

Señores
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISIÓN DE NUEVAS CREACIONES
E. S. D.

SUPERINDUSTRIA Y COMERCIO
Radicación : 06010919 00000002 Folios: 207
Fecha (MM): 2006-03-23 14:26:26
Trámite : 002 PATENTES y REGISTRO/ 444 RESPUESTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Ref.: Expediente No. 06-010.919
Solicitud de Registro para Patente de
Invención denominada SISTEMA Y METODO
PARA ESTABLECER QUE UN SERVIDOR Y UN
CORRESPONDIENTE TIENEN E.MAIL SEGURO
Y COMPATIBLE.

Solicitante: Microsoft Corporation

Darío Cárdenas Navas identificado como aparece al ple de mi firma, me dirijo a ese Despacho dando respuesta al Oficio No. 2113 de fecha 23 de Febrero, 2006 adjuntando los documentos restantes dentro de la solicitud de patente en referencia:

1. Copia auténtica de los documentos donde constan las cesiones del derecho a las patente reivindicadas otorgadas por los inventores a favor del solicitante debidamente Apostilladas y con sus correspondientes traducciones oficiales.
2. Copia auténtica del documento de prioridad correspondiente a la patente de los Estados Unidos No. 11/107.011 de fecha Abril 15 de 2005.

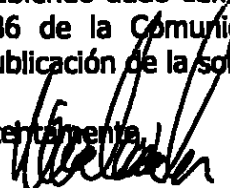
Copia auténtica del documento de prioridad correspondiente a la patente de los Estados Unidos No. 60/659.279 de de fecha Marzo 7 de 2005.

Tal como consta en el Expediente el recibo oficial 06-8.876 de fecha Febrero 2 de 2006 y 06-08.876 de Febrero 2 de 2006 correspondientes a las reivindicaciones de prioridad fue presentado junto con la solicitud de patente radicada ante ese Despacho el día 6 de Febrero de 2006.

3. Informo a ese Despacho que como solicitud nacional deberá tomarse la descripción de la Solicitud de Patente no provisional No. 11/107.011, cuyo texto se adjunta al presente memorial y que ya obra en el expediente de la referencia.
4. Extracto para publicación.

Habiendo dado cumplimiento a los requerimientos de forma establecidos por la Decisión 486 de la Comunidad Andina, atentamente solicito a ese Despacho proceda con la publicación de la solicitud de patente en referencia.

Atentamente,


Darío Cárdenas Navas.
c.c. 17.066.629 de Bogotá
t.p. 1.250 C.S.J. 

APOSTILLE*(Convention de La Haye du 5 octobre 1961)*

1. Country: United States of America

This public document

2. has been signed by M. Sias

3. acting in the capacity of Certifying Officer

4. bears the seal/stamp of U.S. Patent and Trademark Office

Certified

5. at Washington, D.C.

6. the third of January, 2006

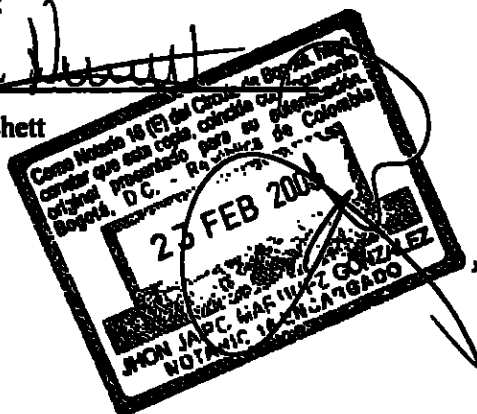
7. by Assistant Authentication Officer, United States Department of State

8. No. 06007989-6

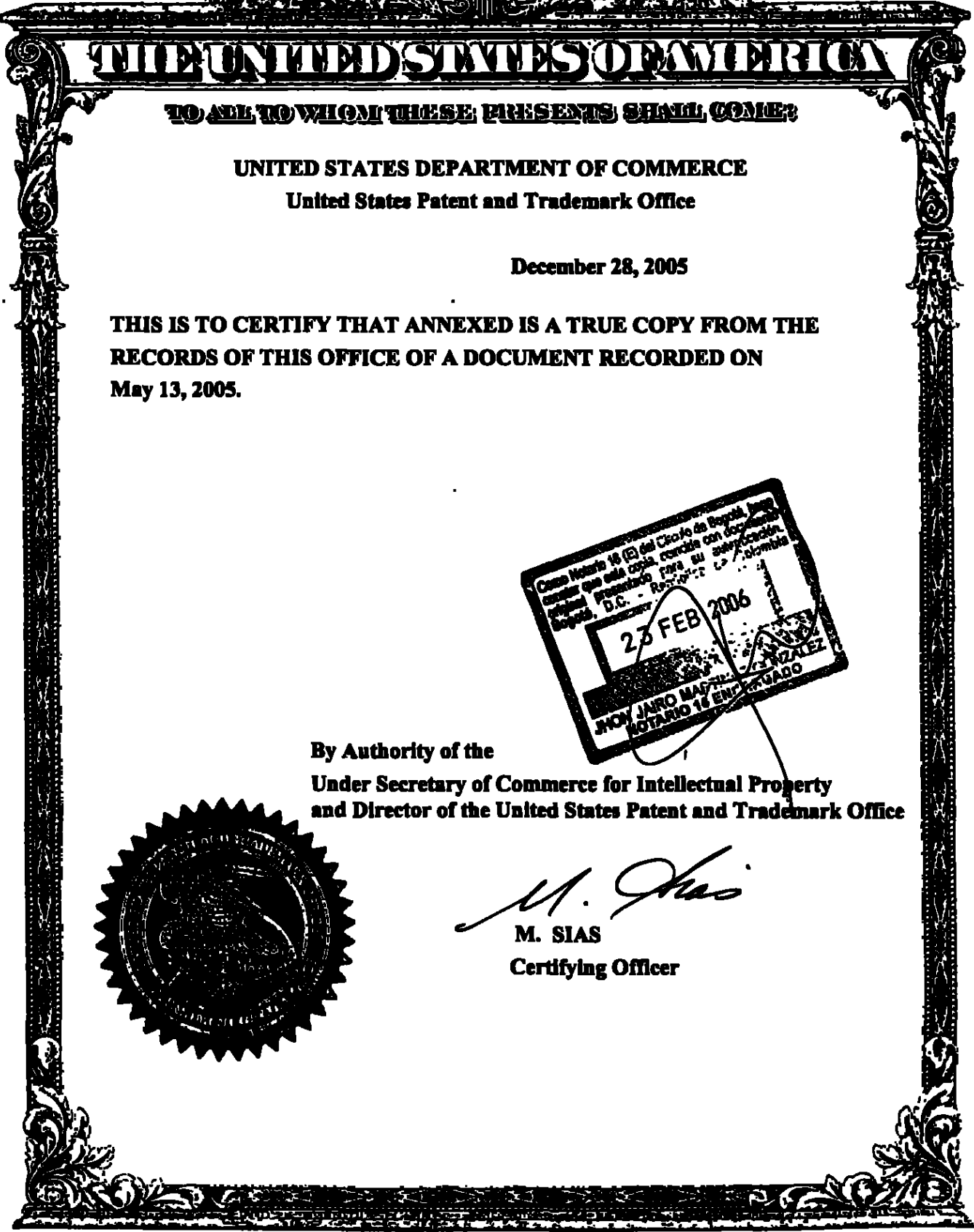
9. Seal/Stamp:

10. Signature:

Patrick O. Hatchett
Patrick O. Hatchett



A 1408869



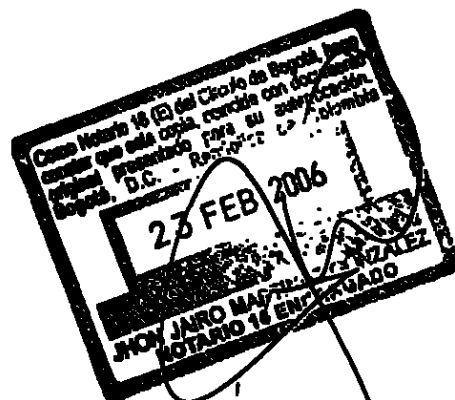
THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

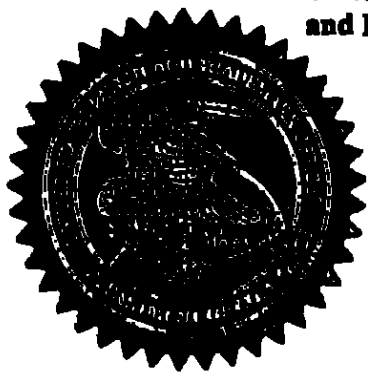
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

December 28, 2005

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF A DOCUMENT RECORDED ON
May 13, 2005.



By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office



M. Sias
M. SIAS
Certifying Officer

166

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	NEW ASSIGNMENT										
NATURE OF CONVEYANCE:	ASSIGNMENT										
CONVEYING PARTY DATA											
<table><tr><th>Name</th><th>Execution Date</th></tr><tr><td>Eric D. Tribbia</td><td>04/14/2006</td></tr><tr><td>Travor W. Freeman</td><td>04/14/2005</td></tr></table>		Name	Execution Date	Eric D. Tribbia	04/14/2006	Travor W. Freeman	04/14/2005				
Name	Execution Date										
Eric D. Tribbia	04/14/2006										
Travor W. Freeman	04/14/2005										
RECEIVING PARTY DATA											
<table><tr><td>Name:</td><td>Microsoft Corporation</td></tr><tr><td>Street Address:</td><td>One Microsoft Way</td></tr><tr><td>City:</td><td>Redmond</td></tr><tr><td>State/Country:</td><td>WASHINGTON</td></tr><tr><td>Postal Code:</td><td>98052</td></tr></table>		Name:	Microsoft Corporation	Street Address:	One Microsoft Way	City:	Redmond	State/Country:	WASHINGTON	Postal Code:	98052
Name:	Microsoft Corporation										
Street Address:	One Microsoft Way										
City:	Redmond										
State/Country:	WASHINGTON										
Postal Code:	98052										
PROPERTY NUMBERS Total: 1											
<table><tr><th>Property Type</th><th>Number</th></tr><tr><td>Application Number:</td><td>80608279</td></tr></table>		Property Type	Number	Application Number:	80608279						
Property Type	Number										
Application Number:	80608279										
CORRESPONDENCE DATA											
Fax Number: (314)231-4342 <i>Correspondence will be sent via US Mail when the fax attempt is unsuccessful.</i> Phone: 3142316400 Email: uspatents@senniger.com Correspondent Name: Robert M. Bain Address Line 1: One Metropolitan Square, 16th Floor Address Line 2: Senniger Powers Address Line 4: St. Louis, MISSOURI 63102											
NAME OF SUBMITTER:	Robert M. Bain										
Total Attachments: 1 source=00078147#page1.tif											



500031382

PATENT
REEL: 016013 FRAME: 0231

4

APR 14 2005 12:11 FR

TO 913142314342 P.02/05
MS Docket No. 311616.01
OC Docket No. MSFT 5189

PATENT ASSIGNMENT

I/WE, Eric D. Tribble and Trevor W. Freeman ("ASSIGNOR"), have invented subject matter ("INVENTION") disclosed and/or claimed in a patent application entitled "SYSTEM AND METHOD FOR ESTABLISHING A LINK BETWEEN A SERVER AND A TARGET" ("APPLICATION"), which:

☐ will be filed without this executed PATENT ASSIGNMENT. ASSIGNOR hereby authorizes, and requests, ASSIGNEE'S legal representatives, of SENNIGER POWERS, who are associated with customer number 000038779, to insert here in parenthesis (U.S. Serial No. 69/659,279, filed 02/01/2005) this APPLICATION's U.S. Serial Number and filing date, when known;

☒ was filed on March 7, 2005 and was given U.S. Serial No. 69/659,279;

☐ is filed concurrently herewith;

Microsoft Corporation, a Washington Corporation, on behalf of itself and its successors and assigns ("ASSIGNEE"), is entitled to, and is desirous of acquiring, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and all other applications and patents derived therefrom, such as continuing applications, in and for the United States, its territories, and all foreign countries ("APPLICATION DERIVATIVES")):

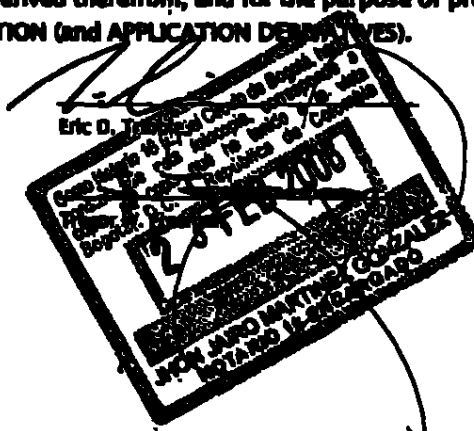
For good and valuable consideration, the receipt of which is hereby acknowledged by the ASSIGNOR, the ASSIGNOR hereby sells, assigns and transfers to the ASSIGNEE, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and APPLICATION DERIVATIVES);

ASSIGNOR agrees to execute all instruments and documents required for the making and prosecution of the APPLICATION (and APPLICATION DERIVATIVES), for litigation regarding letters patent derived therefrom, and for the purpose of protecting and perfecting title to the APPLICATION (and APPLICATION DERIVATIVES).

4/14/05
DATE

4/14/05
DATE

FRACwa



RECORDED: 06/13/2005

PATENT
REEL: 016013 FRAME: 0232

Nora Jiménez de Adam

168

TRADUCCIÓN DEL INGLÉS AL ESPAÑOL DE CUATRO PÁGINAS DE UN DOCUMENTO ORIGINAL ENTREGADO EN UNA CARPETA DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DEL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS, CON COBERTURA DE PLÁSTICO TRANSPARENTE, REALIZADA POR NORA JIMÉNEZ DE ADAM, TRADUCTORA E INTÉRPRETE OFICIAL. TEL: 571-2572804; FEBRERO 8 DE 2006

"APOSTILLE

(Convención De La Haya de octubre 5 de 1961)

1. País: ESTADOS UNIDOS DE AMÉRICA
2. Este documento público fue firmado por: M. SIAS
3. En su calidad de: FUNCIONARIO DE CERTIFICACIONES
4. Lleva el sello de: LA OFICINA DE PATENTES Y MARCAS REGISTRADAS

CERTIFICADO

5. En: WASHINGTON, D.C.
6. El día tres de enero de 2006
7. Por: ASISTENTE DEL FUNCIONARIO DE AUTENTICACIONES DEL DEPARTAMENTO DE ESTADO DE ESTADOS UNIDOS
8. No. 060079889-6
9. Sello: SELLO SECO DEL DEPARTAMENTO DE ESTADOS UNIDOS
10. Firma: PATRICK O. HATCHETT



SEGUNDA PÁGINA:

Emitida en papelería especial con reborde negro-gris con el número A 1408860 en la parte superior izquierda del documento: ESTADOS UNIDOS DE AMÉRICA - PARA AQUÉLLOS A QUIENES PUEDA INTERESAR: EL DEPARTAMENT

1

**DE COMERCIO DE LOS ESTADOS UNIDOS Oficina de Patentes y Marcas
Registradas de los Estados Unidos**

Diciembre 28 de 2005

**ESTE DOCUMENTO CERTIFICA QUE LOS ANEXOS SON COPIA FIEL DEL
DOCUMENTO QUE FUE REGISTRADO EN ESTA OFICINA EL DÍA 13 DE
MAYO DE 2005.**

**Estampilla dorada del Departamento de Comercio - Oficina de Patentes y Marcas
Registradas de los Estados Unidos**

**Bajo la potestad del SUBSECRETARIO DE COMERCIO PARA LA PROPIEDAD
INTELECTUAL Y DIRECTOR DE LA OFICINA DE PATENTES Y MARCAS
REGISTRADAS DE ESTADOS UNIDOS**

(Firma)

M. SIAS

Funcionario de Certificaciones

TERCERA PÁGINA: Papel blanco con lo siguiente en el margen superior derecho: CH
\$40.00 60659279. Al margen superior izquierdo hay un bloque de texto ilegible.

CESIÓN DE LA PATENTE



Versión Electrónica v1.1

Versión Impresa v1.1

Tipo de Presentación:	Nueva Cesión
Característica de la Transferencia:	Cesión

7

8

Información de La Parte que Transfiere

Nombre	Fecha de Ejecución
Eric D. Tribble	04/14/2005
Trevor W. Freeman	04/14/2005

Información de la Parte Receptora

Nombre:	MICROSOFT CORPORATION
Dirección:	One Microsoft Way
Ciudad:	Redmond
Estado/País:	WASHINGTON
Código Postal:	98052

Número Total de Propiedades: 1

Tipo de Propiedad:	Número
Número de Solicitud:	60659279

CORRESPONDENCIA

Número de telefax: (314) 231- 4342

La correspondencia será enviada por correo de los Estados Unidos si el telefax falla

Teléfono: 3142315400

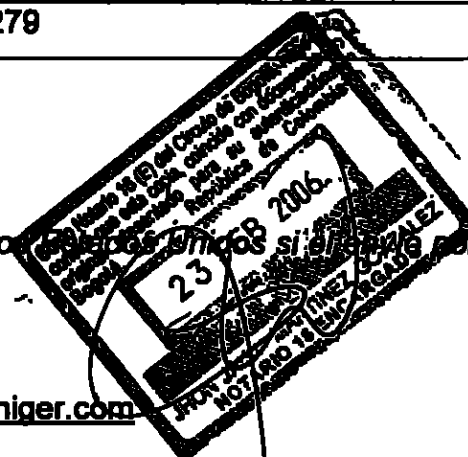
Correo Electrónico: uspatents@senniger.com

Nombre del Correspondiente: Robert M. Bain

Renglón 1 de la Dirección: One Metropolitan Square, 16th Floor

Renglón 2 de la Dirección: Senniger Powers

Renglón 4 de la Dirección: St. Louis, MISSOURI 63102



7

6

171

NOMBRE DE QUIEN ENVÍA:	Robert M. Bain
------------------------	----------------

Número de Anexos: 1 Fuente = 00078147#page1.tif
--

500031382

PATENTE

Carrete: 016013; Pantalla: 0231

CUARTA PÁGINA: Con encabezado de fax Apr 14 2005 12:11 FR TO
913142314342 P02/05

No. de Expediente de MS: 311610.01

No. de Expediente de OC: MSFT 5169

CESIÓN DE PATENTE

YO/NOSOTROS, Eric D. Tribble y Trevor W. Freeman ("CEDENTES") somos los creadores de un asunto ("INVENTO") revelado y/o reivindicado en la solicitud de patente llamado SISTEMA Y MÉTODO PARA ESTABLECER UN VÍNCULO ENTRE UN SERVIDOR Y UN OBJETIVO ("SOLICITUD").

_ Será registrada sin esta CESIÓN DE PATENTE ejecutada. Los CEDENTES por este documento autorizan y solicitan a los representantes legales del CESIONARIO, de Senniger Powers, los cuales están asociados al número de cliente 000038779, la inserción en este paréntesis (No. de serial U.S. 60/659279, presentado el 03/07/2005) del No. de Serie US de la SOLICITUD y su fecha de presentación, si esto es conocido;



☒ Fue presentada el 7 de marzo de 2005 y le fue otorgada el No. de Serial U.S. 60/659,279;

9

9

Microsoft Corporation, una corporación del estado de Washington, en su nombre y en el de sus sucesores y cesionarios ("CESIONARIO") tiene derecho e intenta adquirir la totalidad y la exclusividad de los derechos, títulos e intereses en el INVENTO y la SOLICITUD (y de cualesquiera otra solicitudes y patentes que de éstos se deriven, tales como solicitudes continuas en y para los Estados Unidos, sus territorios y en cualquiera y todos los países extranjeros ("DERIVADOS DE LA SOLICITUD")):

A cambio de contraprestaciones onerosas, el recibo de las cuales se reconocen en este documento por los CEDENTES, éstos por el presente venden, ceden y transfieren al CESIONARIO la totalidad y la exclusividad de los derechos, títulos e intereses en dicho INVENTO y en la SOLICITUD (y en los DERIVADOS DE LA SOLICITUD):

Los CEDENTES acuerdan ejecutar todos los instrumentos y documentos requeridos para elaborar y dar curso a la SOLICITUD (y los DERIVADOS DE LA SOLICITUD) para fines de litigios relacionados con los mismos, para proteger y perfeccionar dicho título sobre la SOLICITUD (y los DERIVADOS DE LA SOLICITUD).

(Firma) _____
Eric D. Tribble

(Firma)
Trevor W. Freeman

FRACwa

✓

۱۷

PATENTE

Carrete: 016013; Pantalla: 0232

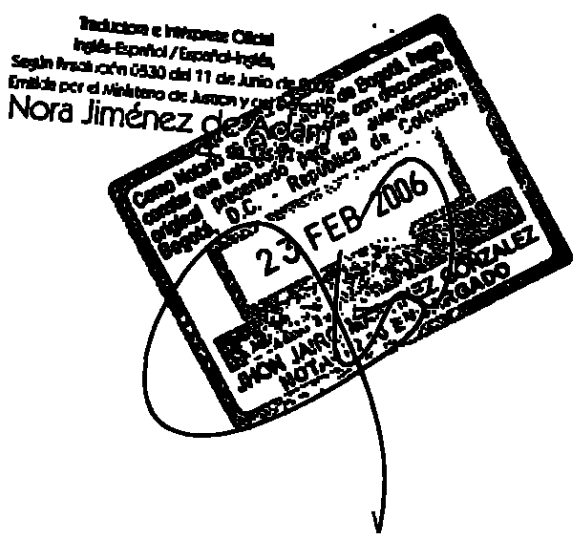
Registrado el 05/13/2005

**CONTRAPORTADA: LOGO DEL DEPARTAMENTO DE COMERCIO DE
ESTADOS UNIDOS – OFICINA DE PATENTES Y MARCAS REGISTRADAS**

CERTIFICO QUE ESTA ES UNA TRADUCCIÓN FIEL DEL INGLES AL ESPAÑOL DE UN DOCUMENTO QUE HE TENIDO A LA VISTA; QUE SOY TRADUCTORA E INTERPRETE OFICIAL ACREDITADA POR RESOLUCIONES 0035 Y 530 DE LA UNIVERSIDAD NACIONAL DE COLOMBIA Y DEL MINISTERIO DE LA JUSTICIA RESPECTIVAMENTE, Y QUE ESTOY REGISTRADA ANTE EL MINISTERIO DE RELACIONES EXTERIORES DE COLOMBIA

Bogotá, febrero 8 de 2006

Nora Jiménez de Adam
NORA JIMÉNEZ DE ADAM
C.C. 20.335.247



APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. Country: United States of America

This public document

2. has been signed by P. Swain

3. acting in the capacity of Certifying Officer

4. bears the seal/stamp of Patent and Trademark Office

Certified

5. at Washington, D.C.

