</ds:Reference>
</ds:Signature>
...
<m:parameter>
<m:photo>
<xop:Include href='cid:pic123'/>
</m:photo>
</m:parameter>
<m:photo Id="Sig">
GLWBIMSSJQSGRIYSpD ...
</m:photo>
hash()
<m:photo Id="Sig">
</m:photo>
hash()
<ds:Signature>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="…xmldsig-filter2">
<dsf:XPath Filter="intersect">
//m:photo
</dsf:XPath>
<dsf:XPath Filter="subtract">
//m:photo/*
</dsf:XPath>
</ds:Transform>
<ds:Transforms>
<ds:DigestValue>
MgVsO2Z2VsIFLD ...
</ds:DigestValue>
<ds:Reference URI="Sig">
<ds:DigestValue>
AW90KSQKapG3Gy ...
</ds:DigestValue>
</ds:Reference>
</ds:Signature>
...
<m:parameter>
<m:photo>
<xop:Include href='cid:pic123'/>
</m:photo>
</m:parameter>
--MIME_boundary
Content-Type: image/png
Content-TransferEncoding: binary
Content-ID: pic123
Imagen codificada en Binario . . .

Fig. 4

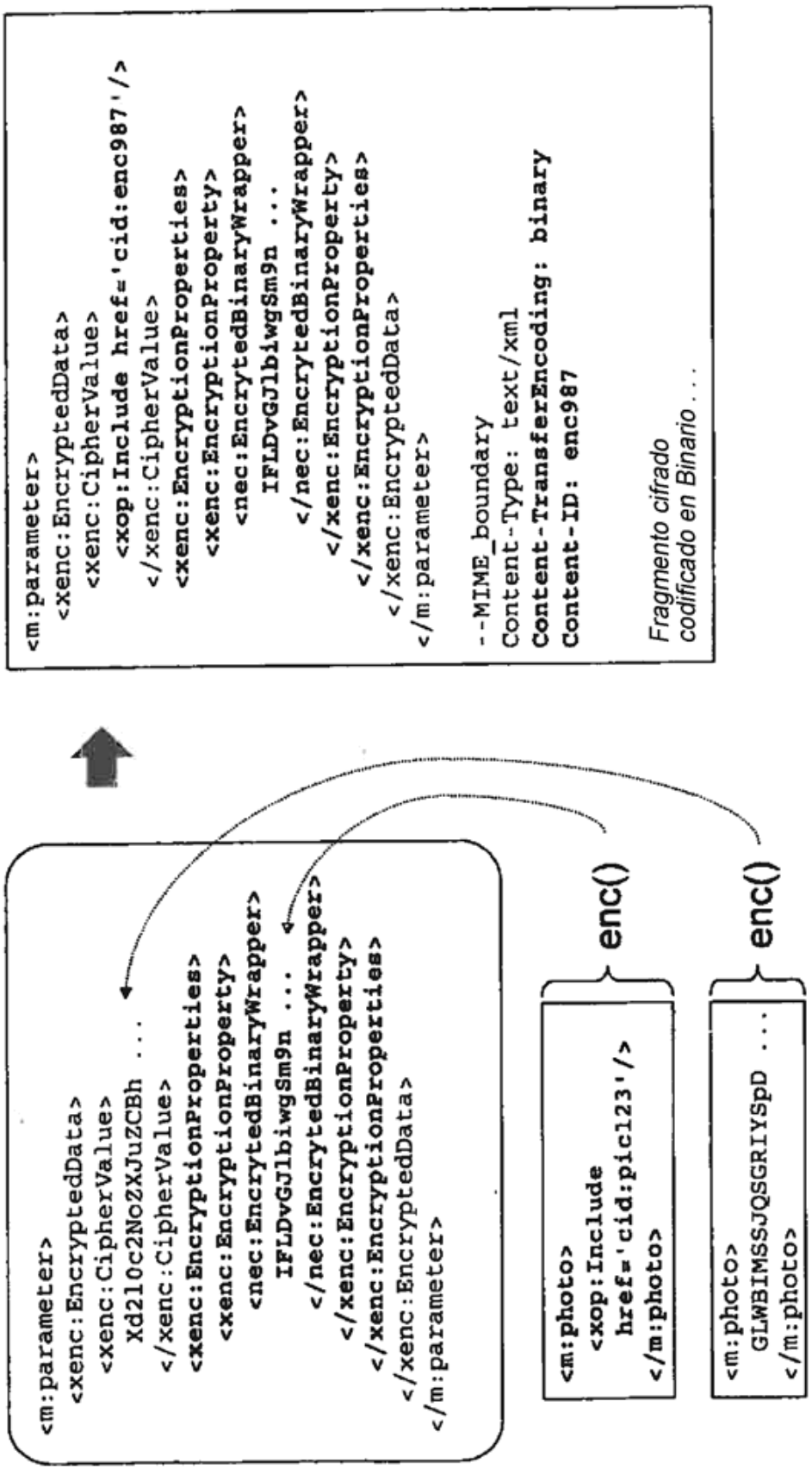
Cifrando fragmento de "foto"
<m:parameter>