6. the thirtieth of December, 2005

7. by Assistant Authentication Officer, United States Department of State

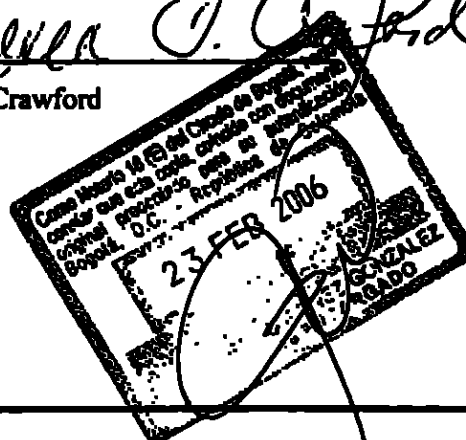
8. No. 06007851-7

9. Seal/Stamp:

10. Signature:

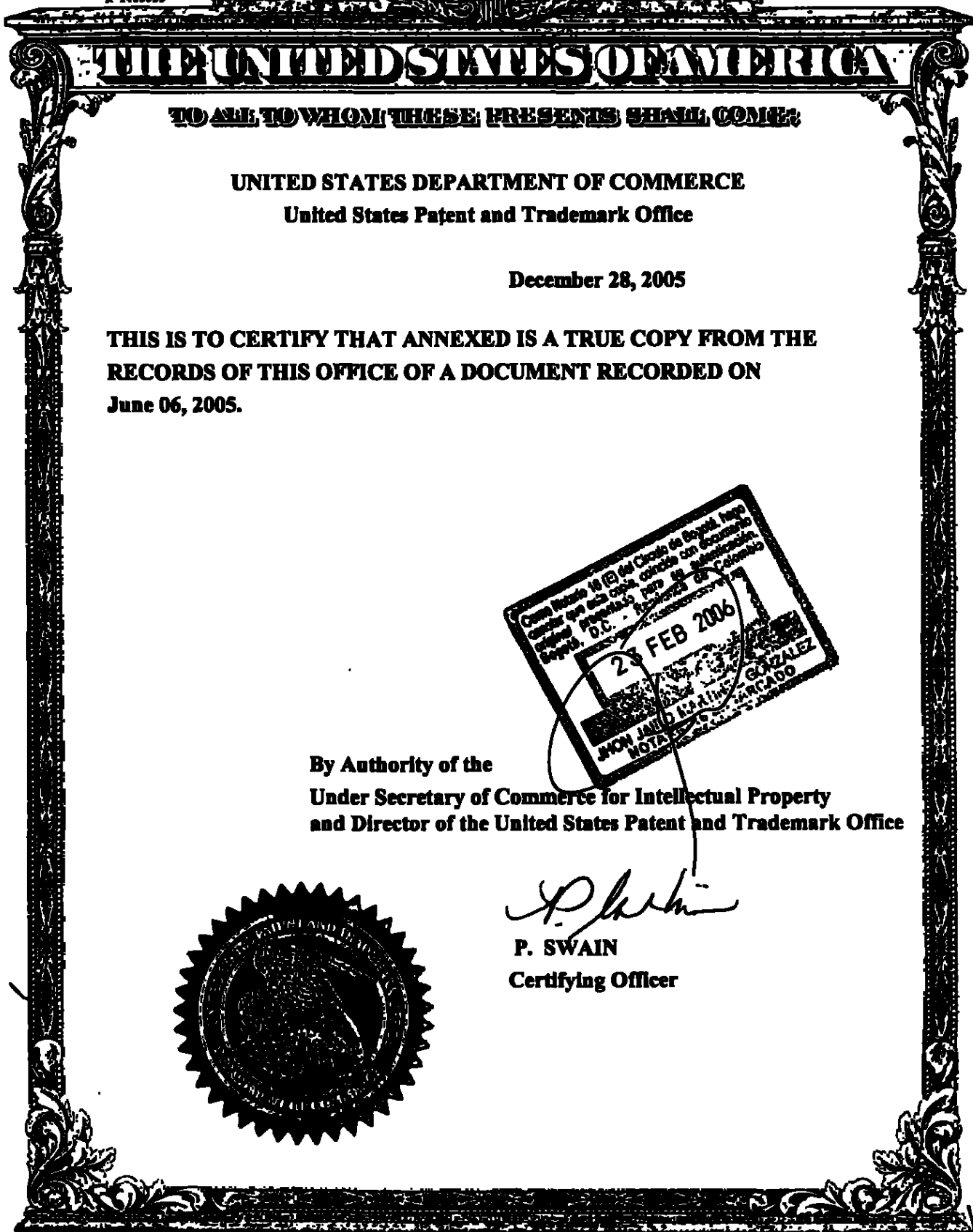
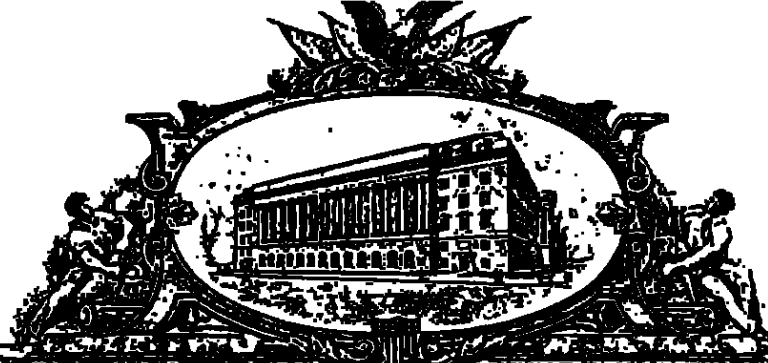
Fernesia T. Crawford

Fernesia T. Crawford



175

A 1400000



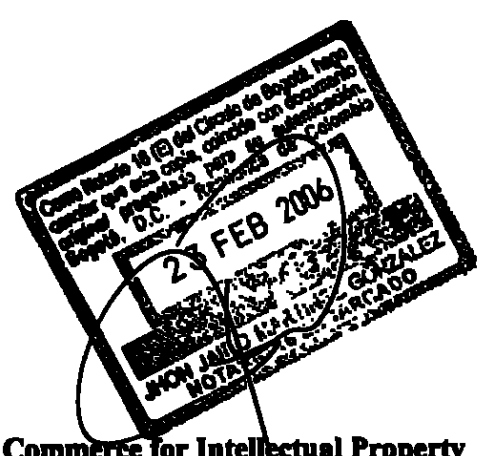
THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

December 28, 2005

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF A DOCUMENT RECORDED ON
June 06, 2005.



By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office



P. Swain
P. SWAIN
Certifying Officer

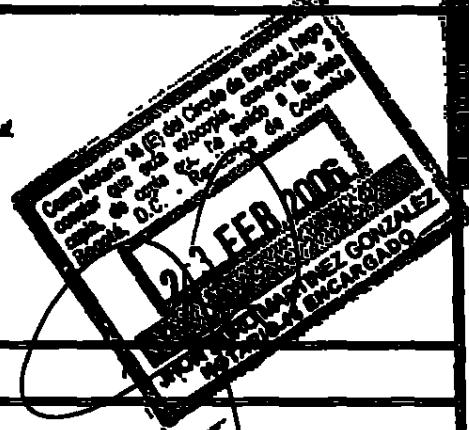
16

176

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

SUBMISSION TYPE:	NEW ASSIGNMENT										
NATURE OF CONVEYANCE:	ASSIGNMENT										
CONVEYING PARTY DATA											
<table border="1"><thead><tr><th>Name</th><th>Execution Date</th></tr></thead><tbody><tr><td>Eric D. Tribble</td><td>04/14/2008</td></tr><tr><td>Trevor W. Freeman</td><td>04/14/2008</td></tr></tbody></table>		Name	Execution Date	Eric D. Tribble	04/14/2008	Trevor W. Freeman	04/14/2008				
Name	Execution Date										
Eric D. Tribble	04/14/2008										
Trevor W. Freeman	04/14/2008										
RECEIVING PARTY DATA											
<table border="1"><tr><td>Name:</td><td>Microsoft Corporation</td></tr><tr><td>Street Address:</td><td>One Microsoft Way</td></tr><tr><td>City:</td><td>Redmond</td></tr><tr><td>State/Country:</td><td>WASHINGTON</td></tr><tr><td>Postal Code:</td><td>98052</td></tr></table>		Name:	Microsoft Corporation	Street Address:	One Microsoft Way	City:	Redmond	State/Country:	WASHINGTON	Postal Code:	98052
Name:	Microsoft Corporation										
Street Address:	One Microsoft Way										
City:	Redmond										
State/Country:	WASHINGTON										
Postal Code:	98052										
PROPERTY NUMBERS Total: 1											
<table border="1"><thead><tr><th>Property Type</th><th>Number</th></tr></thead><tbody><tr><td>Application Number:</td><td>11107011</td></tr></tbody></table>		Property Type	Number	Application Number:	11107011						
Property Type	Number										
Application Number:	11107011										
CORRESPONDENCE DATA											
Fax Number: (314)231-4342 <i>Correspondence will be sent via US Mail when the fax attempt is unsuccessful.</i> Phone: 3142818400 Email: uspatents@senniger.com Correspondent Name: Robert M. Bain Address Line 1: One Metropolitan Square, 16th Floor Address Line 2: Senniger Powers Address Line 4: St. Louis, MISSOURI 63102											
NAME OF SUBMITTER:	Robert M. Bain										
Total Attachments: 1 source=00003353#page1.tif											



500034342

PATENT
REEL: 016095-FRAME: 0930

17

177

PATENT ASSIGNMENT

I/WE, Eric D. Tribble and Trevor W. Freeman ("ASSIGNOR"), have invented subject matter ("INVENTION") disclosed and/or claimed in a patent application entitled "SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL" ("APPLICATION"), which:

☒ will be filed without this executed PATENT ASSIGNMENT. ASSIGNOR hereby authorizes, and requests, ASSIGNEE'S legal representatives, of SENNIGER POWERS, who are associated with customer number 000038779, to insert here in parentheses (U.S. Serial No. 11/07,011, filed 04/15/2005) this APPLICATION's U.S. Serial Number and filing date, when known;

☐ was filed on and was given U.S. Serial No.;

☐ is filed concurrently herewith;

Microsoft Corporation, a Washington Corporation, on behalf of itself and its successors and assigns ("ASSIGNEE"), is entitled to, and is desirous of acquiring, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and all other applications and patents derived therefrom, such as continuing applications, in and for the United States, its territories, and all foreign countries ("APPLICATION DERIVATIVES");

For good and valuable consideration, the receipt of which is hereby acknowledged by the ASSIGNOR, the ASSIGNOR hereby sells, assigns and transfers to the ASSIGNEE, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and APPLICATION DERIVATIVES);

ASSIGNOR agrees to execute all instruments and documents required for the making and prosecution of the APPLICATION (and APPLICATION DERIVATIVES), for litigation regarding letters patent derived therefrom, and for the purpose of protecting and perfecting title to the APPLICATION (and APPLICATION DERIVATIVES).

4/14/05
DATE

4/14/05
DATE

FRACm


Eric D. Tribble

Trevor W. Freeman



RECORDED: 08/08/2005

PATENT
REEL: 016095 FRAME: 0831

15

Nora Jiménez de Adam

178

TRADUCCIÓN DEL INGLÉS AL ESPAÑOL DE CUATRO PÁGINAS DE UN DOCUMENTO ORIGINAL ENTREGADO EN UNA CARPETA DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DEL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS, CON COBERTURA DE PLÁSTIC TRANSPARENTE, REALIZADA POR NORA JIMÉNEZ DE ADAM, TRADUCTORA E INTÉRPRETE OFICIAL. TEL: 571-2572804; FEBRERO 8 DE 2006

"APOSTILLE

(Convención De La Haya de octubre 5 de 1961)

1. País: ESTADOS UNIDOS DE AMÉRICA
2. Este documento público fue firmado por: P. SWAIN
3. En su calidad de: FUNCIONARIO DE CERTIFICACIONES
4. Lleva el sello de: LA OFICINA DE PATENTES Y MARCAS REGISTRADAS

CERTIFICADO

5. En: WASHINGTON, D.C.
6. El día treinta de diciembre de 2005
7. Por: *Asistente del Funcionario de Autenticaciones del Departamento de Estado de los Estados Unidos*
8. No. 06007851-7
9. Sello: SELLO SECO DEL DEPARTAMENTO DE ESTADOS UNIDOS
10. Firma: FERNESIA T. CRAWFORD



SEGUNDA PÁGINA:

Emitida en papelería especial con reborde negro-gris con el número A 1408855 en la parte superior izquierda del documento: **ESTADOS UNIDOS DE AMÉRICA - PARA AQUÉLLOS A QUIENES PUEDA INTERESAR: EL DEPARTAMENTO**

16

DE COMERCIO DE LOS ESTADOS UNIDOS Oficina de Patentes y Marcas Registradas de los Estados Unidos

Diciembre 28 de 2005

ESTE DOCUMENTO CERTIFICA QUE LOS ANEXOS SON COPIA FIEL DEL DOCUMENTO QUE FUE REGISTRADO EN ESTA OFICINA EL DÍA 6 DE JUNIO DE 2005.

Estampilla dorada del Departamento de Comercio - Oficina de Patentes y Marcas Registradas de los Estados Unidos

Bajo la potestad del SUBSECRETARIO DE COMERCIO PARA LA PROPIEDAD INTELECTUAL Y DIRECTOR DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DE ESTADOS UNIDOS

(Firma)

P. SWAIN

Funcionario de Certificaciones

TERCERA PÁGINA: Papel blanco con lo siguiente en el reverso: **CH \$40.00 11107011.**

CESIÓN DE LA PATENTE



Versión Electrónica v1.1

Versión Impresa v1.1

Tipo de Presentación:	Nueva Cesión
Característica de la Transferencia:	Cesión

7

Información de La Parte que Transfiere

Nombre	Fecha de Ejecución
Eric D. Tribble	04/14/2005
Trevor W. Freeman	04/14/2005

Información de la Parte Receptora

Nombre:	MICROSOFT CORPORATION
Dirección:	One Microsoft Way
Ciudad:	Redmond
Estado/País:	WASHINGTON
Código Postal:	98052

Número Total de Propiedades: 1

Tipo de Propiedad:	Número
Número de Solicitud:	1110



CORRESPONDENCIA

Número de telefax: (314) 231- 4342

La correspondencia será enviada por correo de los Estados Unidos si el envío por telefax falla

Teléfono: 3142315400

Correo Electrónico: uspatents@senniger.com

Nombre del Correspondiente: Robert M. Bain

Renglón 1 de la Dirección: One Metropolitan Square, 16th Floor

Renglón 2 de la Dirección: Senniger Powers

Renglón 4 de la Dirección: St. Louis, MISSOURI 63102

7

181

NOMBRE DE QUIEN ENVÍA:	Robert M. Bain
------------------------	----------------

Número de Anexos: 1 Fuente = 00083383#page1.tif
--

500034342

PATENTE

Carrete: 016095; Pantalla: 0930

CUARTA PÁGINA: Con encabezado de fax Apr 14 2005 12:11 FR TO
913142314342 P05/05

No. de Expediente de MS: 311610.02

No. de Expediente de OC: MSFT 5169.1

CESIÓN DE PATENTE

YO/NOSOTROS, Eric D. Tribble y Trevor W. Freeman ("CEDENTES") somos los creadores de un asunto ("INVENTO") revelado y/o reivindicado en una solicitud de patente llamado SISTEMA Y MÉTODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN UNA RELACIÓN SEGURO Y COMPATIBLE ("SOLICITUD") la cual:

☒ Será registrada sin esta CESIÓN DE PATENTE. Los CEDENTES por este documento autorizan y solicitan a los representantes legales del CESIONARIO de Senniger Powers, los cuales están asociados al número de cliente 000038779, la inserción en este paréntesis (No. de serial U.S. 11/107,011, solicitado el 04/15/2005) del No. de Serie US de la SOLICITUD y su fecha de presentación, si esto es conocido;

_ Fue solicitada el _____ y le fue otorgada el No. de Serial U.S. _____;

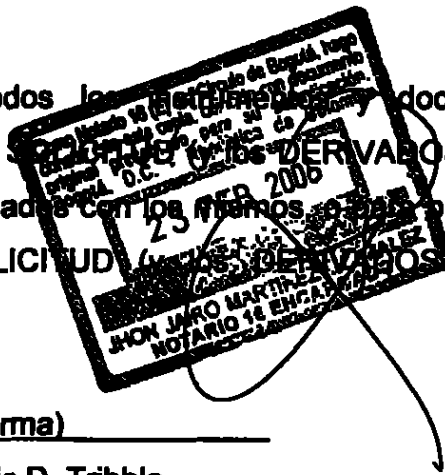
u

_ Se presenta junto con estos documentos;

Microsoft Corporation, una corporación del estado de Washington, en su nombre y en el de sus sucesores y cesionarios ("CESIONARIO") tiene derecho e intenta adquirir la totalidad y la exclusividad de los derechos, títulos e intereses en el INVENTO y la SOLICITUD (y de cualesquiera otra solicitudes y patentes que de éstos se deriven, tales como solicitudes continuas en y para los Estados Unidos, sus territorios y en cualquiera y todos los países extranjeros ("DERIVADOS DE LA SOLICITUD"));

A cambio de contraprestaciones onerosas, el recibo de las cuales se reconocen en este documento por los CEDENTES, éstos por el presente venden, ceden y transfieren al CESIONARIO la totalidad y la exclusividad de los derechos, títulos e intereses en dicho INVENTO y en la SOLICITUD (y en los DERIVADOS DE LA SOLICITUD);

Los CEDENTES acuerdan ejecutar todos los documentos requeridos para elaborar y dar curso a la SOLICITUD (y los DERIVADOS DE LA SOLICITUD) para fines de litigios relacionados con los mismos, así como proteger y perfeccionar dicho título sobre la SOLICITUD (y los DERIVADOS DE LA SOLICITUD).



4/14/05
Fecha

(Firma)
Eric D. Tribble

4/14/05
Fecha

(Firma)
Trevor W. Freeman

FRACwa

PATENTE

✓

✓

Carrete: 016095; Pantalla: 0931

Registrado el 06/06/2005

**CONTRAPORTADA: LOGO DEL DEPARTAMENTO DE COMERCIO DE
ESTADOS UNIDOS – OFICINA DE PATENTES Y MARCAS REGISTRADAS**

CERTIFICO QUE ESTA ES UNA TRADUCCIÓN FIEL DEL INGLES AL ESPAÑOL DE UN DOCUMENTO QUE HE TENIDO A LA VISTA; QUE SOY TRADUCTORA E INTERPRETE OFICIAL ACREDITADA POR RESOLUCIONES 0035 Y 530 DE LA UNIVERSIDAD NACIONAL DE COLOMBIA Y DEL MINISTERIO DE LA JUSTICIA RESPECTIVAMENTE, Y QUE ESTOY REGISTRADA ANTE EL MINISTERIO DE RELACIONES EXTERIORES DE COLOMBIA

Bogotá, febrero 8 de 2006

Nora Jiménez de Adam
NORA JIMÉNEZ DE ADAM
C.C. 20.335.247



184

TRADUCCIÓN DEL INGLÉS AL ESPAÑOL DE UNA PORCIÓN DE UN DOCUMENTO ORIGINAL ENTREGADO EN UNA CARPETA DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DEL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS, CON COBERTURA DE PLÁSTICO TRANSPARENTE, REALIZADA POR NORA JIMÉNEZ DE ADAM, TRADUCTORA E INTÉRPRETE OFICIAL. TEL: 571-2572804; FEBRERO 8 DE 2006

Emitido en papelería especial con reborde negro-gris con el número PA 1409082 en la parte superior izquierda del documento: "ESTADOS UNIDOS DE AMÉRICA - A TODOS LOS BENEFICIARIOS DE ESTE DOCUMENTO: EL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS Oficina de Patentes y Marcas Registradas de los Estados Unidos

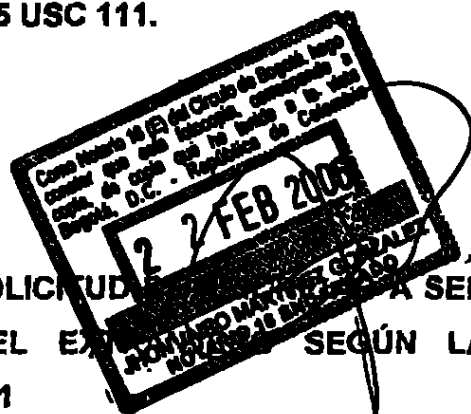
Diciembre 28 de 2005

ESTE DOCUMENTO CERTIFICA QUE LOS ANEXOS SON COPIA FIEL DE LOS DOCUMENTOS REGISTRADOS EN LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DE LOS ESTADOS UNIDOS CORRESPONDIENTES A LA SOLICITUD DE PATENTE IDENTIFICADA A CONTINUACIÓN, QUE CUMPLEN CON LOS REQUISITOS PARA QUE LES SEA OTORGADA UNA FECHA DE REGISTRO DE ACUERDO CON 35 USC 111.

NÚMERO DE SOLICITUD: 11/107,011

FECHA DE REGISTRO: abril 15 de 2005

EL CÓDIGO DE PAÍS Y EL NÚMERO DE SOLICITUD UTILIZADO PARA SU REGISTRO EN EL EXTRANJERO DEBE SER SEGÚN LA CONVENCION DE PARÍS ES EL US11/107.011



22

185

Estampilla dorada del Departamento de Comercio - Oficina de Patentes y Marcas Registradas de los Estados Unidos

Bajo la potestad del SUBSECRETARIO DE COMERCIO PARA LA PROPIEDAD INTELECTUAL Y DIRECTOR DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS

(Firma)

T. WALLACE

Funcionario de Certificaciones

SEGUNDA PÁGINA: Papel blanco con lo siguiente: SELLADO CON LOS NÚMEROS 112948 DEL U.S. PTO - 11/107011, CÓDIGO DE BARRAS 041505. A LA IZQUIERDA: SELLO CON EL NÚMERO 17414 U.S. PTO SEGUIDO DEL CÓDIGO DE BARRAS CON EL NÚMERO 041505.

SENNIGER POWERS

Attorneys at Law - Patent - Trademarks - Litigation - Copyrights - Technology - Antitrust (Abogados - Patentes - Marcas Registradas - Litigios - Derechos de Autor - Tecnología - Monopolios)

One Metropolitan Square

16th Floor

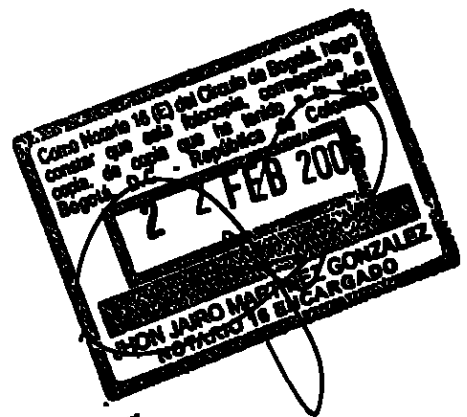
Saint Louis, Missouri 63102

314-231-5400 V

314-231-4342 F

SENNIGER.COM

Frank R. Agovino



Abril 15 de 2005

23

TRANSMISIÓN DE SOLICITUD DE PATENTE DE UTILIDAD

(Para solicitudes nuevas no provisionales, según 37 CFR 1.53 (b))

No. Expediente del Abogado: MS#311610.02 (5169.1)

Nombre Primer Inventor: Eric D. Tribble

Título **SISTEMA Y MÉTODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE**

No. de Etiqueta de Correo Expreso EL 462439036 US

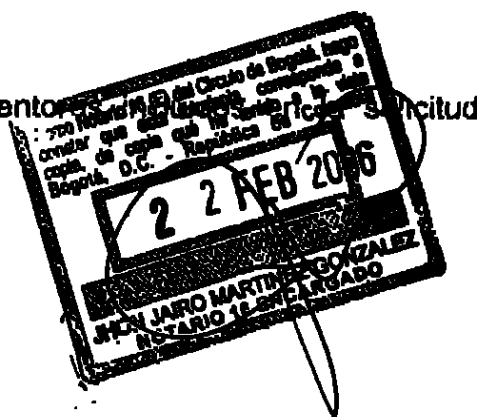
PARA: Comisionado de Patentes

P.O. Box 1450

Alexandria, Virginia 22313 -- 1450

ELEMENTOS DE LA SOLICITUD

1. ☒ Formato de transmisión de honorarios (original y duplicado).
 2. ☐ El solicitante reclama su condición de pequeña entidad.
 3. ☒ Especificación (páginas Totales 26)
 4. ☒ Gráficas (Páginas totales 8)
 5. Juramento o Declaración (Páginas totales 2)
 - a. ☒ (Original o copia) ejecutada
 - ☐ Nueva (sin ejecutar)
 - b. ☐ Copia de una solicitud previa (para continuación/división completar la casilla 19)
 - i. ☐ ELIMINACIÓN DE INVENTOR (ES)
- Declaración anexa firmada eliminando inventor (ES) de la solicitud previa.



Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005

TERCERA PÁGINA:

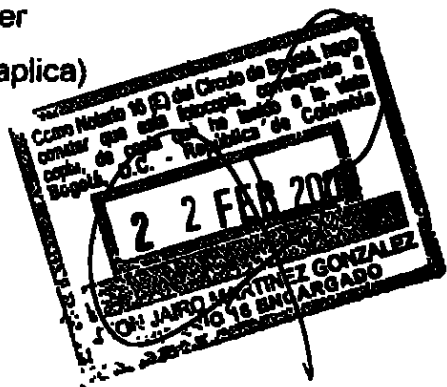
6. ☐ Inclusión por Referencia (utilizable en caso de que la casilla 5b esté señalada)

La revelación completa de la solicitud previa para la cual se proporciona una copia del juramento o de la declaración en la casilla 5b, se considera como parte de la revelación de esta solicitud y queda incluida por referencia por medio del presente.

7. ☒ Ficha técnica de la solicitud
8. ☐ Duplicado de CD-ROM o CD-R, tabla grande o Programa de Computador (Apéndice)
9. ☐ Transmisión de Secuencia de Nucleótido y/o Aminoácido (si aplican, todas las necesarias)
- a. ☐ Formato Legible por el Computador
- b. ☐ Listado de Secuencia de Especificación en:
- i. ☐ CD-ROM o CD-R (2 copias); o
- ii. ☐ Papel
- c. ☐ Declaraciones confirmando identidad de las copias previas.

PARTES COMPLEMENTARIAS A LA SOLICITUD

10. ☐ Papeles de la Cesión (cubierta y documento (s))
11. ☐ 37 CFR 3.73(b) Declaración ☒ Poder
12. ☐ Documento de traducción al inglés (si aplica)
13. ☐ IDS con PTO/SB/O8A
☐ Copias de citas IDS
14. ☐ Enmienda preliminar
15. ☒ Carta de acuse de recibo



188

16. _ Solicitud y Certificación de No Publicación. Se anexa Formato PTO/SB/35
17. _ Copia certificada de Documentos Prioridad en caso de reivindicar prioridad extranjera
18. _ Documento separado identificando los Abogados/Apoderados para ser Nombrados para el Registro
19. _ Otros:

2

**Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005**

CUARTA PÁGINA:

EN CASO DE SER UNA CONTINUACIÓN DE PATENTE, MARQUE LAS CASILLAS APROPIADAS Y SUMINISTRE LA INFORMACIÓN SOLICITADA A CONTINUACIÓN

20. ☐ Continuación ☐ División ☐ Continuación Parcial de solicitud previa
no. _____
- ☒ Solicitud completa según la Solicitud provisional No. 60/659,279, presentada
el 7 de marzo de 2005.

Información de la solicitud previa: Examinó:

DIRECCIÓN DE CORRESPONDENCIA

21. Dirección de Correspondencia: No. de cliente
Atn.: Frank R. Agovino



✓

Respetuosamente,

(Firma)

Frank R. Agovino -Reg. No. 27,416

FRAcwa

3

**Copla suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005**

QUINTA PÁGINA: Papel blanco con lo siguiente a la izquierda: SELLO CON EL
NÚMERO 17414 U.S. PTO SEGUIDO DEL CÓDIGO DE BARRAS CON EL
NÚMERO 041505

TRANSMISIÓN DE GASTOS

No. de Solicitud a ser asignado

Fecha de Presentación Abril 15 de 2005

Inventor (es) Eric D. Tribble et al.

No. de Expediente del Abogado MS#311610.02 (MSFT 5169.1)

☐ El solicitante reivindica condición de entidad pequeña

MÉTODO DE PAGO

☐ El Comisionado queda autorizado por el presente a debitar los gastos de la cuenta de Depósito No. 19-1345. El mismo queda autorizado a acreditar cualquier pago o acreditar cualquier exceso de pago a la Cuenta de Depósito No. 19-1345.



☒ Cheque adjunto. El Comisionado queda autorizado por el presente para debitar

cualquier pago o acreditar cualquier exceso de pago a la Cuenta de Depósito No. 19-1345.

CÁLCULO DE GASTOS

1. ☒ TASA BÁSICA DE PRESENTACIÓN, BÚSQUEDA Y REVISIÓN

(Tipo: Utilidad) Subtotal (1) \$ 1,000.00

2. ☐ TASA POR REIVINDICACIÓN ADICIONAL

Reivindicaciones totales ____ - ____ (HP) = ____ x Tasa ____ = \$ ____

Reivindicaciones indep. ____ - ____ (HP) = ____ x Tasa ____ = \$ ____

Tasa por Múltiples reivindicaciones dependientes \$ ____

(HP= número más alto de reivindicaciones pagadas)

Subtotal (2) \$ ____

3. ☐ TASA POR TAMAÑO DE LA SOLICITUD

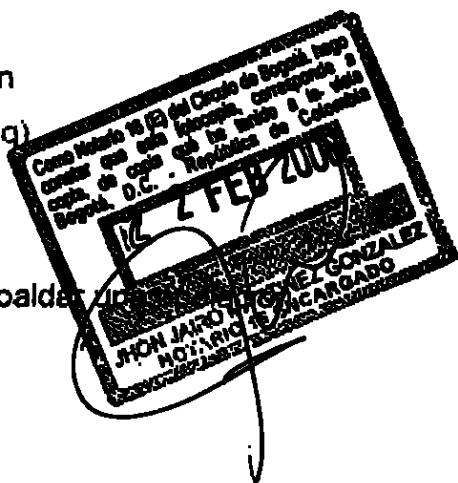
Págs. Totales ____ - 100 = ____ / 50 = ____ x \$250 = \$ ____

(Solicitud y gráficas) (redondear a un número entero)

Subtotal (3) \$ ____

4. ☐ OTRAS TASAS

- ☐ ____ meses de tiempo adicionales
- ☐ Declaración de revelación de información
- ☐ Gastos de procesamiento 37 CFR 1.17 (g)
- ☐ Especificación no en inglés
- ☐ Notificación de apelación
- ☐ Presentación de un documento para respaldar
- ☐ Solicitud para una audiencia oral
- ☐ Otro: _____



Subtotal (4) \$ _____

PAGO TOTAL: \$1,000.00

(Firma) _____ 4/15/05

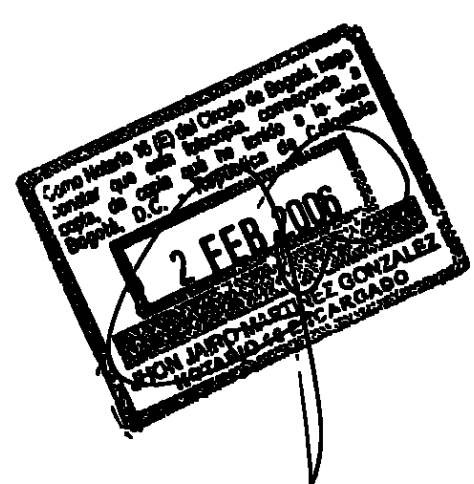
Frank R. Agovino -Reg. No. 27,416 Fecha

Teléfono: 314-231-5400

FRAcwa

No. de Etiqueta de Correo Expreso EV462439036US

**Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005**



SISTEMA Y METODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE

CAMPO TECNICO

[0001] Implementaciones del presente invento se relacionan con el campo de establecer una interconexión compatible entre dos dominios. En particular, implementaciones de este invento se relacionan con un sistema y método para revelar y descubrir servidores de correo con capacidades avanzadas.

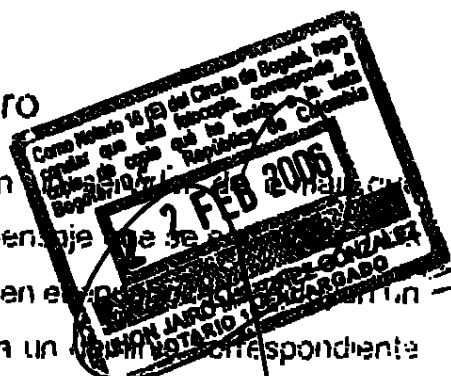
ANTECEDENTES DEL INVENTO

[0002] Algunos sistemas anteriores intentaban identificar al potencial correspondiente comunicándose directamente. Sin embargo, estos sistemas se hacían vulnerables a atacantes cuando se comunicaban, y en particular, podían ser causa o ser vulnerables al SPAM y a ataques de negación de servicio.

[0003] De esta manera, se hace deseable un sistema que enfrente estas y otras desventajas identificando en forma discreta a un potencial correspondiente de tal manera que un vínculo seguro entre un servidor y el potencial correspondiente se pueda establecer.

RESUMEN DEL INVENTO

[0004] Implementaciones del invento incluyen ocasionalmente añadir un encabezado adicional al mensaje de correo electrónico de los dominios potenciales del correspondiente. Los datos en el encabezado son un código que es específico al mensaje que se envía a un dominio potencial y una dirección de correo e-mail a la cual se pueden dirigir los mensajes administrativos de ese correspondiente al servidor. Si el correo en el dominio potencial también se dirige a través de un servidor como el de esta



implementación entonces detectará los mensajes recibidos y determinará que hay más servidores compatibles en el dominio que origina. Puede entonces enviar el tráfico administrativo, tal como solicitudes para establecer una conexión segura, a la dirección administrativa contenida. Este mensaje administrativo también debe contener el secreto que le fue suministrado para ese dominio correspondiente. El receptor para el correo administrativo en el dominio que origina puede entonces descartar cualquier correo que pretenda ser del dominio correspondiente pero que no tiene el secreto asociado al dominio del correspondiente.

[0005] En una implementación, el invento incluye un método para determinar que un dominio correspondiente potencial tiene tecnología de e-mail compatible y segura para establecer un vínculo entre el dominio fuente y el dominio correspondiente. Un secreto de descubrimiento se transmite del dominio fuente al dominio correspondiente. El Secreto de descubrimiento incluye un elemento de datos específico al dominio del correspondiente y una dirección del dominio fuente a la cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad entre el dominio fuente y el dominio correspondiente. El dominio fuente recibe a través de la dirección del dominio fuente una invitación del dominio correspondiente. La invitación incluye un elemento de datos o un elemento correspondiente al elemento de datos que el dominio correspondiente puede utilizar para iniciar el proceso para establecer la compatibilidad con el dominio correspondiente.

[0006] De acuerdo con un aspecto del invento, se administra para que un secreto de descubrimiento se transmita a un dominio correspondiente para establecer que el dominio fuente tiene tecnologías de e-mail compatibles con tecnologías de e-mail comunicaciones. El Secreto de descubrimiento incluye un mensaje un encabezado que se relaciona con el mensaje y un encabezado



adicional anexo al mensaje. El encabezado adicional incluye (1) un elemento de datos específico al dominio correspondiente e incluye una dirección del dominio fuente al cual se le permite al dominio correspondiente enviar un mensaje al dominio fuente para establecer que el dominio correspondiente y dominio fuente tienen tecnologías de e-mail seguras y compatibles, (2) un secreto de descubrimiento y (3) una fecha de vencimiento.

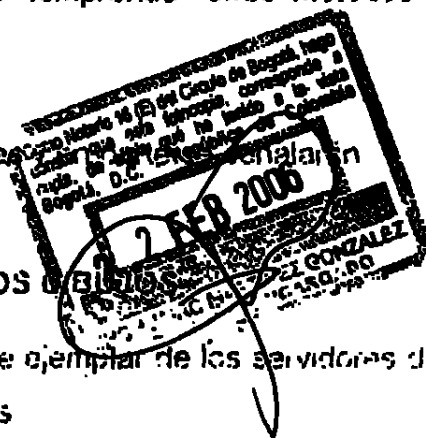
[0007] En otra forma, el invento comprende un sistema para establecer que un correspondiente y un dominio fuente tienen tecnología de e-mail compatible y segura u otra tecnología de e-mail o comunicaciones. Un servidor dominio fuente transmite un secreto de descubrimiento al dominio del correspondiente. El secreto de descubrimiento incluye un elemento de datos específico al dominio del correspondiente y una dirección del dominio fuente a la cual al dominio del correspondiente se le permite enviar un mensaje para establecer que el correspondiente y el dominio fuente tienen tecnologías de e-mail compatibles y seguras. Un computador del dominio correspondiente recibe el secreto de descubrimiento incluido en el elemento de datos y la dirección del dominio fuente. El Computador del dominio correspondiente transmite una invitación del dominio del correspondiente a la dirección del dominio fuente. La invitación incluye un elemento de datos o un elemento correspondiente al elemento de datos.

[0008] En forma alterna, el invento puede comprender otros métodos y aparatos varios.

[0003] Otros rasgos en parte serán aparentes.

DESCRIPCIÓN BREVE DE LOS OBJETOS

[0010] La figura 1 es un diagrama de bloque ejemplar de los servidores de red 1 y 2 con una mensajería segura entre ellos.



[0011] La figura 2 es un diagrama de flujo que muestra el flujo de trabajo entre un servidor de dominio fuente y un correspondiente potencial (por ejemplo, un servidor de dominio correspondiente) de acuerdo con el invento.

[0012] La figura 3 es un diagrama de bloque ejemplar que muestra un administrador de mensajes seguro de acuerdo con el invento.

[0013] La figura 4 es un diagrama de flujo que muestra la operación de búsqueda de ruta de la Administración de mensajes segura (SMM) de acuerdo con el invento.

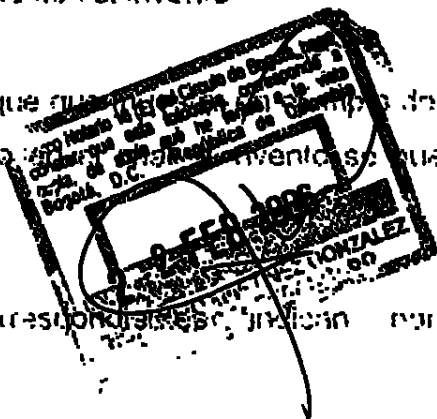
[0014] La figura 5 es un diagrama de flujo que muestra las operaciones de búsqueda de ruta de un trabajador SMM de acuerdo con el invento.

[0015] La figura 6 es un diagrama de bloque ejemplar que muestra un resumen del flujo de trabajo inter-organización entre un servidor (administración A) y un correspondiente (administración B) de acuerdo con el invento.

[0016] La figura 7 es un diagrama de flujo que muestra un diagrama de estado luego de que una nueva asociación de seguridad se ha implementado entre un servidor y un correspondiente de acuerdo con el invento.

[0017] La figura 8 es un diagrama de bloque que muestra un diagrama de un ambiente de sistema de computación adecuado para implementar el invento.

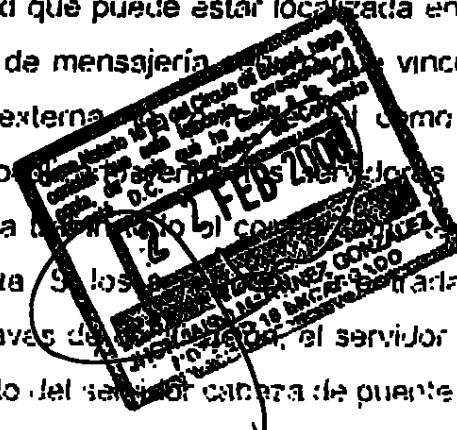
[0018] Caracteres de referencia correspondientes indican partes correspondientes a través de todos los dibujos.



DESCRIPCIÓN DETALLADA DEL INVENTO

[0019] El invento se relaciona con un sistema y método para determinar que un correspondiente potencial tiene tecnología de e-mail compatible y segura para comenzar el proceso de establecer un vínculo entre el servidor y el correspondiente. En particular, el invento se relaciona con un sistema y método para iniciar el proceso de establecer un vínculo seguro para el despliegue de e-mail seguro. El invento le permite a un servidor determinar que un correspondiente potencial se puede establecer como un objetivo porque la tecnología de e-mail es compatible y segura. Como resultado, una vez se identifica al correspondiente potencial, el servidor puede intercambiar información de material clave con el correspondiente potencial para establecer un vínculo seguro.

[0020] El objetivo de la firma y codificación del dominio de acuerdo con el invento es suministrar un mecanismo de transporte independiente para intercambiar mensajes confidenciales y autenticados por el servidor entre los servidores. La figura 1 es un diagrama de bloque ejemplar de los servidores de entrada 1 y 2. Los servidores 1 y 2 tienen un vínculo de mensajería seguro entre ellos. El servidor puede estar separado por una firewall opcional a través del cual pueden estar conectados a servidores cabeza de puente (que no se muestran), que pueden ser parte de un sistema de mensajería seguro y separado. Los servidores de entrada 1 y 2 forman una sub-red que puede estar localizada entre una red interna confiable, tal como el sistema de mensajería seguro, y una red externa, tal como la Internet pública. Los firewalls también están localizados entre los servidores de entrada y la Internet. Los servidores de entrada 1 y 2 codifican todo el correo puerta a puerta. Si los servidores cabeza de puente no comparten las mismas llaves de codificación, el servidor de entrada no puede decodificar el correo codificado del servidor cabeza de puente.

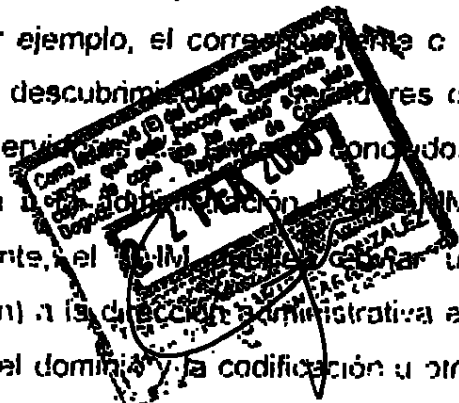


0

o de trabajo ocurrido en el mes de febrero de 2006. El servidor indica que no ha sido sancionado por el jefe de la oficina de trabajo.

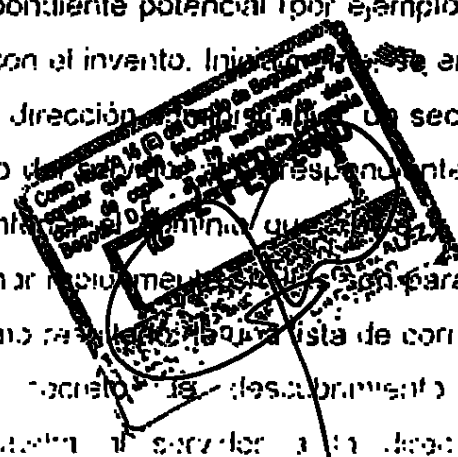
minimizar que el proceso del secreto de descubrimiento sea vulnerable a un ataque, el sistema y método del invento no utiliza una dirección codificada en duro en su secreto de descubrimiento. Sin embargo, se considera que en una implementación una dirección única se puede utilizar con el secreto de descubrimiento para que se incluya en cualquier e-mail para esa dirección. Como resultado, únicamente los mensajes de las partes que han visto el secreto de descubrimiento (que incluye el secreto de descubrimiento) pueden enviar a la dirección administrativa. Por lo tanto, en una implementación preferida, se utiliza una dirección única, y el secreto de descubrimiento se debe suministrar en todos los mensajes. En forma alterna, la dirección indicada es un nombre de casilla de correo aleatorio que puede rotar con un intervalo razonable, por ejemplo, semanalmente. Mientras que este enfoque aleatorio es una opción, es una implementación menos preferida. Para asegurar que la vulnerabilidad se minimiza, el secreto de descubrimiento está ligado al dominio que envía, por ejemplo, el dominio fuente, y al dominio al que le envía, por ejemplo el dominio correspondiente. En el evento de que el secreto de descubrimiento esté disponible para un tercer partido el único dominio que se afectaría es el dominio cuya dirección de invitación estaba comprometida.

[0024] De una manera, el secreto de descubrimiento puede ser un encabezado 822 que contiene la dirección efímera 822 para negociar y la fecha de vencimiento de la dirección 822 relativa a cuando el mensaje se envió. El correo entrante lo escanea el servidor que recibe (por ejemplo, el correo que entra al servidor del correspondiente) para secretos de descubrimiento y los compara con los de entrada y los compara contra una lista de servicios de descubrimiento conocidos. Cualquier adición a esa lista se les comunica a los administradores de SMM. Cuando se descubre un nuevo correspondiente, el SMM genera un mensaje de pruebas (por ejemplo, una invitación) a la dirección administrativa en el otro SMM para ofrecer un turno en la firma del dominio y la codificación u otro servicio. Cuando se recibe una invitación de otro administrador SMM se el



mensaje se puede verificar bajo la política de confiabilidad existente entonces el SMM local puede invocar una política para automáticamente aceptar la invitación. En forma alterna, el administrador SMM pueden requerir de una aprobación manual antes de aceptar la invitación. Tan pronto se recibe la aceptación de la invitación por el servidor, si el mensaje es intrínsecamente verificable, entonces el SMM que recibe podría invocar una política para automáticamente iniciar el uso de la firma y codificación del dominio. Primero envía un mensaje de prueba codificado con un número aleatorio único y espera un reconocimiento (que incluye el número aleatorio único) para asegurarse que el correo seguro se puede decodificar al otro lado. Nótese que la invitación y mensaje de aceptación están firmados con una llave autoritaria del SMM, mientras que en el mensaje de prueba y el reconocimiento están firmados con una llave de firmas (que es un hijo de la llave autoritaria). El proceso rutinario que firma y codifica el correo sólo tiene la autoridad de firmar con la llave de firmas (por seguridad). Por lo tanto, el correo de prueba y el reconocimiento también verifican que un correo seguro va a funcionar con la llave de firma, no únicamente con la llave autoritaria. La configuración de un nuevo dominio seguro es un proceso no sincronizado y no se utiliza para datos reales hasta que el vínculo se confirme operacional con la recepción del reconocimiento del mensaje de prueba antes de hacer anuncios administrativos.

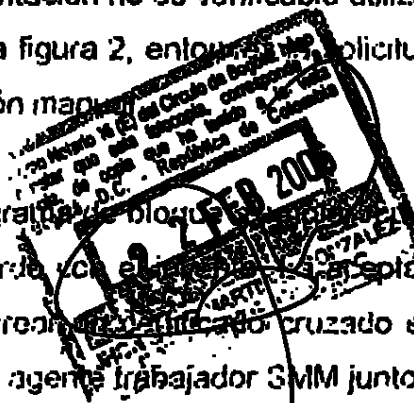
[0025] La figura 2 es un diagrama ejemplar que muestra el flujo de trabajo entre un servidor dominio fuente y un correspondiente potencial (por ejemplo, un computador de dominio objetivo) de acuerdo con el invento. Inicialmente, se envía un secreto de descubrimiento que incluye una dirección de correo electrónico, un secreto de descubrimiento y una fecha de vencimiento del secreto de descubrimiento. El secreto de descubrimiento también debe contener una dirección de correo electrónico que se puede utilizar para determinar si el secreto de descubrimiento es válido para su uso, porque ellos pueden haber sido como resultado de una vista de correo. Cuando el correspondiente reconoce el secreto de descubrimiento, el correspondiente envía una invitación de correo al servidor a la dirección



38

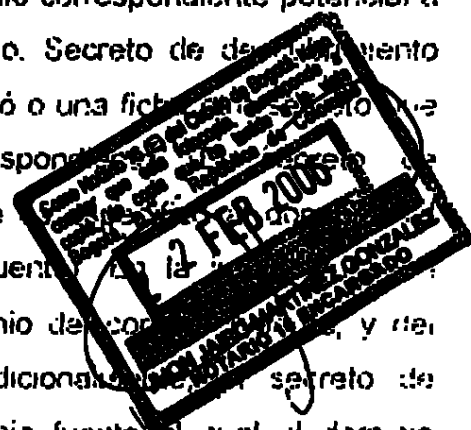
administrativa que era parte del secreto de descubrimiento. En una implementación, sólo responde al descubrimiento si también ha enviado correo "al" dominio. Por lo tanto un spammer no puede inducir al dominio fuente a que lo invite (porque usted, para comenzar, nunca les envió correo). La invitación del correspondiente incluye una dirección administrativa del correspondiente, una fecha de vencimiento, un certificado y el secreto de descubrimiento y otra información (por ejemplo, el Id del flujo de trabajo, información del contacto, dominios de envío y recibo, etc.). En respuesta, el servidor envía una aceptación a la dirección administrativa del correspondiente de la dirección administrativa del servidor e incluye en la aceptación la fecha de vencimiento, el certificado, el secreto de descubrimiento y una firma. Esta es una opción administrativa, aunque la política por defecto puede incluir una respuesta automática. En una implementación, se puede restringir a un funcionamiento manual, o únicamente responder si la certificación del que invita cumple cierta política de confiabilidad. Luego de que se recibe la aceptación, el correspondiente envía un mensaje de prueba al servidor y el mensaje de prueba lo reconoce el servidor para establecer la conexión que pone a la asociación en estado de alerta. Puede involucrar una acción administrativa automática para avanzar del estado de alerta al estado activo. Puede involucrar un paso adicional para pasar del estado activo (que utiliza la relación segura pero no la crea) al estado autenticado (que cree en la identidad que asegura el otro partido). Si el mensaje de invitación no es verificable utilizando la política de confiabilidad como se mostró en la figura 2, entonces la solicitud se puede poner en cola en espera de una aprobación manual.

[0026] En referencia a la figura 3, un diagrama de flujo muestra un administrador de mensajes seguros de acuerdo con el flujo de la invitación por el correspondiente puede crear un certificado cruzado en el agente administrativo SMM que luego lo envía al agente trabajador SMM junto con el certificado de codificación. (El certificado cruzado se crea generalmente para asociaciones autenticadas (para poder definir lo que ellas pueden autenticar). Las



asociaciones activas lo tienen todo ejemplo el certificado cruzado. El certificado cruzado restringe el conjunto de nombres que la nueva confianza permite / la restricción de la comunicación con el dominio del servidor de entrada. En este punto, se distribuye a todos los trabajadores los certificados e información en cuanto a la nueva asociación. También se puede distribuir la llave de la sesión de la administración SMM a todos los trabajadores SMM de tal manera que todos los trabajadores utilicen la misma llave para reducir el tamaño de la memoria cache. Para permitir el escalamiento, la llave privada de de codificación correspondiente para el certificado de codificación debe estar disponible en todo el Internet de frente a los servidores de entrada para permitir la decodificación del correo entrante. Esto se genera en un solo sitio, por ejemplo, el agente administrador, y se distribuye a todos los trabajadores del servidor. Una vez que se establece una relación de confianza, se debe mantener. Por ejemplo, el certificado original se puede retener y una solicitud de renovación enviarse al otro SMM antes de que el certificado venza. El certificado hijo de firma y codificación también se puede actualizar frecuentemente.