<xenc:EncryptedData>
<xenc:CipherValue>
Xd210c2NoZXJuZCBh ...
</xenc:CipherValue>
<xenc:EncryptionProperties>
<xenc:EncryptionProperty>
<nec:EncrytedBinaryWrapper>
IFLDvGJlbiwgSm9n ...
</nec:EncrytedBinaryWrapper>
</xenc:EncryptionProperty>
</xenc:EncryptionProperties>
</xenc:EncryptedData>
</m:parameter>
<m:photo>
<xop:Include
href='cid:pic123'/>
</m:photo>
enc()
<m:photo>
GLWBIMSSJQSGRIYSpD ...
</m:photo>
enc()
Serialización de MTOM
<m:parameter>
<xenc:EncryptedData>
<xenc:CipherValue>
<xop:Include href='cid:enc987'/>
</xenc:CipherValue>
<xenc:EncryptionProperties>
<xenc:EncryptionProperty>
<nec:EncrytedBinaryWrapper>
IFLDvGJlbiwgSm9n ...
</nec:EncrytedBinaryWrapper>
</xenc:EncryptionProperty>
</xenc:EncryptionProperties>
</xenc:EncryptedData>
</m:parameter>
--MIME_boundary
Content-Type: text/xml
Content-TransferEncoding: binary
Content-ID: enc987
Fragmento cifrado
codificado en Binario . . .