[0027] Vez en la perspectiva del servidor, el método de acuerdo con el invento comienza el proceso para establecer un vinculo entre un dominio fuente y un dominio correspondiente. Inicialmente, un servidores de dominio fuente transmite un secreto de descubrimiento a un dominio correspondiente potencial a través de un mensaje aleatorio o pseudo aleatorio. Secreto de descubrimiento incluye un elemento de datos tal como se mencionó o una ficha de registro que se asigna específicamente al dominio correspondiente. El secreto de descubrimiento incluye un secreto compartido que se genera en el dominio fuente y el dominio correspondiente (y posiblemente al dominio frecuente). La información de la profunda, es una porción de la semilla, del dominio de correspondiente, y del dominio fuente (en algún orden específico). Adicionalmente, el secreto de descubrimiento incluye una dirección en el dominio fuente al cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad.



entre el servidor del dominio fuente y el computador objetivo. El servidor del dominio fuente recibe una invitación del dominio correspondiente, invitación que está dirigida a la dirección del dominio fuente que se había suministrado previamente. La invitación incluye un elemento de datos en el secreto de descubrimiento o un elemento correspondiente al elemento de datos en el secreto de descubrimiento. Esto permite que el servidor del dominio fuente inicie un proceso para establecer la compatibilidad entre el servidor del dominio correspondiente y el servidor del dominio fuente tan pronto recibe el servidor del dominio fuente una invitación del servidor del dominio correspondiente. Como se anotó en la figura 2, el servidor del dominio fuente transmite al servidor del dominio correspondiente una aceptación para establecer la compatibilidad entre los dos.

[0028] En una implementación, el dominio fuente transmite en forma selectiva el secreto de descubrimiento a dominios correspondientes de donde el dominio fuente ha enviado el mensaje. Forma alterna o adicionalmente, el dominio fuente puede enviar un secreto de descubrimiento a dominios correspondientes que sean identificado anteriormente.

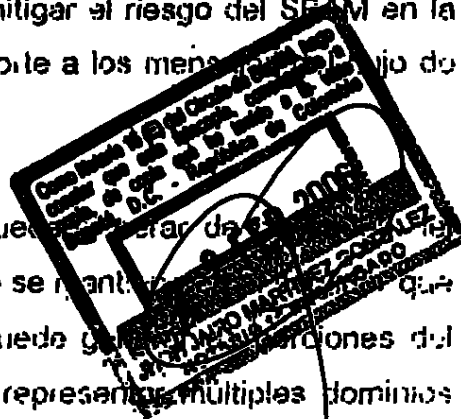
[0029] En una implementación, el secreto de descubrimiento puede estar anexo al mensaje que se envió específicamente para llevar el secreto de descubrimiento. En una implementación del invento, un servidor de e-mail ocasionalmente añade un encabezado adicional (un "x-head") al mensaje que se va a distribuir a otro dominio e-mail. Los datos en el encabezado incluyen un secreto que es específico al dominio del correspondiente, el dominio al cual el mensaje administrativo del dominio correspondiente se dirige de vuelta al servidor de e-mail, como también incluyen la dirección de correo electrónico al dominio del correspondiente, el dominio del remitente, un correo electrónico adicional, y rasgos adicionales. Si el correo en el dominio del correspondiente también se dirige a través de un servidor que implementa este invento, entonces podrá detectar el



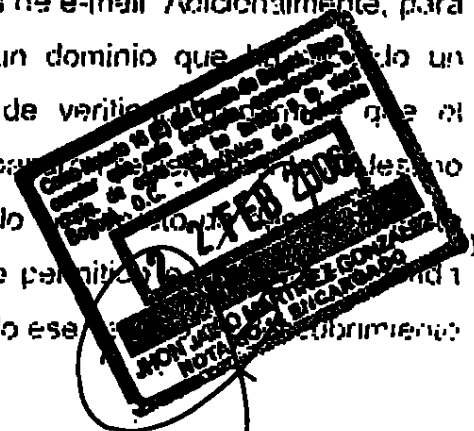
encabezado adicional y determinar que puede haber un servidor compatible en el dominio que origina. El dominio del correspondiente entonces dirige el tráfico administrativo tales como, la petición para establecer una conexión segura, a la dirección de e-mail administrativa contenida. El controlador de correo para el correo administrativo en el dominio que origina puede entonces descartar cualquier correo que pretende ser del dominio del correspondiente pero que no contiene el secreto correspondiente al dominio del correspondiente. Aunque esto no suministra una seguridad absoluta de que el correo administrativo que se recibe es del dominio que origina, si minimiza la vulnerabilidad al SPAM en la dirección administrativa y asegura que un atacante que puede ver los e-mails para el dominio correspondiente únicamente puede intentar imitar la dirección administrativa del dominio del correspondiente a diferencia de cualquier dominio.

[0030] En una implementación, el invento se incrementa utilizando un encabezado, llamado un secreto de descubrimiento (llamado a veces también una mención), que se anexa aun e-mail saliente del dominio fuente. Este secreto de descubrimiento revela la disponibilidad de una función especial en el servidor de correo que origina el e-mail saliente mientras evita la necesidad para generar mensajes adicionales y posiblemente no deseables. Como se anoto anteriormente, la dirección de e-mail administrativa estarían incluidas en la mención y habría un secreto por-dominio para mitigar el riesgo del SPAM en la dirección de e-mail administrativa. Esto daría soporte a los mensajes de trabajo en la dirección de e-mail administrativa.

[0031] El secreto de descubrimiento se puede generar de un dominio correspondiente y una semilla secreta que se mantiene en el dominio que origina. Secreto de descubrimiento también se puede generar de las direcciones del dominio fuente, porque términos servidor puede representar múltiples dominios fuente. Una implementación podría potencialmente tener una 'fuente' para todos los dominios en el servidor fuente. Esto permite en una semilla única se compartida



a través de múltiples servidores de tal manera que cada servidor va a generar términos secreto de descubrimiento único a cualquier dominio correspondiente. Cuando un mensaje administrativo se recibe en el servidor que origina (porque está dirigido a la dirección administrativa incluida en la mención), el secreto de descubrimiento suministrado en el mensaje administrativo es chequeado por el servidor que origina. Para chequear el secreto de descubrimiento, el servidor de e-mail pueden generar (o almacenar) un secreto de descubrimiento para el dominio que envió el mensaje administrativo utilizando la semilla interna actual. Si el secreto de descubrimiento generado es mismo que el secreto en el mensaje administrativo, entonces ese mensaje tiene el secreto de descubrimiento correcto y pasa a través a su destino apropiado para la negociación de mensajes. La negociación de los mensajes se pasa entre dominios. Si el secreto de descubrimiento no concuerda, entonces el mismo proceso se aplica a secretos de descubrimiento anteriores (hasta un número limitado). Sin ninguna de las semillas actuales válidas se puede utilizar para generar el secreto de descubrimiento que concuerda con el secreto de descubrimiento en el mensaje entrante, entonces el mensaje no se considera válido y se descarta o se rechaza, y no se pasa a su destino eventual para los mensajes administrativos. Esto previene ataques de SPAM no autorizados contra el receptor del mensaje administrativo, que puede no ser capaces de hacer frente a volúmenes grandes de e-mail. Adicionalmente, para prevenir ataques de negación de servicio de un dominio que ha aceptado un secreto de descubrimiento válido, el proceso de verificación que el servidor mantenga la pista de cuantos mensajes para un dominio particular o utilizando un dominio particular. Cuando ese número excede un límite permitido, los mensajes administrativos adicionales utilizando ese secreto de descubrimiento se descartan o se rechazan.

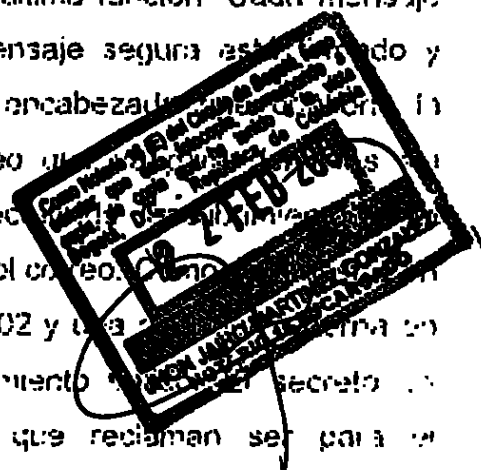


[0032] La figura 4-3 de drama de flujo se muestra las operaciones de la secuencia de ruta administrativa del SAM de acuerdo con el evento 1.

205

verificación de firma y la decodificación debe suceder antes que el proceso anti-SPAM por qué la salida de la verificación es necesaria para fijar las banderas de propiedad del mensaje utilizadas por el agente anti-SPAM. La verificación de firmas debe suceder después del estado de bloque y otras funciones a nivel del protocolo de dirección o IP por lo tanto, el proceso comienza recibiendo mensajes en la dirección del dominio fuente al cual dominio correspondiente se le permite enviar un mensaje en 402. Si se determina en 404 el secreto de descubrimiento no es válido para el dominio que envía, el mensaje se abandona en 406 y la búsqueda de ruta termina. Si el secreto de descubrimiento es válido, el proceso procede a 408 para determinar si el dominio tiene una cantidad máxima o una tasa que se haya excedido. Si el máximo será excedido, el mensaje se descarta en 406, de lo contrario, si la firma es válida en 410 el mensaje se envía al agente administrador local. Sin embargo, la verificación de firma no necesariamente sucede en el trabajador, generalmente sucede en el SMM.

[0033] La figura 5 es un diagrama del flujo que demuestra las operaciones de búsqueda de ruta de un trabajador SMM de acuerdo con el invento. El SMM es el Administrador de Mensajería Segura; los trabajadores son los servidores que el SMM administra/controla y que hacen el procesamiento del tráfico de correo. La firma y codificación del SMM es generalmente la última función. Cada mensaje que va a un dominio con una asociación de mensaje segura está firmado y codificado. Este componente también inserta el encabezado de dirección efímera actual SMM para todo el correo que va a una asociación de seguridad. El trabajador le añadirá un secreto de descubrimiento apropiado pero no lo hace sólo para asegurar el correo. Como se muestra en la figura 5, el dominio busca una firma válida en 502 y una dirección efímera en 504 luego de encontrar un secreto de descubrimiento válido. El secreto de descubrimiento sólo se chequea en mensajes que reclaman ser para una asociación de seguridad, no en correo normal si la firma es válida y no hay dirección efímera el mensaje se envía al agente trabajador local en 506. Si hay una

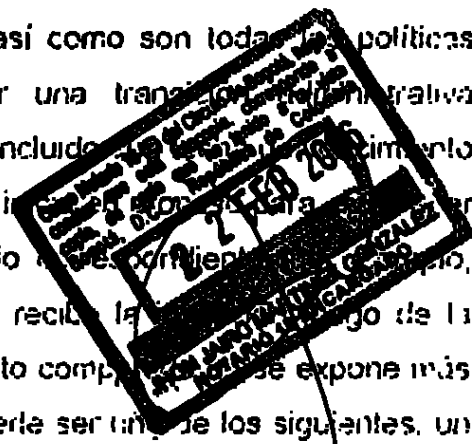


43

dirección externa se envía a ella. Si el mensaje aparece con el dominio asegurado una firma inválida se trata en forma idéntica a como si la firma no estuviera presente. La fuente del mensaje no se autentica.

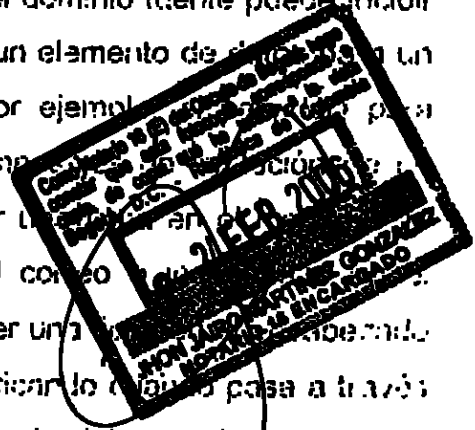
[0034] En una implementación, el flujo de trabajo inter organización como se muestra en las figuras 6 está implementado entre organizaciones administrativas que representan el ciclo de vida de la relación. Otros giros son posibles: las llaves tienen certificaciones asociadas a ellas. Las certificaciones pueden o para con más frecuencia que las llaves. Hay firmas, codificación, certificaciones de autoridad y llaves, todas las cuales rotan en forma independiente. También, puede haber más tarde secuencias de reconocimiento/pruebas. El flujo de trabajo lo ejecuta el agente administrativo SMM y puede tener un intercambio para lograr una rotación (la rotación es el término para la actualización a una nueva llave o certificado). La figura siguiente es un diagrama de estado que muestra la nueva asociación de seguridad. Este diagrama únicamente considera los casos positivos y terminales. No incluye otros aspectos tales como la re-transmisión de mensajes antes del límite de re-transmisión.

[0035] Otros rasgos opcionales del invento incluye en lo siguiente que se puede implementar en forma separada o en combinación. La distinción entre asociación activa y autenticada es "opcional", así como son todas las políticas distintas que se pueden aplicar para hacer una transición administrativa automática. El secreto de descubrimiento puede incluirse en el elemento de descubrimiento y entre el caso de servidor del dominio fuente no incluye el caso de cliente del dominio destino. La compatibilidad con el computador del dominio destino puede ser por el elemento de descubrimiento, servidor) cuando el servidor del dominio fuente recibe la información de descubrimiento de la fecha de vencimiento de tal manera que el secreto compartido se expone más y más sobre el tiempo. El elemento de datos puede ser uno de los siguientes, un secreto por dominio que incluye un número aleatorio o pseudo aleatorio para criptografía.



201

computador del dominio correspondiente (por ejemplo, el servidor) un secreto generado con una porción del computador del dominio correspondiente (por ejemplo, el servidor) y una semilla de secreto que se utiliza para generar secretos por dominio para más de un dominio, y un secreto por dominio generado codificando el computador del dominio correspondiente (por ejemplo, el servidor) y una fecha de vencimiento del secreto. El elemento de datos puede incluir el secreto en cuyo caso el servidor del dominio fuente puede recordar el secreto o puede verificar el secreto recibido del computador del dominio del correspondiente (por ejemplo, el servidor) re-computando y luego comparando el secreto actual para el computador del dominio correspondiente (por ejemplo, servidor) con el secreto incluido en el secreto de descubrimiento. El elemento de datos se puede seleccionar de una pluralidad de secretos múltiples que son válidos en tiempos que se sobrepone para cada computador del dominio del correspondiente (por ejemplo, el servidor) de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación de un computador de el dominio correspondiente (por ejemplo, el servidor) a la dirección administrativa del dominio que origina. Se puede imponer un límite en el número de mensajes que se le pasan a la dirección del servidor del dominio fuente con un elemento de datos particular del tal manera que la negación de ataques al servicio utilizando un elemento de datos correcto se mitiga. El servidor del dominio fuente puede incluir la habilidad de sobrepasar los requerimientos para un elemento de datos a un computador del dominio correspondiente (por ejemplo, el servidor) para permitir la autorización fuera-de-banda de enviar mensajes a la dirección de el dominio particular. El elemento de datos puede ser un secreto de descubrimiento en un encabezado del correo electrónico del mensaje o el elemento de datos puede ser una clave de cifrado del correo y el cuerpo del mensaje puede ser codificado cuando pasa a través de un servidor de correo. El servidor fuente de dominio puede soportar los múltiples secretos de descubrimiento y claves en forma simultánea para el correo electrónico y verificar en mensaje de Internet la subdominios del computador a la

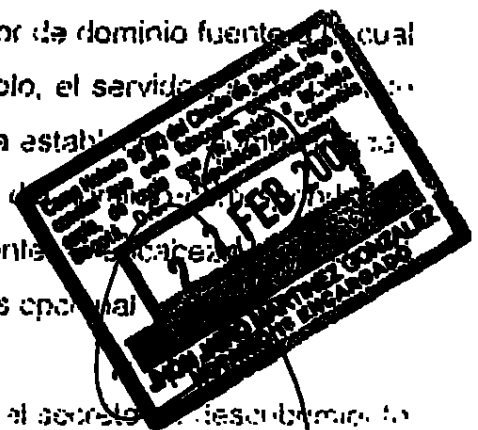


25

208

dominio correspondiente (por ejemplo, el servidor) verificando el secreto de descubrimiento entrante contra secreto de descubrimiento para el computador del dominio correspondiente (por ejemplo, el servidor). El elemento de datos puede ser un secreto de descubrimiento e incluir información de la versión para el servidor dominio fuente e incluir las funciones que el servidor dominio fuente soporta.

[0036] En una implementación el invento comprende una estructura de datos para qué secreto de descubrimiento se transmita de servidor dominio fuente al computador del dominio correspondiente (por ejemplo, el servidor). Como se anotó anteriormente, este secreto de descubrimiento se utiliza para establecer la compatibilidad entre servidor de dominio fuente y el computador de dominio correspondiente (por ejemplo, el servidor). En forma alterna, se podría utilizar para otros propósitos entre los dos dominios. Por ejemplo, se podría utilizar para que se acordaran de acuerdo en enviar un formato propietario (NEF en niveles de texto o HTML) que no tendría nada que ver con codificación o seguridad. La estructura de datos incluye un mensaje y su encabezado usual relacionado con el mensaje. Adicionalmente, la estructura de datos incluye un encabezado adicional anexo al mensaje y un encabezado de mensaje que incluye elementos de datos específicos al computador del dominio correspondiente (por ejemplo, el servidor) el encabezado también incluye una dirección del servidor de dominio fuente al cual computadora del dominio correspondiente (por ejemplo, el servidor) puede enviar un mensaje al servidor del dominio fuente para establecer comunicación entre el servidor del dominio fuente y el computador del dominio correspondiente (por ejemplo, el servidor). Como se anotó anteriormente, el encabezado debe incluir una fecha de vencimiento, aunque esto es opcional.



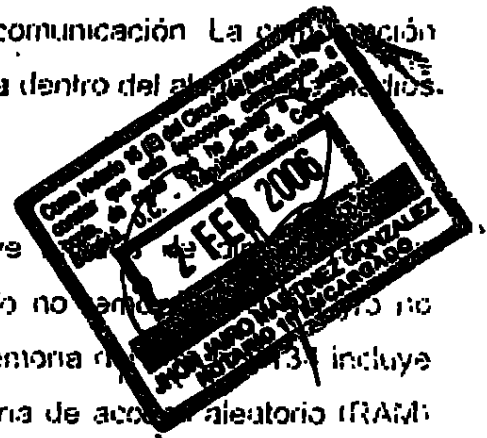
[0037] Adicionalmente como en forma alternativa, el secreto de descubrimiento puede ser un mensaje con un dominio correspondiente único y/o un mensaje a un dominio correspondiente que es un servidor. El mensaje único al dominio

ul

209

ser cualquier medio disponible que el computador 130 pueda acceder. Como ejemplo y no como limitante, el medio legible por computador comprende los medios de almacenaje en computador y medios de comunicación. Los medios de almacenaje en computadoras incluyen los volátiles y no-volátiles, removibles y no-removibles incrementados en cualquier tecnología o método para almacenar información tal como instrucciones legibles por computador, estructuras de datos, módulos de programa u otros datos, por ejemplo, los medios de almacenaje en computador incluyen RAM, ROM, EEPROM, memorias flash y otras tecnologías de memoria, CD-ROM, discos versátiles digitales(DVD) u otros medios de almacenaje en discos ópticos, cassettes magnéticos, cintas magnéticas, almacenaje en discos magnéticos u otros dispositivos de almacenaje magnético, u otros medios que se puedan utilizar para almacenar la información deseada y que el computador 130 pueda acceder. Los medios de comunicación típicamente constan de instrucciones legibles por computador, estructuras de datos, módulos de programas, u otros datos en señal de datos modulada tales como ondas transportadoras u otros medios de transporte mecánico e incluyen cualquier medio para distribuir información. Aquellos diestros en el arte están familiarizados con la señal de datos modulada, que tienen una o más de sus características fijas o alterados de tal manera que codifican la información en la señal. Los medios alambreados, tales como redes alambreadas o conexiones alambreadas en forma directa, y medios inalámbricos, tales como acústicos, RF, infrarrojos, y otros medios inalámbricos son ejemplos de medios de comunicación. La combinación de cualquiera de los anteriores también está incluida dentro del alcance de los medios legibles por computador.

[0040] La memoria del sistema 134 incluye un computador en la forma de memoria removible y/o no removible. En la implementación que se muestra, la memoria del sistema 134 incluye la memoria de sólo lectura (ROM) 136 y la memoria de acceso aleatorio (RAM) 138. Un sistema básico de entrada/salida (BIOS) que contienen las rutinas



210

13

Q

۴

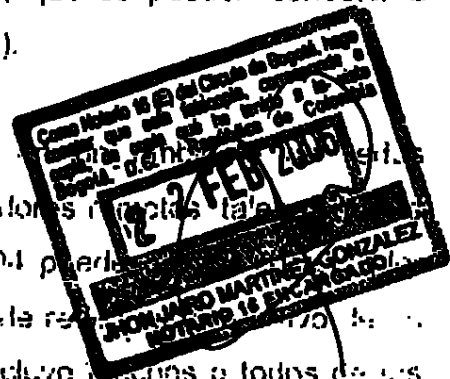


3

módulos de programa 174, y datos de programa 176. Nótese que estos componentes pueden ser iguales a o diferentes al sistema operativo 144, programas de aplicación 146 y otros módulos de programa 148, y datos de programa 150. El sistema operativo 170, los programas de aplicación 172, otros módulos de programa 174, y datos de programa 176 tienen distintos números para mostrar que, por lo menos, son copias distintas.

[0043] Un usuario puede entrar comandos e información en el computador 130 a través de dispositivos de entrada o dispositivos de selección en la interfase del usuario, tal como un teclado 130 y dispositivos de señalamiento 132 (por ejemplo ratón, trackball, un bolígrafo o una almohadilla táctil). Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, un joystick, un panel de juegos, un disco satelital, un escáner, o cosas parecidas. Estos y otros dispositivos de entrada están conectados a la unidad procesadora 132 a través de la interfase de entrada 134 que está acoplada al bus 136, pero puede estar conectada por otras interfaces u estructuras de bus, tales como puertos paralelos, puertos de juego, o el Bus Genial Universal (USB). Un monitor 138 otros tipos de dispositivos de visualización también se conectan al bus del sistema 136 a través de una interfase, tal como la interfase de videos 130. Adicionalmente al monitor 138, el computador frecuentemente incluye otros dispositivos de salida periféricos (que no se muestran) tal como una impresora o parlantes, que se pueden conectar a través de una interfase periférica (que no se muestra).

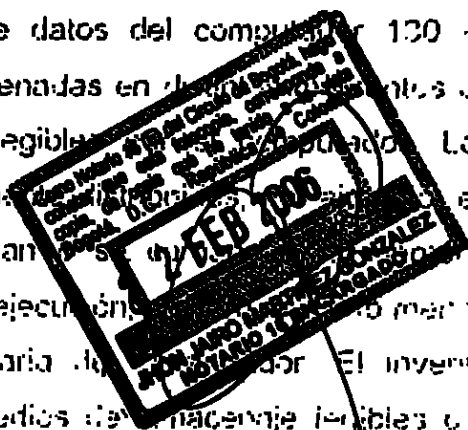
[0044] El computador 130 pueden operar haciendo conexiones lógicas a uno o mas computadores remotos 171. El computador remoto 171 puede ser un servidor, un busador de datos, un PC de red, o cualquier otro nodo de red común, y típicamente incluye muchos o todos de los elementos descritos anteriormente relativos al computador 130. Las conexiones lógicas que se muestran en la figura 3 se hacen en una red de área local (LAN). En



para red de área amplia (WAN) 138, pero también puede incluir otros tipos. La LAN 136 y/o la WAN 138 pueden ser redes alámbricas, redes inalámbricas, o una combinación. Estos ambientes de redes son comunes en oficinas, negocios, redes amplias de computadores, Internet os, y redes globales de computadores, por ejemplo, Internet.

[0045] Cuando se utilizan en un ambiente de redes de área local, el computador 130 estará conectado a la LAN 136 a través de una interfase de redes o adaptador 166. Cuando y se utilizan en un ambiente en un tender redes de área local, el computador 130 incluye típicamente una modem 178 u otros medios para establecer comunicación con la WAN 138, tal como Internet. El modem 178, que puede ser interno o externo, está conectado al pos del sistema 133 a través de una interfase de usuario de entrada 184, u otro mecanismo apropiado. En un ambiente de redes, los módulos de programa que se muestran relativos al computador 130, o porciones de, se pueden almacenar en un dispositivo de almacenaje de memoria remoto (que no se muestran). Como ejemplo, y no como limitante, la figura 8 muestra programas de aplicación remotos 192 como residiendo en el dispositivo de memoria. Las conexiones de redes que se muestran son ejemplares y otros medios para establecer un vínculo de comunicación entre computadores se puede utilizar.

[0046] Generalmente, el procesador de datos del computador 130 es programable por medio de instrucciones almacenadas en dispositivos de los componentes de almacenaje legibles. Los programas y el sistema operativo están típicamente almacenados en discos floppy o CD-ROMs. De ahí se instalan en la memoria secundaria del computador. En el momento de ejecución, se cargan típicamente en la memoria electrónica primaria del computador. El invento descrito aquí incluye estos y otros tipos de medios de almacenaje legibles por computador cuando tales medios contienen instrucciones o datos para

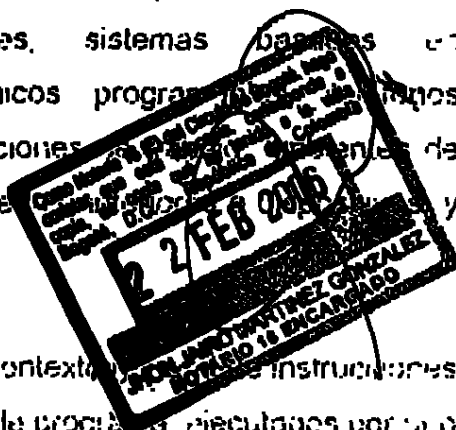


implementar los pasos descritos más abajo en conjunto con un microprocesador u otros procesadores de datos. El invento también incluye al computador en sí mismo cuando está programado de acuerdo a los métodos y técnicas descritos acá.

[0047] Con un propósito ilustrativo, los programas y otros componentes de programas ejecutables, tales como el sistema operativo, se muestran en bloques discretos. Se reconoce sin embargo, que estos programas y componentes residen en varios momentos en distintos componentes de almacenaje del computador, y son ejecutados por el procesador(es) del computador.

[0048] Aunque descrito en relación al ambiente de sistema de computación ejemplar, incluyendo el computador 130 el invento es funcional con muchos otros ambientes de sistema de computación de propósito general o especial y con otras configuraciones. El ambiente de sistema de computación no tiene la intención de sugerir ningún tipo de limitación en cuanto al alcance o funcionalidad del invento. Aún más, el ambiente de sistema de computación no se debe interpretar como teniendo ningún tipo de dependencia o requerimiento relacionado con uno o más combinaciones de los componentes ilustrados en el ambiente operativo ejemplar. Ejemplos de sistemas de cómputo, ambientes, y/o configuraciones que pueden ser adecuadas para uso con el invento incluyen, pero no están limitadas a, computadores personales, computadores servidores, computadores de mano, laptops, sistemas con multi procesadores, sistemas basados en microprocesadores, cajas, productos electrónicos programables, teléfonos móviles, PCs de red, mini- computadores, estaciones de trabajo, sistemas de cómputo distribuidos que incluyen cualesquiera de los anteriores y demás.

[0049] El invento se puede describir en el contexto de programas ejecutables por computador, tales como módulos de programas ejecutados por uno

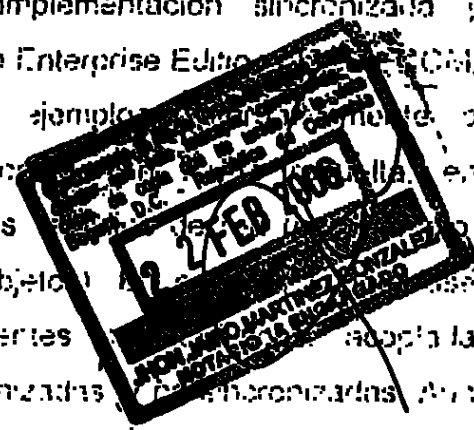


215

o más computadoras o dispositivos. Generalmente, los módulos de programa incluyen, pero no están limitados a, rutinas, programas, objetos, componentes y estructuras de datos que ejecutan tareas particulares o implementan tipos de datos abstractos particulares. El invento también se puede practicar en un ambiente de cómputo distribuido donde las tareas las ejecuta un dispositivo de procesamiento remoto que está ligado a través de una red de comunicaciones. En un ambiente de cómputo distribuido, los módulos de programa pueden estar localizados tanto en los medios de almacenaje locales como remotos incluyendo los dispositivos de almacenaje de la memoria.

[0050] Una interfase en el contexto de la arquitectura de software incluye módulos de software, componentes, porciones de código, y otras secuencias de instrucciones ejecutables por computador. La interfase incluye, por ejemplo, un primer módulo que accede a un segundo módulo para ejecutar tareas de cómputo en beneficio del primer módulo. El primero y segundo módulos incluyen, en un ejemplo, interfaces de aplicaciones de programación (APIs) tales como las suministradas por el sistema operativo, interfaces de modelo de componentes de objetos (COM) por ejemplo, Para aplicaciones de comunicación colega-colega, y el intercambio de nivel datos en interfaces con formato de lenguaje de marcación extensible (XML)/(por ejemplo, para comunicación entre servicios de red).

[0051] La interfase puede ser una implementación sincronizada y fuertemente acoplada tal como la Java 2 Platform Enterprise Edition (J2EE) COM, o la distribuida COM (DCOM), estos son ejemplos. Alternativamente, la interfase puede estar acoplada débilmente, en implementaciones no sincronizadas como en los que utilizan el protocolo de acceso simple de objetos (SOAP) o cualquier combinación de las siguientes. La interfase puede ser acoplada débilmente en formas síncronas o asíncronas.



53

216

más, la interfase se puede conformar a un protocolo estándar, un protocolo con propietario, o una combinación de protocolos estándar y con propietario.

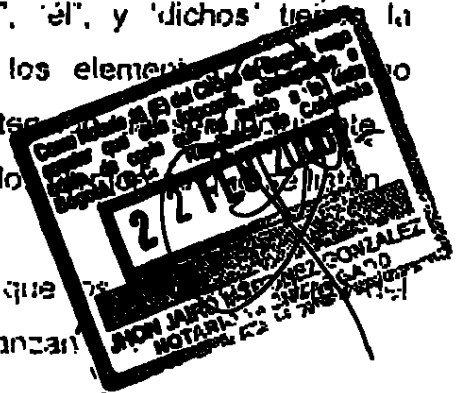
[0052] La interfase descrita hasta puede ser toda parte de una interfase única o puede estar implementada en interfases separadas o una combinación de ellas. Las interfases pueden ejecutarse localmente o en forma remota para suministrar la funcionalidad. Aún más, la interfase puede incluir más o menos funcionalidades que las ilustradas o descritas acá.

[0053] Cuando está en operación, el computador 130 funciona ya sea como el servidor de dominio fuente o el computador de dominio correspondiente (que puede ser una servidor) para ejecutar las instrucciones ejecutables por computador como se anotó anteriormente, y como se ilustró en las figuras 2-7.

[0054] El orden de ejecución de los métodos ilustrados y descritos acá no es esencial, al menos de que se especifique. Esto es, dos elementos y métodos se pueden ejecutar en cualquier orden, al menos de que se especifique lo contrario, y que los métodos pueden incluir más o menos elementos que aquellos que se presentan acá. Por ejemplo, se considera que ejecutar un elemento particular antes, contemporáneo con, o luego de otro elemento está dentro del alcance del invento.

[0055] Cuando se introduce un elemento que del invento presente o en una de sus implementaciones, los artículos 'un', 'una', 'él', y 'dichos' tienen la intención de significar que hay uno o más de los elementos. Los artículos 'comprende', 'incluye', y 'constará de' tiene la intención de significar que puede haber elementos adicionales que los elementos.

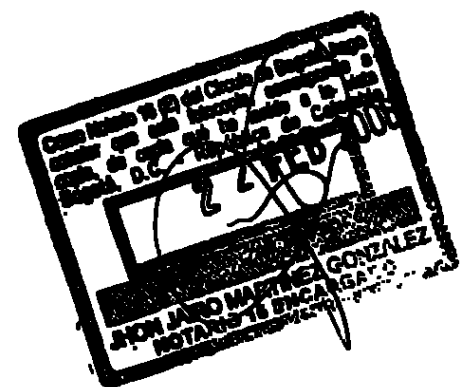
[0056] En vista de lo anterior, se puede ver que los métodos y otros resultados ventajosos se alcanzan.



59

217

[0057] Como se pueden hacer varios cambios en la construcción, materiales, productos, y métodos, sin alejarse del alcance del invento, se prefiere que todo el material contenido en la descripción anterior y que se muestra en los dibujos que la acompañan se debe interpretar como ilustrativa y no limitante en ningún sentido.



53

Lo que se reivindica es

1. Un método para determinar que un dominio correspondiente potencial tiene tecnología de e-mail segura y compatible para establecer un vínculo entre el dominio fuente y un dominio correspondiente y que comprende

Transmitir un secreto de descubrimiento de un dominio fuente a un dominio correspondiente donde el secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y donde el secreto de descubrimiento incluye una dirección del dominio fuente al cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad entre el dominio fuente y el dominio correspondiente; y
Recibir del dominio fuente a través de la dirección del dominio fuente una invitación del dominio correspondiente donde la invitación incluye el elemento de datos o un elemento correspondiente al elemento de datos que el dominio correspondiente puede utilizar para iniciar un proceso para establecer la compatibilidad con el dominio correspondiente

2. El método de la reivindicación 1 comprende además transmitir una aceptación del dominio fuente al dominio correspondiente para establecer que el correspondiente y el dominio fuente tienen tecnologías de e-mail seguras u otra tecnología de e-mail o de comunicaciones

3. El método de la reivindicación 1 donde el secreto de descubrimiento se transmite en forma selectiva a por lo menos uno de los siguientes

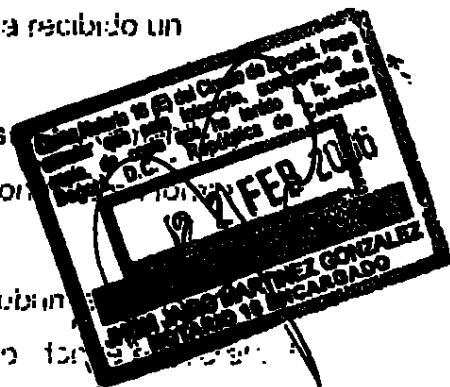
Dominios correspondientes de donde el dominio fuente ha recibido un mensaje

Dominios correspondientes específicamente identificados

Dominios correspondientes a través de mensajes seleccionados

4. El método de la reivindicación 1 donde el secreto de descubrimiento

se transmite en respuesta a una acción de usuario por



descubrimiento es un mensaje con un dominio correspondiente único; donde el secreto de descubrimiento es un mensaje a un dominio correspondiente que es un operador; donde el secreto de descubrimiento es un mensaje único a un dominio correspondiente para cada llave; o donde el secreto de descubrimiento es un mensaje enviado con una determinación basada en el tiempo.

5. El método de la reivindicación 1 donde el secreto de descubrimiento comprende un encabezado adicional que incluye el elemento de datos y la dirección del dominio fuente.

6. El método de la reivindicación 1 donde el secreto de descubrimiento comprende unas fechas de vencimiento y donde el dominio fuente no establece que los dominios correspondientes y fuente tienen tecnologías de e-mail segura y compatible cuando el dominio fuente recibe la invitación luego de la fecha de vencimiento.

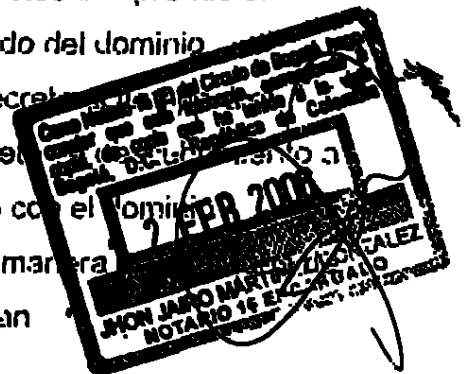
7. El método de la reivindicación 1 donde el elemento de datos es por lo menos uno de los siguientes:

un secreto por dominio que incluye un número aleatorio o pseudo aleatorio para cada dominio correspondiente;

un secreto generado a través de porciones del dominio correspondiente y de la semilla de secreto que se utilizó para generar los secretos por dominio para más de un dominio; y

un secreto por dominio generado codificando el dominio correspondiente y una fecha de vencimiento del secreto.

8. El método de la reivindicación 1 donde el elemento de datos comprende un secreto y donde el dominio fuente verifica el secreto recibido del dominio correspondiente re-computando y luego comparando el secreto con el secreto del dominio correspondiente con el secreto incluido en el secreto. La verificación de la autenticidad de los datos del cual el dominio fuente únicamente correspondió con el dominio correspondiente potencial que suministró el secreto de tal manera que la negación de servicio del dominio correspondiente se mitigan.



9. El método de la reivindicación 1 donde el elemento de datos se selecciona de una pluralidad de secretos múltiples simultáneos y válidos para cada dominio correspondiente de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación de un dominio correspondiente a la dirección administrativa del dominio que origina.

10. El método de la reivindicación 1 comprende además la imposición de un límite en el número de mensajes que se pasan a la dirección del dominio fuente con un elemento de datos particular mediante el cual se mitigan los ataques de negación de servicio utilizando elementos de datos correcto.

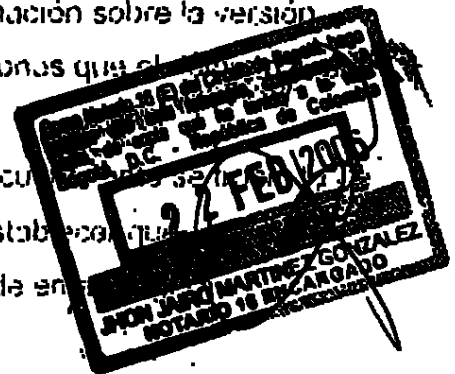
11. El método de la reivindicación 1 comprende además incluir la habilidad de sobrepasar los requerimientos para un elemento de datos para un dominio correspondiente dado para permitir la autorización fuera de banda y enviar un mensaje de invitación de un dominio particular.

12. El método de la reivindicación 1 donde el elemento de datos es una ficha en el mensaje, la secreto de descubierto en el encabezado de un correo o manifestado en el cuerpo del mensaje o donde el elemento de datos es una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando pasa a través de servidor de correos.

13. El método de la reivindicación 1 comprende además el soporte a múltiples fichas simultáneas válidas para el mismo dominio y la verificación de los mensajes de invitación de sub-dominios del dominio correspondiente verificando la ficha de entrada contra fichas para el dominio correspondiente.

14. El método de la reivindicación 1 donde el elemento de datos es una mención y comprende además la inclusión en la mención de información sobre la versión para el dominio fuente e incluyendo en la mención funciones que el dominio fuente soporta.

15. Una estructura de datos para una un secreto de descubierto que se pasa de un dominio fuente a un dominio correspondiente para establecer una comunicación entre el dominio fuente y el dominio correspondiente basados en tecnologías de encriptación, que comprende:

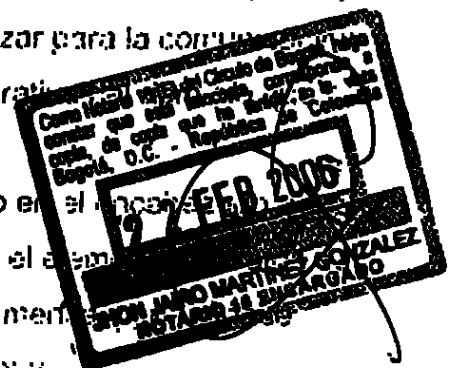


221

Un mensaje; un encabezado relacionado con el mensaje y
 Un encabezado adicional anexo al mensaje y que incluye (1) un elemento de
 datos específico al dominio correspondiente que incluye una dirección del
 dominio fuente a la cual el dominio correspondiente se le permite enviar un
 mensaje al dominio fuente para establecer que el dominio correspondiente y el
 dominio fuente tienen tecnologías de email segura y compatible, (2) un secreto
 de descubrimiento y (3) una fecha de vencimiento.

15 La estructura de datos de las reivindicación 15 donde el elemento de datos es
 por lo menos uno de los siguientes:

- Un secreto por dominio que incluye un número aleatorio o pseudo-aleatorio
 para el dominio correspondiente;
- Un secreto generado a través de porciones del dominio correspondiente y una
 familia secreta que se utiliza para generar los secretos por dominio para más
 de un dominio;
- Un secreto por dominio generado codificando el dominio correspondiente y una
 fecha de vencimiento del secreto;
- Un secreto y donde el dominio fuente verifica el secreto recibido del dominio
 correspondiente re-computando y luego comparando el secreto actual para el
 dominio correspondiente con el secreto incluido en el secreto de
 descubrimiento;
- Un elemento de datos se selecciona de una pluralidad de secretos múltiples
 que se superponen para cada dominio correspondiente de tal manera que hay
 una pluralidad de secretos válidos que se pueden utilizar para la comunicación
 de un dominio correspondiente a la dirección administrativa
 original;
- Una ficha en el mensaje de secreto de descubrimiento en el encabezado
 o incrustado en el cuerpo del mensaje o donde el elemento de datos
 está en el encabezado del correo y el cuerpo del mensaje
 o tomado cuando pasa a través del servidor de correo; y



28

Una mención que comprende además incluye en la mención la información de versión para el dominio fuente y incluye en la mención funciones apoyadas por el dominio fuente.

17. Un sistema para establecer que los dominios correspondiente y fuente tienen tecnologías de email segura y compatible, y que comprende

Un servidor dominio fuente transmitiendo un secreto de descubrimiento al dominio correspondiente donde el secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y donde el secreto de descubrimiento incluye una dirección del dominio fuente a la cual se le permite al dominio correspondiente enviar un mensaje para establecer que el correspondiente y el dominio fuente tienen tecnologías de email segura y compatible, y

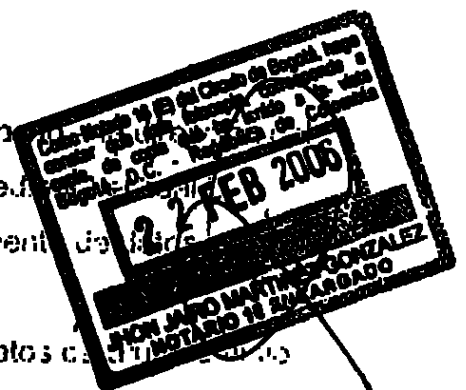
un computador del dominio correspondiente recibiendo e incluyendo el elemento de datos y la dirección del dominio fuente a donde el computador dominio correspondiente le transmite una invitación del dominio correspondiente a la dirección del dominio fuente donde la invitación incluye el elemento de datos o un elemento correspondiente al elemento de datos.

18. El sistema de la reivindicación 17 donde el servidor de dominio fuente transmite una aceptación del dominio fuente para el dominio correspondiente para establecer que los dominios fuente y correspondiente tienen tecnología de email segura y compatible y donde el servidor del dominio fuente inicia un proceso para establecer un vínculo con un computador del dominio correspondiente tan pronto recibe de servidor del dominio fuente la invitación; y

Comprende además uno de los siguientes.

Imponer un límite en el número de mensajes que se pueden enviar al dominio fuente con un elemento de datos particular mediante la limitación de los ataques de servidor utilizando un elemento de datos de ataque.

Sobrepasar los requerimientos para un elemento de datos de ataque correspondiente dato para permitir una acción fuera de banda para una y



mensajes de invitación de un dominio particular y dar soporte a múltiples fichas válidas para el mismo dominio y verificar los mensajes de invitación de subdominios del dominio correspondiente verificando el secreto de descubrimiento entrante contra los secretos de descubrimiento para el dominio correspondiente.

19. El sistema de la reivindicación 17 donde el secreto de descubrimiento transmitido por el servicio del dominio fuente comprende por lo menos uno de los siguientes:

Un secreto de descubrimiento selectivo transmitido al dominio correspondiente de donde el dominio fuente ha recibido un mensaje;

Un secreto de descubrimiento transmitido en forma selectiva al dominio correspondiente identificado específicamente por adelantado o ser designado en forma aleatoria del dominio correspondiente;

Un mensaje que se genera en respuesta a una acción de usuario;

Un mensaje con un dominio correspondiente único;

Un mensaje a un dominio correspondiente que es la dirección de una operadora de servidor;

Un mensaje único al dominio correspondiente para cada llave;

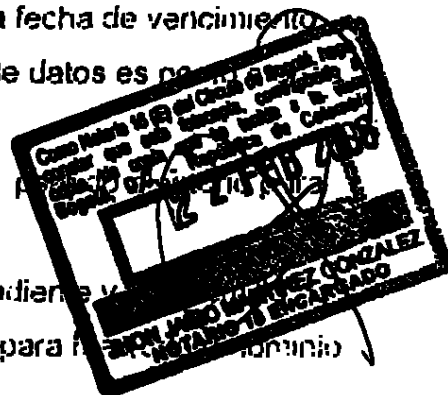
Un mensaje enviado con una determinación basada en el tiempo;

Un encabezado adicional que incluye un elemento de datos y una dirección del dominio fuente; y una fecha de vencimiento donde el dominio fuente no inicia el proceso para establecer un vínculo con el dominio correspondiente cuando la invitación que recibe el dominio fuente es posterior a la fecha de vencimiento.

20. El sistema de la reivindicación 17 donde el elemento de datos es por lo menos uno de los siguientes

Un secreto por dominio que incluye un número aleatorio o pseudoaleatorio transmitido al dominio correspondiente;

Un secreto generado con porciones del dominio correspondiente y un secreto que se utiliza para generar el secreto por dominio para el dominio correspondiente.



224

Una secreto por dominio generado codificando el dominio correspondiente y una fecha de vencimiento del secreto,

Un secreto y donde el dominio fuente verifica el secreto recibido del dominio correspondiente re calculando y luego comparando el secreto actual para el dominio correspondiente con el secreto incluido en el secreto de descubrimiento,

Un elemento de datos se selecciona de una pluralidad de múltiples secretos que se superponen para cada dominio correspondiente de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación de un dominio correspondiente a la dirección administrativa del dominio que origina,

Una ficha en el mensaje de secreto de descubrimiento en el encabezado del correo o incrustadas en el cuerpo del mensaje o donde el elemento de datos es una ficha en el encabezado del correo y el cuerpo del mensaje permanezca codificando cuando pasa a través de servidor de correo; y

Una mención que comprende la inclusión en la mención de información de la versión para el dominio fuente y que incluye en la mención funciones soportadas por dominio fuente



62

RESUMEN

Un secreto de descubrimiento se transmite de un dominio fuente a un dominio correspondiente. El secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y punto al secreto de descubrimiento incluye una dirección del dominio fuente a la cual se permite al dominio correspondiente enviar un mensaje para determinar que un correspondiente potencial en tener tecnologías de e-mail segura incompatible para establecer un vínculo entre el dominio fuente y el dominio correspondiente. El secreto de descubrimiento no reside en dominio correspondiente incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio del dominio correspondiente al la dirección del dominio fuente. La invitación incluye el elemento de datos o elemento de datos correspondiente al elemento de datos. El dominio fuente inicia un proceso para establecer un vínculo con el dominio correspondiente tan pronto recibe del dominio fuente la invitación.



SOLICITUD DE PATENTE

DECLARACION Y PODER DEL ABOGADO

ROTULO DEL ABOGADO NO.
MSFT5169.1

ROTULO MS NO.
311.610.02

Como inventor mencionado más abajo, declaro por medio de la presente que:
mi dirección de residencia/correo y ciudadanía son como aparecen más abajo al lado de mi nombre;

yo creo que soy el primero, único y original inventor (si sólo aparecen un nombre en la lista más abajo) o uno de los originales, primeros inventores conjuntos (si se utilizan nombres plurales más abajo) de el teme que se reivindica y para el cual se busca una patente del invento llamado:

SISTEMA Y MÉTODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE

especificaciones que se entregan con la presente al menos de que la siguiente casilla este marcada:

() se presentó en _____ cómo solicitud de EU Serial No. o Solicitud Internacional PCT Numero _____ y se enmendo _____ (si aplica).