Fig. 5

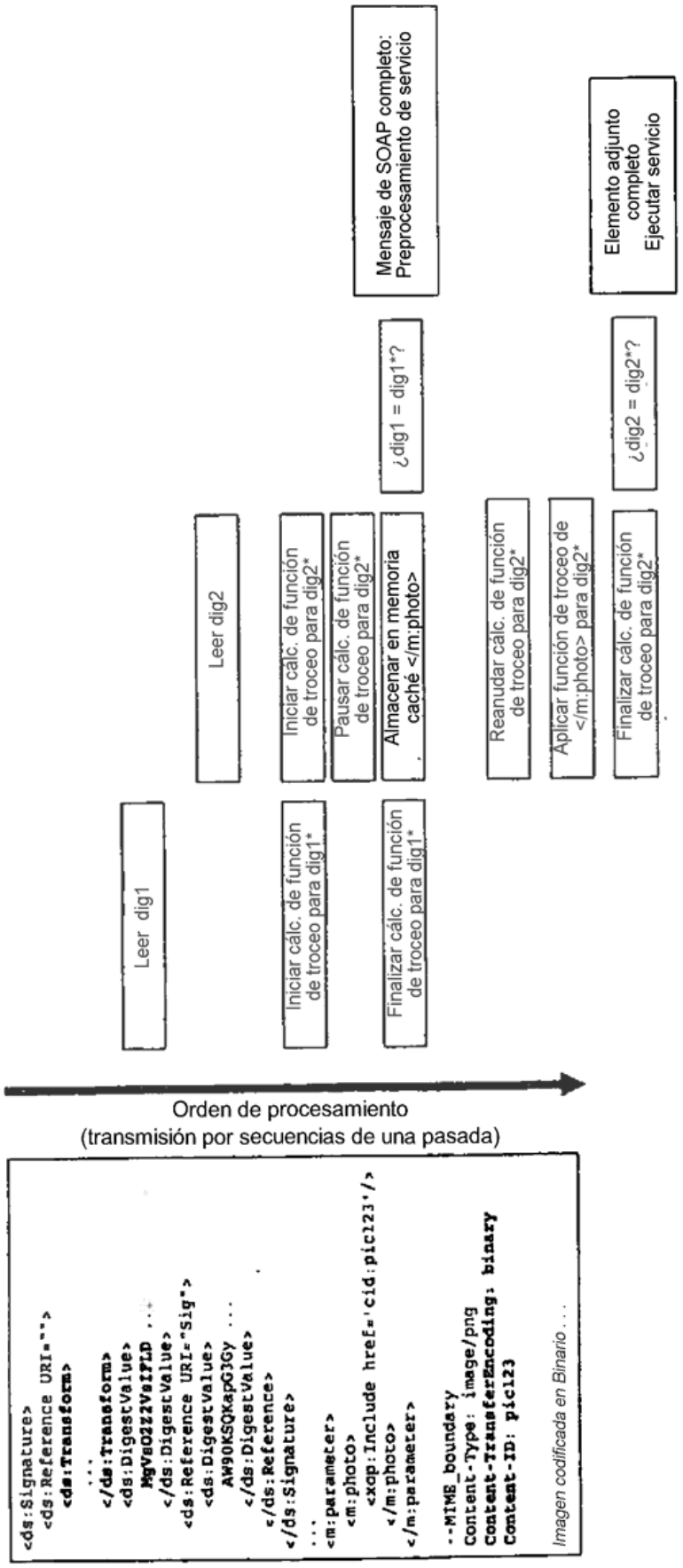
<ds:Signature>
<ds:Reference URI="">
<ds:Transform>
...
</ds:Transform>
<ds:DigestValue>
HgVsO2i2VaIFLD ...
</ds:DigestValue>
<ds:Reference URI="Sig">
<ds:DigestValue>
AW9OKSQXapGJGy ...
</ds:DigestValue>
</ds:Reference>
</ds:Signature>
...
<m:parameter>
<m:photo>
<xop:Include href='cid:pic123'/>
</m:photo>
</m:parameter>
--MIME_boundary
Content-Type: image/png
Content-Transfer-Encoding: binary
Content-ID: pic123
Imagen codificada en Binario ...
Orden de procesamiento
(transmisión por secuencias de una pasada)
Leer dig1
Leer dig2
Iniciar cálc. de función de troceo para dig1*
Iniciar cálc. de función de troceo para dig2*
Pausar cálc. de función de troceo para dig2*
Finalizar cálc. de función de troceo para dig1*
Almacenar en memoria caché </m:photo>
¿dig1 = dig1*?
Reanudar cálc. de función de troceo para dig2*
Aplicar función de troceo de </m:photo> para dig2*
Finalizar cálc. de función de troceo para dig2*
¿dig2 = dig2*?
Mensaje de SOAP completo: Preprocesamiento de servicio
Elemento adjunto completo
Ejecutar servicio