Declaro por medio de la presente que he revisado entendido el contenido de las especificaciones identificadas anteriormente, incluyendo las reivindicaciones, como se enmendaron con cualquier enmienda referida anteriormente. Yo reconozco el deber de divulgar toda la información que es material de la patente como se define en 37 CFR 1.56.

Solicitud (es) extranjeras y para con reivindicaciones de prioridad extranjeras por medio de la presente régimen y con la prioridad extranjera bajo los beneficios del Título 45 del código de los estados unidos sección 119 de ciudadanía extranjera para patente como inventores certificados enumerados en la solicitud de prioridad identificado más abajo cualquier solicitud extranjera para la cual se reivindica la prioridad: (es) su certificados que tienen una fecha de entrega anterior a la de la solicitud de la cual se reivindica la prioridad:

PAIS	SOLICITUD	FECHA DE ENTREGA	FECHA DE ENTREGA DE LA SOLICITUD DE PATENTE

Comisión de Patentes y Marcas Registradas
Calle de la Industria 100, 2do. Piso
Ciudad de México, D.F. 06702
Tel: 52 55 52 00 00
Fax: 52 55 52 00 00
www.patentes.gob.mx
JUAN MARQUEZ GONZALEZ
NOTARIO PUBLICO
9 11 00 00

PODER DEL ABOGADO:

227

Por medio de la presente, yo como inventor mencionado designo como abogado (s)
y/o agente (s) asociados con

Cliente No. 000038779

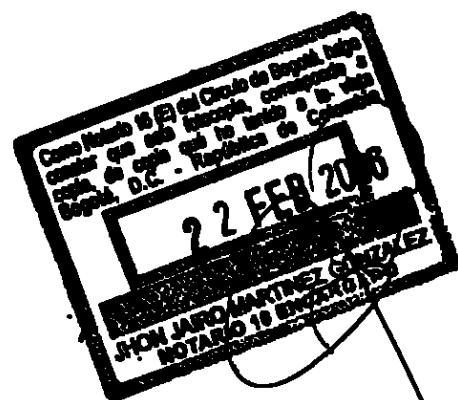
Procesar esta solicitud y atender los negocios relacionados en la Oficina de Patentes
y Marcas registradas.

Enviar la correspondencia a:

Dirija las llamadas telefónicas:

Frank R. Agovino
Senniger Powers, Leavitt & Roedl
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102

Frank R. Agovino
(314) 231-5400



65

228

DECLARACION Y PODER DEL ABOGADO

ROTULO DEL ABOGADO NO.
MSFT5169.1

ROTULO MS NO.
311.610.02

Por medio de la presente declaro que todas afirmaciones aquí presentes son verdad y que todas las declaraciones sobre información y creencias las creo verdaderas; y más aún que todas las declaraciones fueron hechas con el conocimiento de que la falsedad en las declaraciones se castigan con multas o prisión, o ambas, bajo la sección 1001 del título 18 del Código de los Estados Unidos y que tales falsedades pueden arriesgar la validez de la solicitud o de cualquier patente que se emita

Nombre completo del inventor: Eric D. Tribble Ciudadanía: EU

Residencia: Redmond, Washington 98033

Dirección de correo: One Microsoft Way, Redmond, Washington 98052-6399

Firma del inventor

Fecha

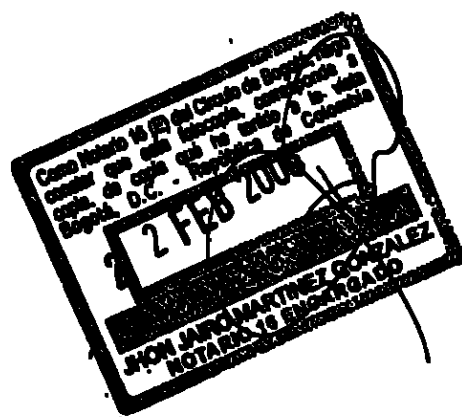
Nombre completo del inventor: Trevor W. Freeman Ciudadanía: Gran Bretaña

Residencia: Redmond, Washington

Dirección de correo: One Microsoft Way, Redmond, Washington 98052-6399

Firma del inventor

Fecha



46

FIG 1

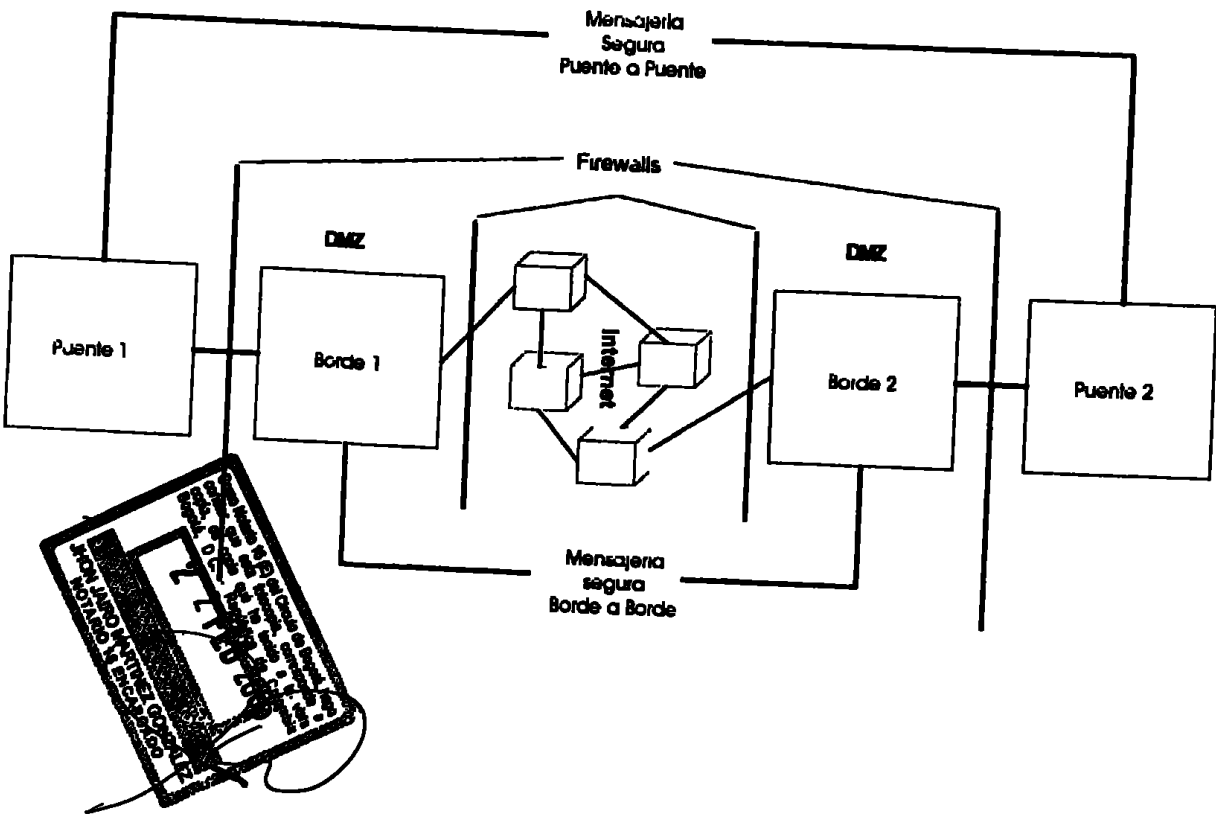
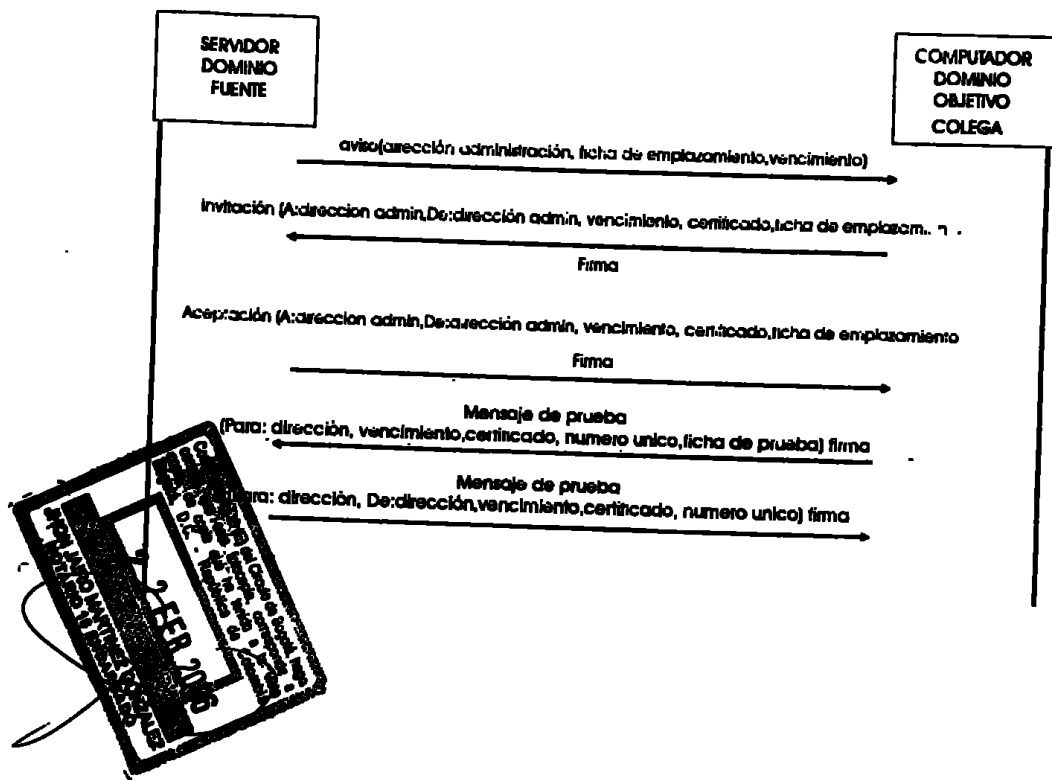
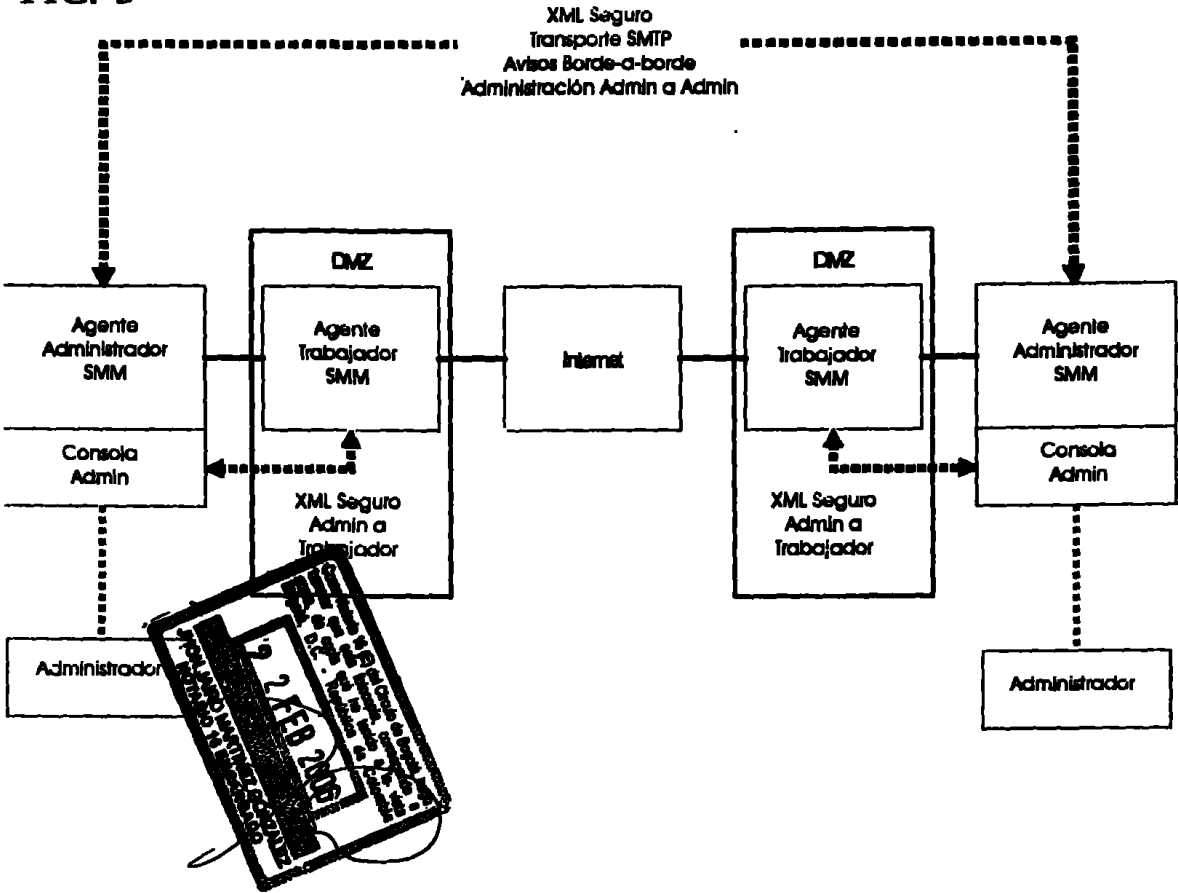


FIG. 2



63

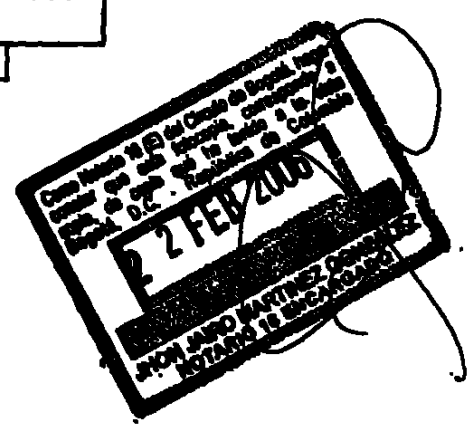
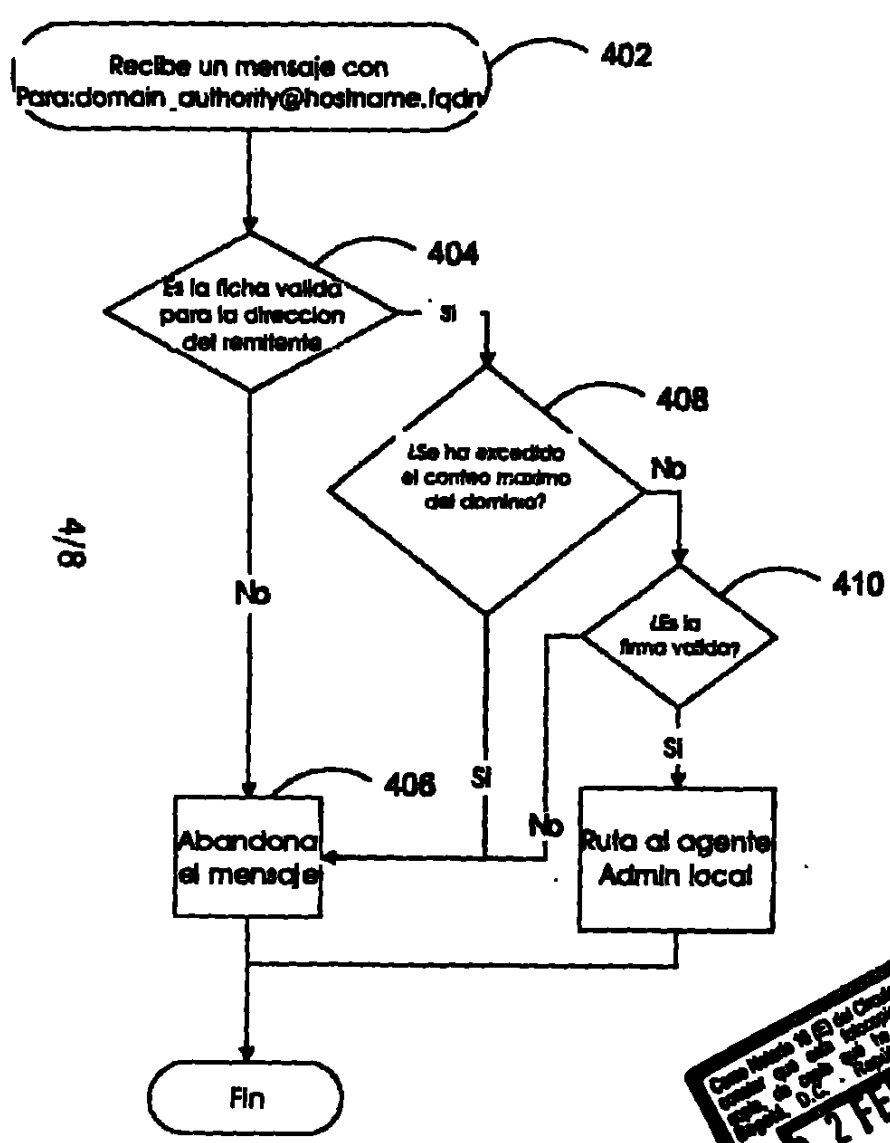
FIG. 3



3/8

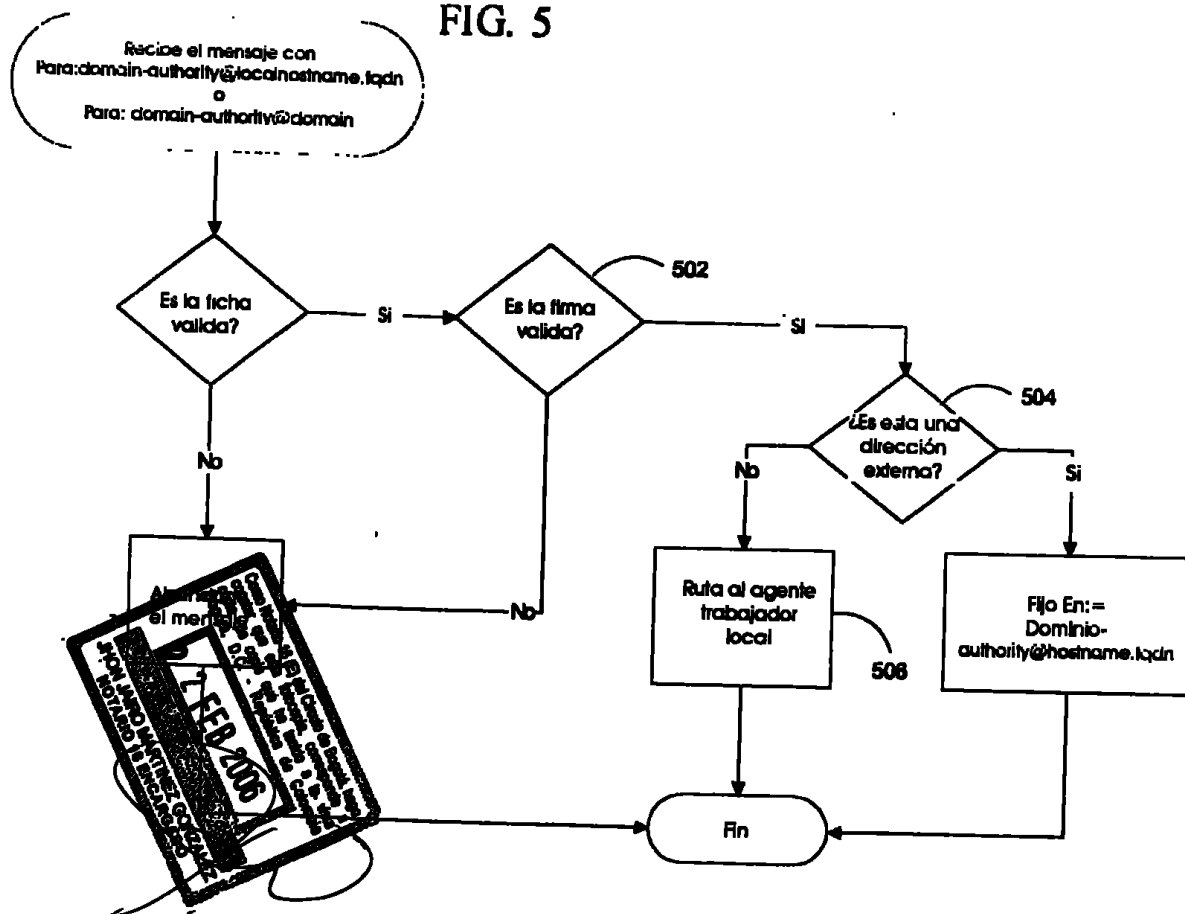
2

FIG. 4



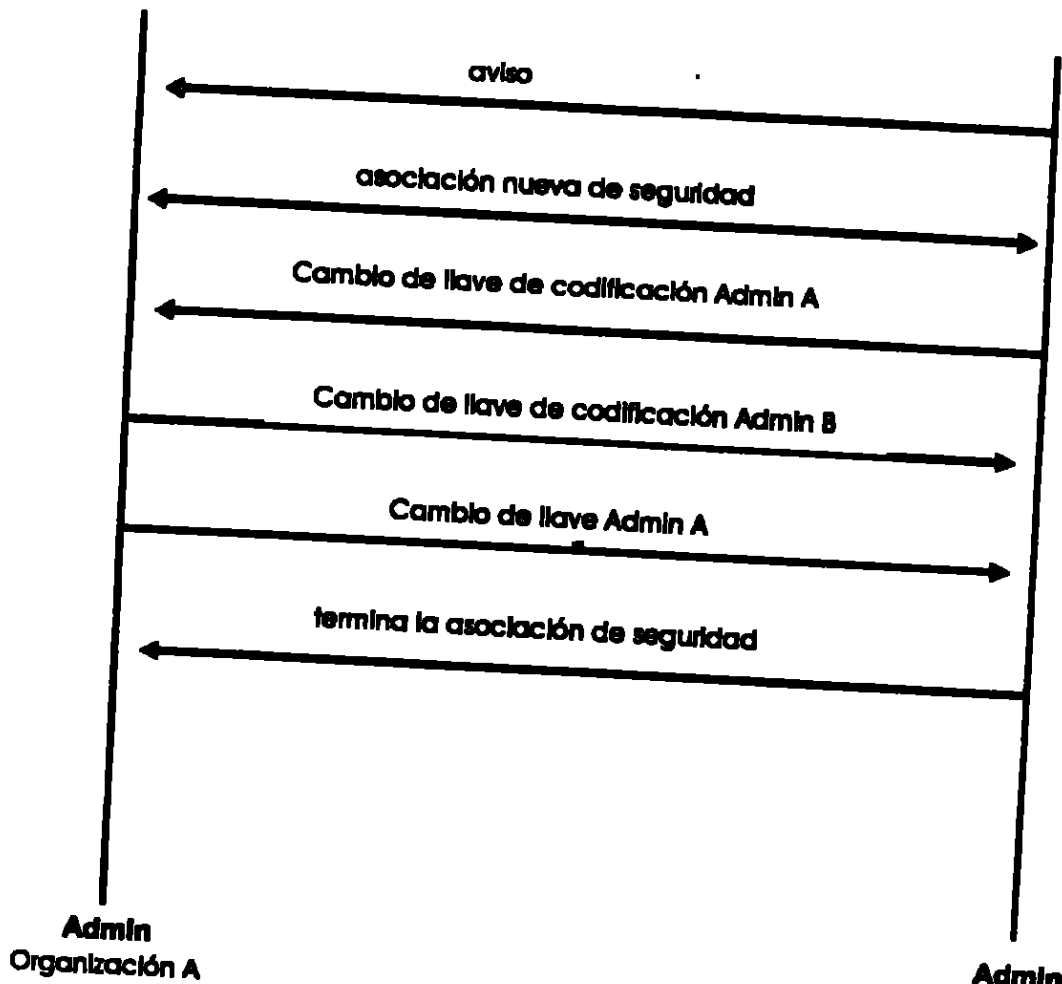
20

FIG. 5



4

FIG. 6



8/9

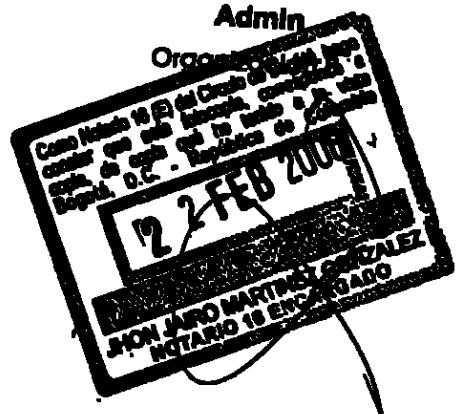
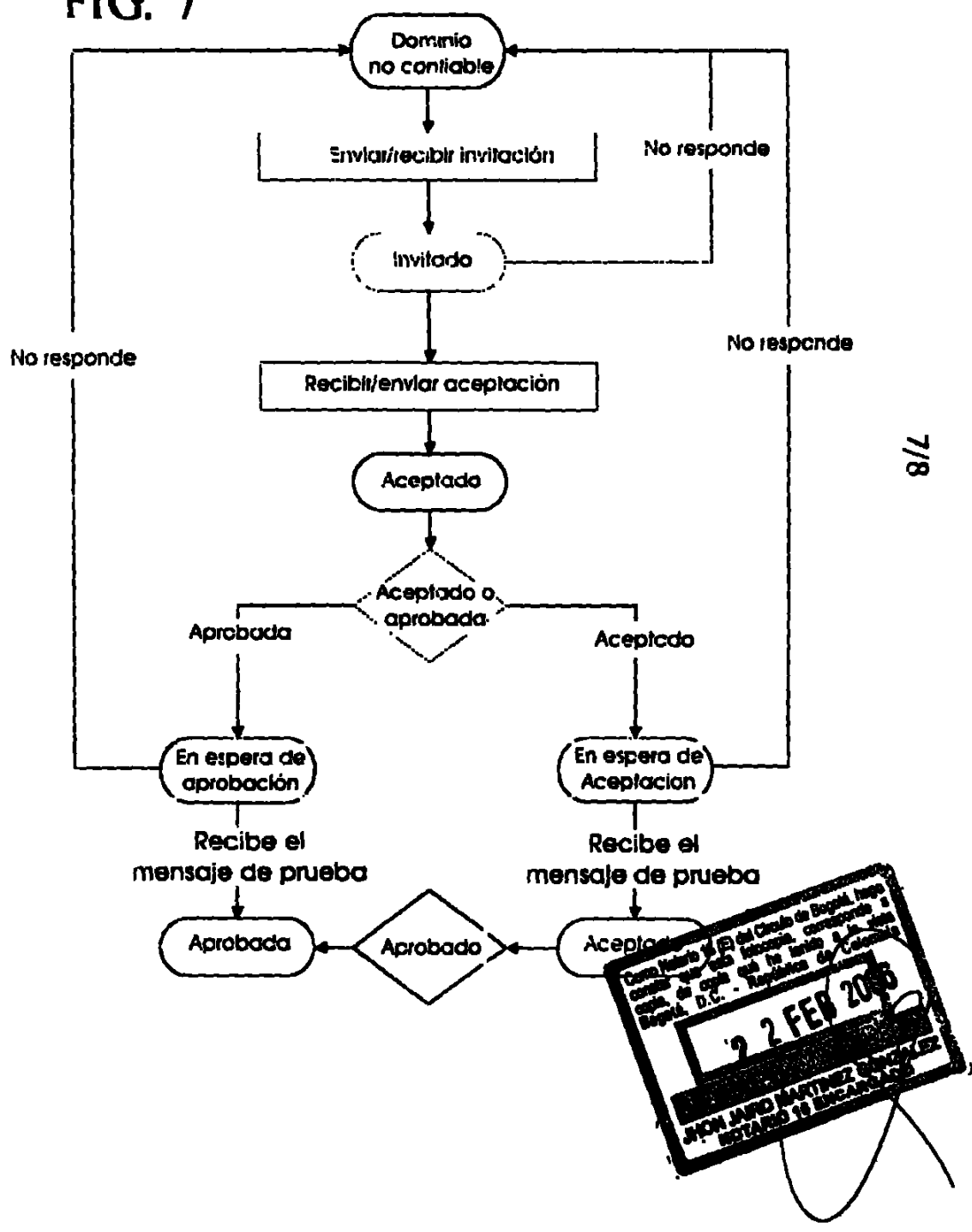
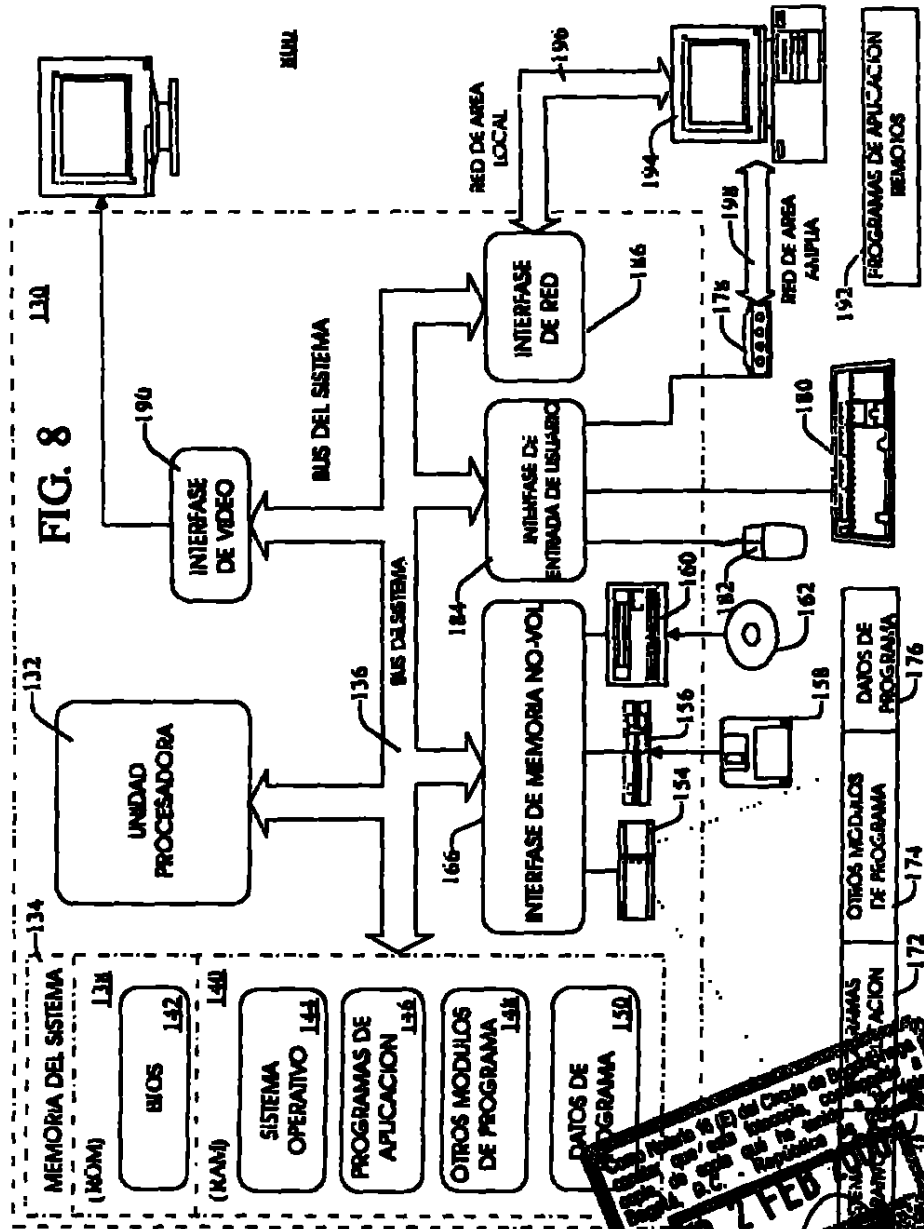


FIG. 7





27 FEB 1993
JUAN JAVIER MARTINEZ CAMPAZ
NOTARIO 18 ENCARGO

27

FICHA TÉCNICA DE LA SOLICITUD
INFORMACIÓN DE LA SOLICITUD

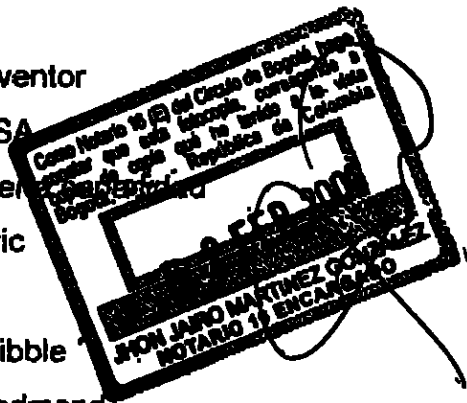
Tipo de solicitud: Regular
Asunto: Utilidad
Clasificación Propuesta: En blanco
Unidad de Grupo de Arte Propuesta: En blanco
Título: **SISTEMA Y MÉTODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE**

Expediente del Abogado: MS#311610.02 (5169.1)
Solicitud de Publicación Anticipada: NO
Solicitud de No publicación: NO
Figura Gráfica Propuesta: 1
Total Hojas de Gráficas: 8
Pequeña Entidad: NO
Petición incluida: NO

INFORMACIÓN DEL SOLICITANTE

Tipo de Autoridad del Solicitante:
País de Ciudadanía Principal:
Condición:
Primer Nombre:
Segundo Nombre:
Apellido:
Ciudad de Residencia:
Estado o Provincia de residencia:
País de Residencia:

Inventor
USA
Plen
Eric
D.
Tribble
Redmond
WA
USA



Calle de la Dirección Postal: 15600 NE 8th Street, B1#777
Ciudad de la Dirección Postal: Bellevue
Estado o Provincia de la Dirección Postal: WA
País de la Dirección Postal: USA
Código Postal de la Dirección Postal: 98008

Página 1 Inicial 4/15/05

Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el 12/23/2006

SIGUIENTE PÁGINA:

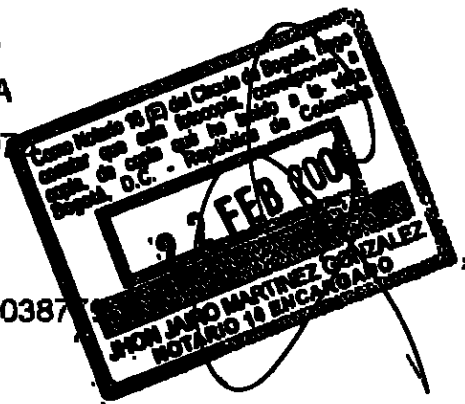
Tipo de Autoridad del Solicitante: Inventor
País de Ciudadanía Principal: Gran Bretaña
Condición: Plena capacidad
Primer Nombre: Trevor
Segundo Nombre: W.
Apellido: Freeman
Ciudad de Residencia: Sammamish
Estado o Provincia de residencia: WA
País de Residencia: USA
Calle de la Dirección Postal: 2022 236th Avenue SE
Ciudad de la Dirección Postal: Sammamish
Estado o Provincia de la Dirección Postal: WA
País de la Dirección Postal: USA
Código Postal de la Dirección Postal: 9807

Información de Correspondencia

No. de Correspondencia del Cliente: 000038779

Información de Representación

No. de Representante del Cliente: 000038779



239

Información de Prioridad Doméstica			
Solicitud	Tipo de Continuidad	Solicitud Principal	Fecha de Radicación de Sol. Principal
Esta misma	Una solicitud reivindicando beneficios según 35 USC 119 (e)	60/659,279	03/07/05

Información de Prioridad Extranjera			
País:	No. de Solicitud:	Fecha de Presentación:	Prioridad Reivindicada:

Página 2

Inicial 4/15/05

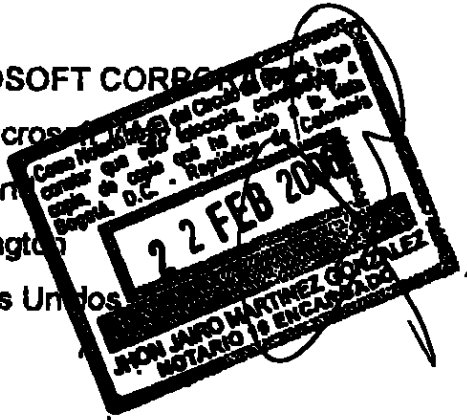
Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el 12/23/2005

SIGUIENTE PÁGINA:

INFORMACIÓN DEL CESIONARIO:

Nombre del Cesionario:
Calle de la Dirección Postal:
Ciudad de la Dirección Postal:
Estado o Provincia la Dirección Postal:
País la Dirección Postal:
Código Postal la Dirección Postal:

MICROSOFT CORP
One Micros
Redmon
Washington
Estados Unidos
98052



22

240

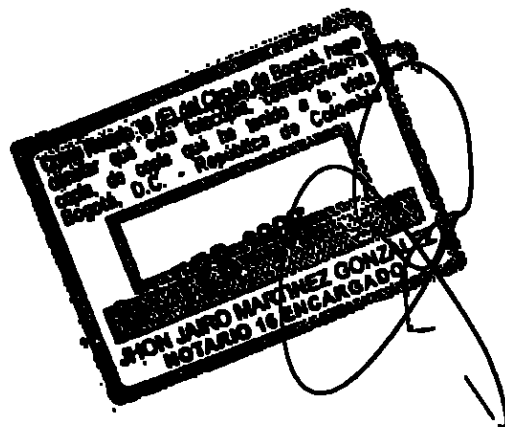
Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005

**CONTRAPORTADA: LOGO DEL DEPARTAMENTO DE COMERCIO DE
ESTADOS UNIDOS – OFICINA DE PATENTES Y MARCAS REGISTRADAS**

CERTIFICO QUE ESTA ES UNA TRADUCCIÓN FIEL DEL INGLES AL
ESPAÑOL DE UN DOCUMENTO QUE HE TENIDO A LA VISTA; QUE SOY
TRADUCTORA E INTERPRETE OFICIAL ACREDITADA POR RESOLUCIONES
0035 Y 530 DE LA UNIVERSIDAD NACIONAL DE COLOMBIA Y DEL
MINISTERIO DE LA JUSTICIA RESPECTIVAMENTE, Y QUE ESTOY
REGISTRADA ANTE EL MINISTERIO DE RELACIONES EXTERIORES DE
COLOMBIA

Bogotá, febrero 8 de 2006

NORA JIMÉNEZ DE ADAM
C.C. 20.335.247



28

241

PA 1403082



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:
UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

December 28, 2005

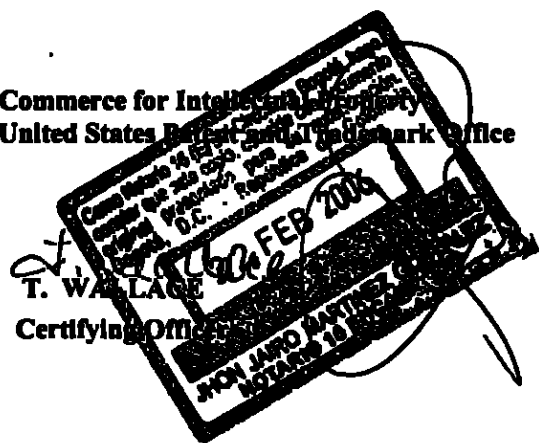
**THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM
THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK
OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT
APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A
FILING DATE UNDER 35 USC 111.**

APPLICATION NUMBER: 11/107,011

FILING DATE: April 15, 2005

**THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY
APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS
CONVENTION, IS US11/107,011**

**By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office**



22

ENNIGER
POWERS

ATTORNEYS
AT LAW

PATENTS
TRADEMARKS

LITIGATION
COPYRIGHTS

TECHNOLOGY
ANTITRUST

ONE METROPOLITAN SQUARE
18TH FLOOR
SAINT LOUIS, MISSOURI 63102

314-531-5400 V
314-531-4343 F

ENNIGER.COM

FRANK R. ARDING

April 15, 2005

112948 U.S. PTO

11/107011

041505

UTILITY PATENT APPLICATION TRANSMITTAL
(new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket Number: MS#311610.02 (5169.1)

First Named Inventor: Eric D. Tribble

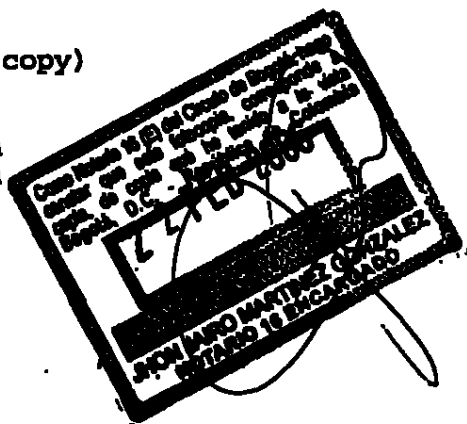
Title: SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A
CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL

Express Mail Label Number: EL 462439036 US

TO: Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION ELEMENTS

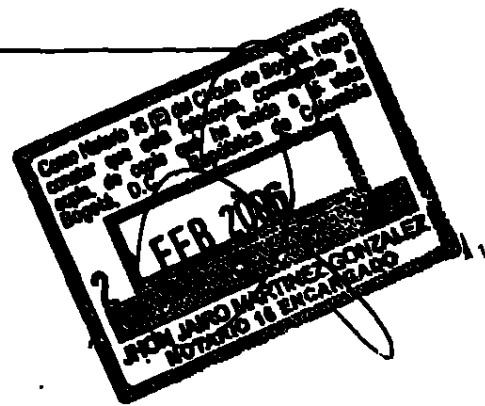
1. ☒ Fee Transmittal Form
(original and duplicate)
2. ☐ Applicant claims small entity status
3. ☒ Specification [Total Pages 26]
4. ☒ Drawings [Total Sheets 8]
5. Oath or Declaration [Total Pages 2]
 - a. ☒ Newly executed (original or copy)
☐ New (unexecuted)
 - b. ☐ Copy from a prior application
(for continuation/divisional with
Box 19 completed)
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached
deleting inventor(s) named
in prior application.



- 243
6. ☐ Incorporation By Reference
(useable if Box 5b is marked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 5b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
7. ☒ Application Data Sheet
8. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
9. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
- a. ☐ Computer Readable Form
- b. ☐ Specification Sequence Listing on:
- i. ☐ CD-ROM or CD-R (2 copies); or
- ii. ☐ paper
- c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

10. ☐ Assignment Papers (cover sheet & document(s))
11. ☐ 37 CFR 3.73(b) Statement ☒ Power of Attorney
12. ☐ English Translation Document (if applicable)
13. ☐ IDS with PTO/SB/OSA ☐ Copies of IDS Citations
14. ☐ Preliminary Amendment
15. ☒ Return Receipt Postcard
16. ☐ Request and Certification for Non-Publication. Form PTO/SB/35 is attached.
17. ☐ Certified Copy of Priority Document(s) if foreign priority is claimed
18. ☐ Separate Paper Identifying Attorneys/Agent to be Designated of Record
19. ☐ Other: _____



244

**IF A CONTINUING APPLICATION, CHECK APPROPRIATE
BOXES AND SUPPLY THE REQUISITE INFORMATION**

20. ☐ Continuation ☐ Divisional ☐ Continuation-in-Part
of prior application No.: _____

☒ Complete Application based on provisional Application
No. 60/659,279, filed March 7, 2005.

Prior application information: Examiner:
Group Art Unit:

CORRESPONDENCE ADDRESS

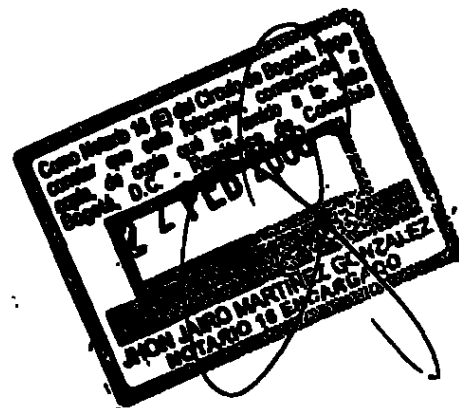
21. Correspondence Address: Customer Number 000038779
Attention: Frank R. Agovino

Respectfully submitted,

Frank R. Agovino

Frank R. Agovino, Reg. No. 27,416

FRACwa



FEE TRANSMITTAL

245

Application Number to be assigned
Filing Date April 15, 2005
Inventor(s) Eric D. Tribble et al.
Attorney Docket Number MS#311610.02 (MSFT 5169.1)

17414 U.S. PTO

☐ Applicant claims small entity status.

METHOD OF PAYMENT

- ☐ The Commissioner is hereby authorized to charge the indicated fees to Deposit Account No. 19-1345. The Commissioner is hereby authorized to charge any under payment or credit any over payment to Deposit Account No. 19-1345.
- ☒ Check Enclosed. The Commissioner is hereby authorized to charge any under payment or credit any over payment to Deposit Account No. 19-1345.

FEE CALCULATION

1. ☒ BASIC FILING, SEARCH AND EXAMINATION FEES
(Type: Utility) Subtotal (1) \$1,000.00

2. ☐ EXCESS CLAIM FEES
 Total Claims - (HP) = x Fee = \$
 Indep Claims - (HP) = x Fee = \$
 Multiple Dependent Claims Fee \$
 (HP = highest number of claims paid for)
 Subtotal (2) \$

3. ☐ APPLICATION SIZE FEE
 Total Pages - 100 = + 50 = x \$250 = \$
 (Application + Drawings) (round up to whole \$)
 Subtotal (3) \$

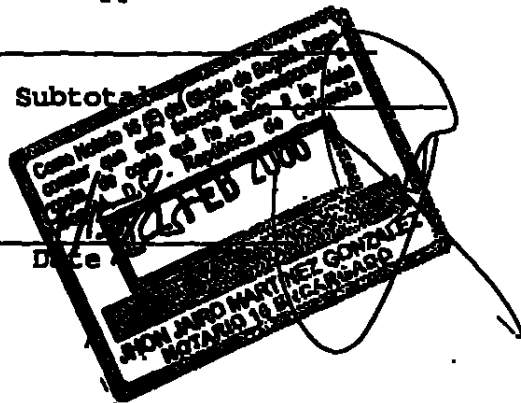
4. ☐ OTHER FEE(S)
☐ month extension of time
☐ Information disclosure statement
☐ 37 CFR 1.17(q) processing fee
☐ Non-English specification
☐ Notice of Appeal
☐ Filing a brief in support of appeal
☐ Request for oral hearing
☐ Other:

Subtotal

TOTAL AMOUNT OF PAYMENT \$1,000.00

Frank R. Agovino
Frank R. Agovino, Reg. No. 27,416
Telephone: 314-231-5400

FRACwa
Express Mail Label No. EV462439036US



85

246

SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL

TECHNICAL FIELD

[0001] Embodiments of the present invention relate to the field of establishing a compatible interconnection between two domains. In particular, embodiments of this invention relate to a system and method to reveal and discover mail servers with advanced capabilities.

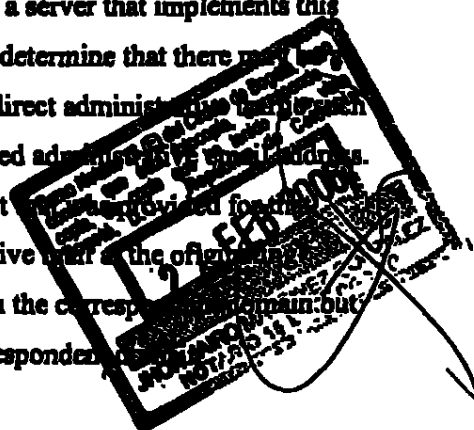
BACKGROUND OF THE INVENTION

[0002] Some prior systems attempt to identify potential correspondents by communicating directly. However, these systems become vulnerable to attackers when communicating and, in particular, can cause or be vulnerable to SPAM and denial of service attacks.

[0003] Accordingly, a system is desired to address one or more of these and other disadvantages by discretely identifying a potential correspondent so that a secure link between a server and a potential correspondent may be established.

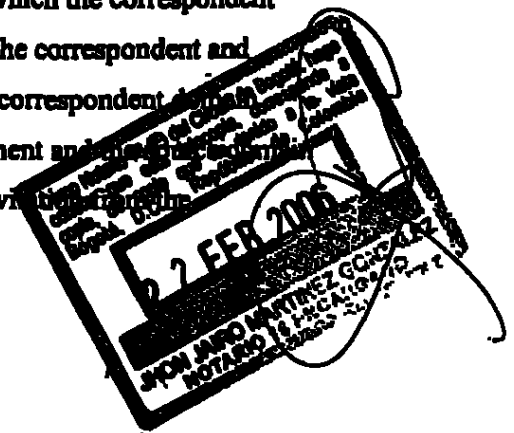
SUMMARY OF THE INVENTION

[0004] Embodiments of the invention include an email server which occasionally adds an additional header to a message that will be delivered to potential correspondent domains. The data in the header includes a secret that is specific to a message sent to a particular correspondent domain and an email address to which administrative messages from that correspondent domain can be directed to the server. If mail at the correspondent domain is also directed through a server that implements this embodiment, then it will detect the additional header and determine that there may be a compatible server at the originating domain. It can then direct administrative messages such as requests to establish a secure connection to the contained administrative email address. Such administrative messages must also contain the secret information provided for the correspondent domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the correspondent domain but that does not contain the secret corresponding to the correspondent domain.