Fig. 6

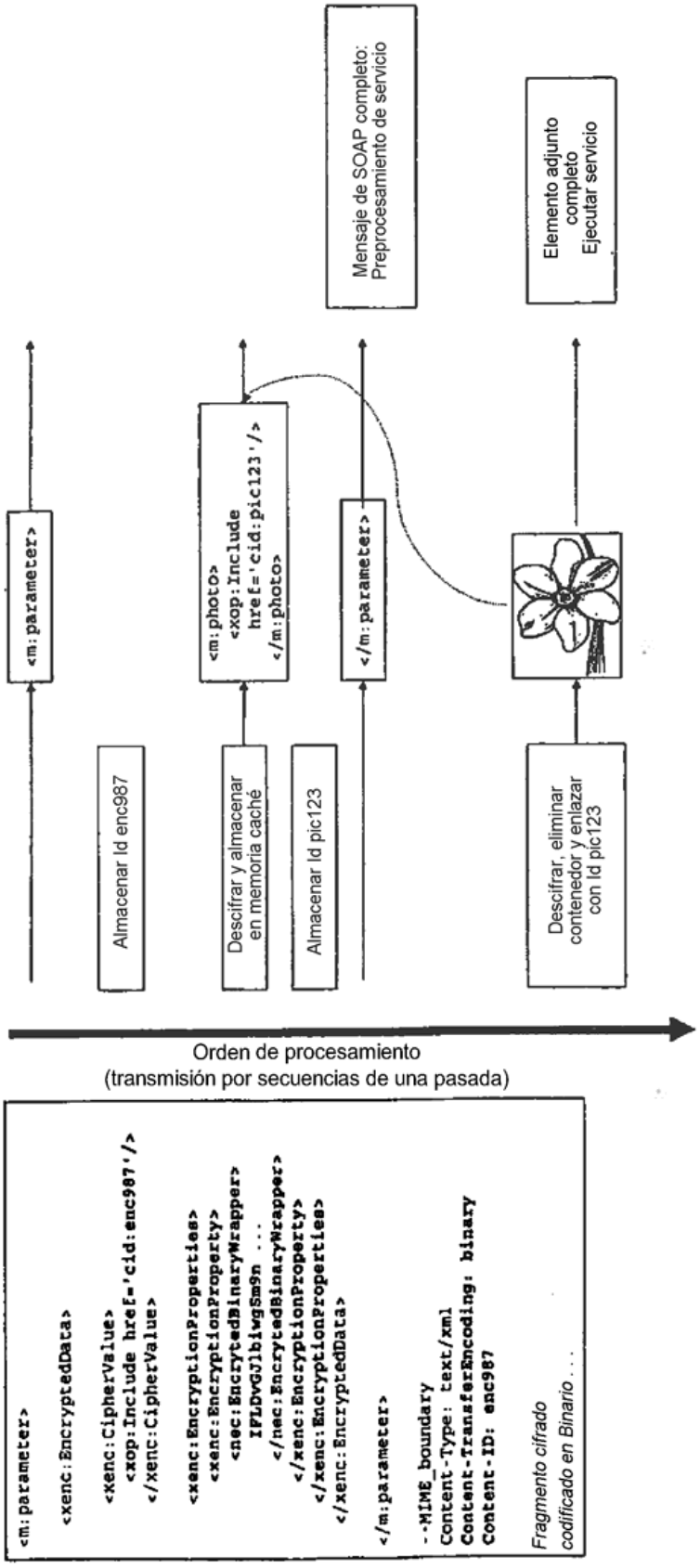
<m:parameter>
<xenc:EncryptedData>
<xenc:CipherValue>
<xop:Include href='cid:enc987'/>
</xenc:CipherValue>
<xenc:EncryptionProperties>
<xenc:EncryptionProperty>
<nec:EncrytedBinaryWrapper>
IFLDvGJlbivgSm9n ...
</nec:EncrytedBinaryWrapper>
</xenc:EncryptionProperty>
</xenc:EncryptionProperties>
</xenc:EncryptedData>
</m:parameter>
--MIME_boundary
Content-Type: text/xml
Content-Transfer-Encoding: binary
Content-ID: enc987
Fragmento cifrado
codificado en Binario ...
Orden de procesamiento
(transmisión por secuencias de una pasada)
<m:parameter>
Almacenar Id enc987
<m:photo>
<xop:Include
href='cid:pic123'/>
</m:photo>
Descifrar y almacenar
en memoria caché
Almacenar Id pic123
</m:parameter>
Mensaje de SOAP completo:
Preprocesamiento de servicio
Descifrar, eliminar
contenedor y enlazar
con Id pic123
Elemento adjunto
completo
Ejecutar servicio

Fig. 7