84

[0007] In another form, the invention comprises a system for establish that the correspondent and source domains have compatible secure email technology or other email or communication technology. A source domain server transmits a discovery secret to the correspondent domain. The discovery secret includes a data element specific to the correspondent domain and a source domain address to which the correspondent domain is permitted send a message in order to establish that the correspondent and source domains have compatible secure email technology. A correspondent domain computer receives the discovery secret including the data element and the source domain address. The correspondent domain computer transmits an invitation to the



248

correspondent domain to the source domain address. The invitation includes the data element or an element corresponding to the data element.

[0008] Alternatively, the invention may comprise various other methods and apparatuses.

[0009] Other features will be in part apparent and in part pointed out hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is an exemplary block diagram of gateway servers 1 and 2 having secure messaging therebetween.

[0011] FIG. 2 is an exemplary diagram illustrating workflow between a source domain server and a potential correspondent (e.g., a correspondent domain server) according to the invention.

[0012] FIG. 3 is an exemplary block diagram illustrating a secure message manager according to the invention.

[0013] FIG. 4 is a flow diagram illustrating operation of secure message management (SMM) administrative routing according to the invention.

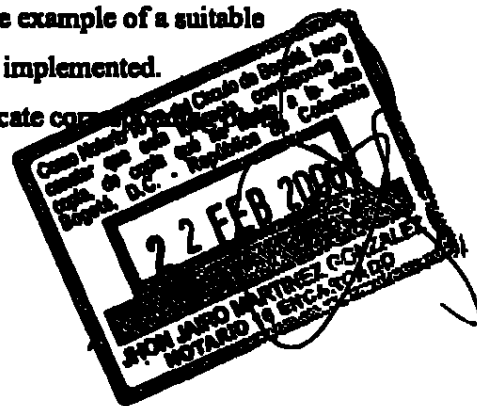
[0014] FIG. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention.

[0015] FIG. 6 is an exemplary block diagram illustrating an inter-organization workflow summary between a server (admin organization A) and a correspondent (admin organization B) according to the invention.

[0016] FIG. 7 is a flow diagram illustrating a state diagram after a new security association implemented between a server and a correspondent according to the invention.

[0017] FIG. 8 is a block diagram illustrating one example of a suitable computing system environment in which the invention may be implemented.

[0018] Corresponding reference characters indicate corresponding elements throughout the drawings.



26

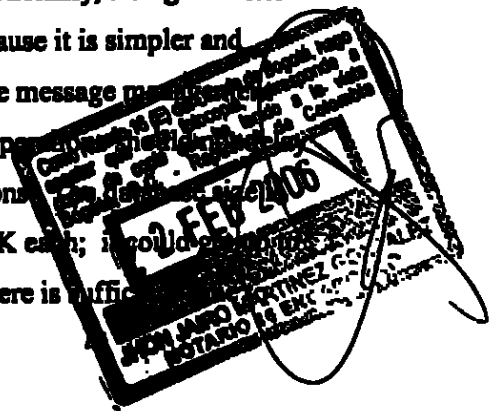
249

DETAILED DESCRIPTION OF THE INVENTION

[0019] The invention relates to a system and method for determining that a potential correspondent has compatible secure email technology in order to begin the process of establishing a link between a server and a correspondent. In particular, the invention relates to a system and method for initiating the process of establishing a secure link for the deployment of secure email. The invention allows a server to determine that a potential correspondent can be established as a target because of compatible secure email technology. As a result, once a potential correspondent is identified, the server can exchange key material information with the potential correspondent in order to establish the secure link.

[0020] The objective of domain signing and encryption according to the invention is to provide a transport independent mechanism to exchange confidential and server authenticated messages between servers. Fig. 1 is an exemplary block diagram of gateway servers 1 and 2. The gateway servers 1 and 2 have a secure messaging link therebetween. The servers may be separated by an optional firewall through which they may be connected to bridgehead servers (not shown), which may be are part of a separate, secure messaging system. Gateway servers 1 and 2 form a sub-network that may be located between a trusted internal network, such as the secure messaging system linking bridgehead servers and an untrusted external network, such as the public internet. Firewalls are also positioned between the gateway servers and the Internet. The gateway servers treat all mail as clear text and encrypt all mail gateway to gateway. If the gateway and bridgehead servers do not share the same encryption keys, the gateway servers cannot decrypt bridgehead server encrypted mail.

[0021] There is a need for a single point of administration for the authoritative data for all internal and external relationships. Optionally, a single master model rather than a multiple-master model is implemented because it is simpler and because it does not have to resolve replication conflicts. Secure message management (SMM) operations are usually infrequent and delays in SMM operations are usually small (e.g., hundreds of thousands of records of a few K each; a collection of several megabytes, but likely not 100s of megabytes) so that there is sufficient



87

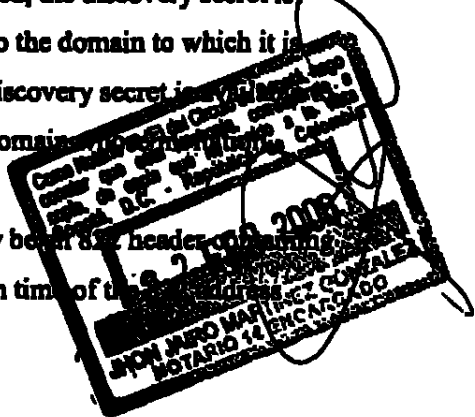
250

repair or replace hardware or do a system restore before any loss of service. In one embodiment, critical data for operation is replicated to other gateway servers. Since there is no single point of management, not all data is replicated and the replicated data is read only.

[0022] A server may engage with a number of other correspondent domains to set up mail links for a specific project. However, the management coordination of such projects does not usually scale. For secure messaging to make an impact, secure mail is enabled with the majority of the organization's business correspondents. This requires the ability to discover which correspondents have gateway servers installed and have a simple organization-to-organization workflow in order to determine whether there should be negotiation to establish a secure mail link.

[0023] The invention enables discovery of gateway servers installed in an organization's correspondents so that a secure connection can be set up. To facilitate discovery, the server indicates (e.g., advertises) the presence of itself with outbound mail by some indication (or advertisement), herein referred to as a discovery secret. To minimize the discovery secret process being vulnerable to attack, the system and method of the invention do not use a hard coded address in its discovery secret. However, it is contemplated that in one embodiment a single address may be used with a discovery secret to be included in any email to that address. As a result, only messages from parties that have seen the discovery secret (which includes the discovery secret) can send to the administrative address. Therefore, in a preferred embodiment, a single address is used, and the discovery secrets must be provided in every message. Alternatively, the indicated address is a random mailbox name which can rotate at a reasonable interval, e.g., weekly. While this random approach is an option, it is usually a less preferred embodiment. To ensure that the vulnerabilities are minimized, the discovery secret is bound to the sending domain, e.g., the source domain, and to the domain to which it is sent, e.g., the correspondent domain. In the event that the discovery secret is sent to a third party the only domain that would be affected is the domain to which the address was compromised.

[0024] In one form, the discovery secret may be an 822 header containing the ephemeral 822 address for negotiation and the expiration time of the

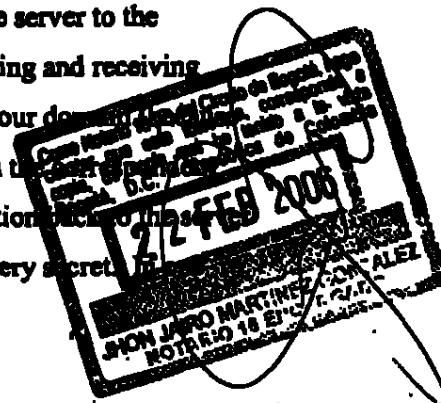


32

251

relative to when the message was sent. Inbound mail is scanned by the receiving server (e.g., correspondent or correspondent server) for discovery secrets from gateway servers and compared against a list of known gateway servers. Any additions to that list are communicated to the local administrative SMM. On discovery of a new correspondent, the SMM can send a probe message (e.g., an invitation) to the administrative address at the other SMM to offer a turn on domain signing and encryption or other services. On receipt of an invitation from another SMM administrator, if the message is verifiable under the existing trust policy then the local SMM could invoke a policy to automatically accept the invitation. Alternatively, the SMM administrator may require manual approval before accepting the invitation. On receipt of the invitation acceptance by the server, if the message is intrinsically verifiable, then the receiving SMM would invoke a policy to automatically start using domain signing and encryption. First, it sends an encrypted ping message with a nonce, and waits for an acknowledgement (that includes the nonce) to ensure that secure mail can be decrypted by the other side. Note that the invitation and acceptance messages are signed with the SMM's authoritative key, whereas the ping and acknowledgement are signed with the signing key (which is a child of the authority key). The process that does routine mail signing and encryption only has the authority to sign with the signing key (for security). Thus, the ping and acknowledgement also verify that secure mail will work with the signing key, not just the authority key. The configuration of a new secure domain is an asynchronous process and is not used for real data until the link is confirmed operationally by receipt of the ping acknowledgements before any administrative prompting.

[0025] Fig. 2 is an exemplary diagram illustrating workflow between a source domain server and a potential correspondent (e.g., target domain computer) according to the invention. Initially, a discovery secret including an administrative address, a discovery secret and an expiration date are sent from the server to the correspondent. The discovery secret should also contain the sending and receiving domains, so that one can quickly determine whether they are for your domain (and they might have been relayed as the result of a mailing list). When the correspondent recognizes the discovery secret, the correspondent sends an invitation addressed to the administrative address that was part of the discovery secret.

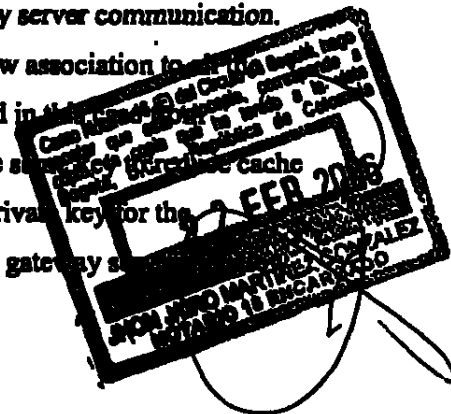


87

252

embodiment, it only responds to the discovery if it has also sent mail "to" the domain. Thus, a spammer cannot induce the source domain to invite them (because you never sent mail to them in the first place). The invitation from the correspondent includes an administrative address of the correspondent, the expiration, a certificate and the discovery secret and other information (e.g., workflow ID, contact information, sending and receiving domains, etc.). In response, the server sends an acceptance to the correspondent's administrative address from the server's administrative address and includes in the acceptance the expiration, the certificate, the discovery secret and a signature. This is administratively optional, though the default policy may include an automatic response. In one embodiment, it can also be restricted to manual, or to only respond if the inviter's certification meets some trust policy. After receipt of the acceptance, the correspondent pings the server and the ping is acknowledged by the server to establish the connection that puts the association into the ready state. It may involve an optionally automated administrative action to advance from the ready state to the active state. It may involve a further step to go from the active state (use the secure relationship but does not believe it) to the authenticated state (believe the identity claimed by the other end). If the invitation message is not verifiable using the trust policy as illustrated in Fig. 2, then the request may be cued awaiting manual approval.

[0026] Referring to Fig. 3, an exemplary block diagram illustrating a secure message manager according to the invention is illustrated. The acceptance of the invitation by the correspondent may create a cross certificate on the administrative SMM agent which is then pushed to the worker SMM agents along with the encryption certificate. (The cross certificate is usually created for authenticated associations (in order to define what they are allowed to authenticate). Active associations have everything except the cross certificate.) The cross certificate constrains the set of names accepted by the new trust and the restriction to domain gateway server communication. At this point, the certificates and information regarding that new association to all workers is distributed. The session key may also be distributed in the administration SMM to all worker SMM so all workers use the same key for the cache size. To allow for scaling out, the corresponding decryption private key for the encryption certificate should be available on all internet facing gateway servers.



90

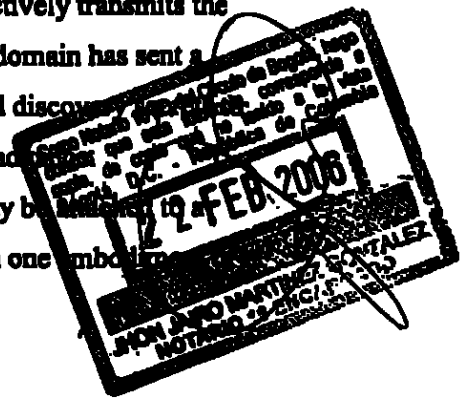
253

any to decrypt inbound mail. This is generated in a single place, i.e., the administration agent, and distributed to all worker servers. Once a trust relationship is established, it should be maintained. For example, the original certificate may be retained and a renewal request sent to the other SMMs before the certificate expires. The child encryption and signing certificate may also be updated frequently.

[0027] From the server's perspective, the method according to the invention begins the process to establish a link between a source domain and a correspondent domain. Initially, a source domain server transmits a discovery secret to potential correspondent domains via random or pseudorandom messages. The discovery secret includes a data element such as a mention or a token or other secret which is specifically assigned to the correspondent domain. The discovery secret includes a shared secret which is specific to the correspondent domain (and possibly the source domain). In the preferred embodiment, it is a hash of the seed, the correspondent domain, and the source domain (in some specified order). In addition, the discovery secret includes an address at the source domain to which the correspondent domain is permitted to send a message in order to establish a compatibility between the source domain server and the target computer. The source domain server receives an invitation from the correspondent domain which invitation is addressed to the source domain address previously provided. The invitation includes the data element in the discovery secret or an element which corresponds to the data element in the discovery secret. This allows the source domain server to initiate a process to establish compatibility between the correspondent domain server and the source domain server upon receipt by the source domain server of the invitation from the correspondent domain server. As noted in Fig. 2, the source domain server transmits an acceptance to the correspondent domain server to establish compatibility therebetween.

[0028] In one embodiment, the source domain selectively transmits the discovery secret to correspondent domains from which the source domain has sent a message. Alternatively or in addition, the source domain may send discovery secret to correspondent domains which have been specifically identified in advance.

[0029] In one embodiment, the discovery secret may be included in a message that was sent specifically to carry the discovery secret. In one embodiment,



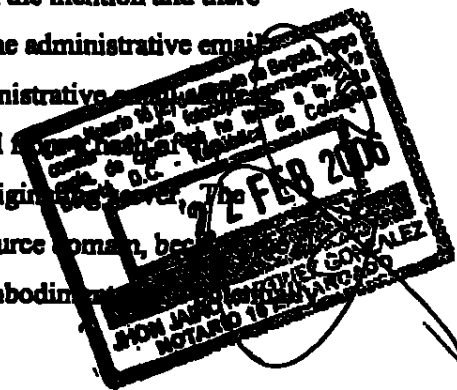
41

254

the invention, an email server occasionally adds an additional header (an "x-header") to a message that will be delivered to another email domain. The data in the header includes a secret that is specific to the correspondent domain and the email address to which the administrative messages from the correspondent domain can be directed back to the email server, as well as including the expiration, correspondent domain, sender domain, optional version, and optional features. If mail at the correspondent domain is also directed through a server that implements this embodiment of the invention, then it will detect the additional header and determine that there may be a compatible server at the originating domain. The correspondent domain then directs administrative traffic such as requests to establish a secure connection to the contained administrative email address. Such administrative messages must also contain the secret (referred to above as "discovery secret") that was provided for the correspondent domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the correspondent domain but that does not contain the secret corresponding to the correspondent domain. Although this does not provide absolute assurance that the received administrative mail is from the originating domain, it does minimize the vulnerability to SPAM at the administrative address and ensures that even an attacker that can see email to the correspondent domain can only attempt to spoof administrative addresses from the correspondent domain rather than from any domain.

[0030] In one embodiment, the invention is implemented by using a header, called a discovery secret (sometimes called a mention), that is attached to an already outbound email from the source domain. This discovery secret reveals the availability of specific functions on the mail server originating the outbound email while avoiding the need for generating additional, possibly undesirable, messages. As noted above, the administrative email address would be included in the mention and there would be a per-domain secret to mitigate risks of SPAM to the administrative email address. This would support workflow messages at the administrative email address.

[0031] The discovery secret may be generated from a hash of the source domain, the correspondent domain and a secret seed that is kept on the originating server. The discovery secret may also be generated from a hash of the source domain, because the same server may represent multiple source domains. One embodiment of the invention

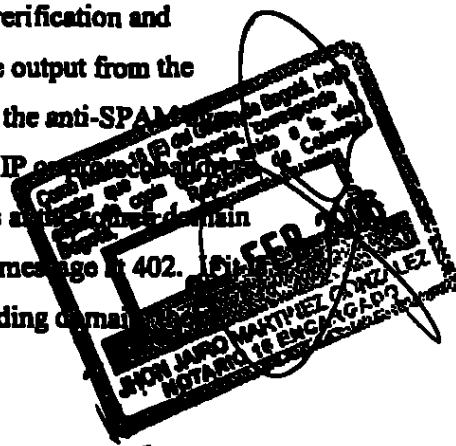


92

255

have a special "source" for all domains at the source server. This allows a single seed to be shared across multiple servers, so that each server will generate the same discovery secret unique to any correspondent domain. When an administrative message is received at the originating server (because it is directed to the administrative address included in the mention), the discovery secret provided in the administrative messages is checked by the originating server. To check the discovery secret, the email server can generate (or store) a discovery secret for the domain that sent the administrative message using the current internal seed. If the generated discovery secret is the same as the one in the administrative messages, then that message has the correct discovery secret and is passed through to the appropriate destination for negotiation messages. Negotiation messages are passed between domains. If the discovery secret does not match, then the same process is applied to prior discovery secrets (up to a bounded number). If none of the currently valid seeds can be used to generate a discovery secret that matches the discovery secret in the incoming message, then the message is not considered valid and is discarded or rejected, and not passed on to the eventual destination for administrative messages. This prevents unauthorized SPAM attacks against the receiver of administrative messages, which may be unable to cope with large volumes of email. Additionally, to prevent denial of service attacks from a domain that received a valid discovery secret, the verification process permits the server to keep track of how many messages were recently passed through to the administrative destination from a particular domain or using a particular discovery secret. When that number exceeds an allowed limit or an allowed rate, further administrative messages using that discovery secret are discarded or rejected.

[0032] Fig. 4 is a flow diagram illustrating operation of the SMM administrative routing according to the invention. The signature verification and decryption must happen before anti-SPAM processing because the output from the verification is necessary to set the message property flags used by the anti-SPAM. Signature verification should happen after the block list and other IP level functions. Thus, the process begins with receiving messages at the domain address to which the correspondent domain is permitted to send a message at 402. If determined at 404 that the discovery secret is not valid for the sending domain,



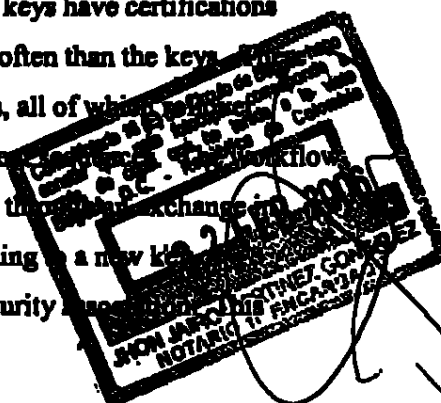
93

256

message is dropped at 406 and the routing process ends. If the discovery secret is valid, the process proceeds to 408 to determine if the domain has a maximum amount or rate which has been exceeded. If the maximum has been exceeded, the message is dropped at 406; otherwise, if the signature is valid at 410 the message is routed to the local administrative agent. However, signature verification need not happen in the worker; it usually happens in the SMM.

[0033] Fig. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention. SMM is the Secure Messaging Manager; workers are the servers that the SMM administers/controls and that do the processing of mail traffic. SMM signing and encryption is the last function generally. Each message going to a domain with a secure message association is signed and encrypted. This component also inserts the header containing the current SMM ephemeral address to all mail going to domains without a security relationship. The worker will add discovery secrets as appropriate, but it does not only do so to secure mail. As shown in Fig. 5, the domain looks for a valid signature at 502 and an external address at 504 after finding a valid discovery secret. The discovery secret is only checked in messages that claim to be for the administrator, not in normal mail. If the signature is valid and there is no external address, the message is routed to the local worker agent at 506. If there is an external address, it is routed to such. If the message appears to be domain-secured, an invalid signature is treated identically as if the signature was not present. The message source is not authenticated.

[0034] In one embodiment, the inter-organizational work flows as illustrated in Fig. 6 are implemented between administrative organizations that represent the lifecycle of a relationship. Other rollovers are possible: keys have certifications associated with them. The certifications may rollover more often than the keys. The keys are signing, encryption, and authority certifications and keys, all of which are managed independently. Also, there can be later ping/acknowledgement of the rollover. The workflow is performed by the SMM administrative agents and may go through an exchange in order to accomplish a rollover (rollover is the term for updating to a new key certificate). Fig. 7 is a state diagram illustrating the new security

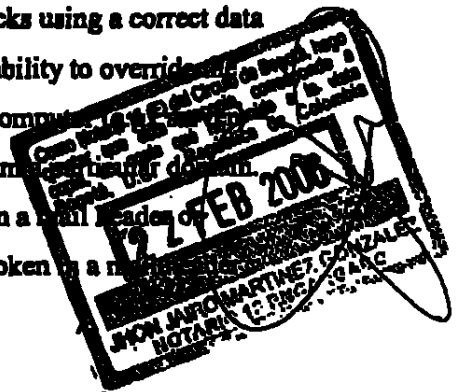


24

257

diagram only considers the positive cases and the terminal cases. It does not include other aspects such as re-transmission of messages prior to the re-transmission limit.

[0035] Other optional features of the invention include the following which may be implemented separately or in combination. The distinction between active and authenticated associations is "optional", as are all the various policies that might be applied to automatically take an administrative transition. The discovery secret may comprise an expiration date in which case the source domain server would not initiate the process to establish compatibility with the correspondent domain computer (e.g., server) computer when receipt by the source domain server of the invitation is after the expiration date so that the shared secret does not become more and more exposed over time. The data element may be at least one of the following: a per domain secret including a random or pseudorandom number for each correspondent domain computer (e.g., server), a secret generated via hashing the correspondent domain computer (e.g., server) and a secret seed that is used to generate per-domain secrets for more than one domain; and a per-domain secret generated by encrypting the correspondent domain computer (e.g., server) and an expiration date of the secret. The data element may comprise a secret in which case the source domain server could remember the secret or could verify the secret received from the correspondent domain computer (e.g., server) by re-computing and then comparing the current secret for the correspondent domain computer (e.g., server) with the secret included in the discovery secret. The data element may be selected from a plurality of multiple secrets which are valid during overlapping times for each correspondent domain computer (e.g., server) so that there are a plurality of valid secrets that can be used for communicating from a correspondent domain computer (e.g., server) to the administrative address of the originating domain. A limit may be imposed on the number of messages that are passed to the source domain server address with a particular data element so that denial of service attacks using a correct data element are mitigated. The source domain server may include the ability to override the requirement for a data element for a given correspondent domain computer to enable out-of-band authorization to send invitation messages from a correspondent domain computer. The data element may be a token in the discovery secret message in a mail header or embedded in the body of a message or the data element may be a token in a message body.



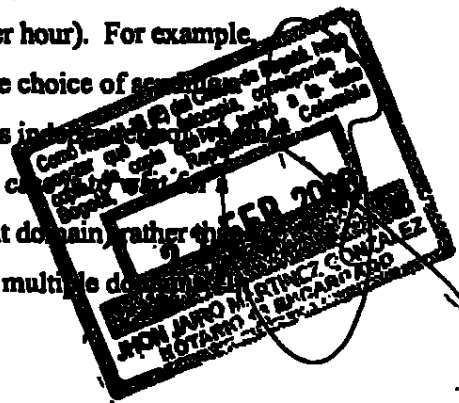
258

258

and the body of the message remains encrypted when passing through a mail server. The source domain server may support multiple simultaneously valid discovery secrets for the same domain and verify invitation messages from sub-domains of the correspondent domain computer (e.g., server) by verifying the incoming discovery secret against discovery secrets for the correspondent domain computer (e.g., server). The data element may be a discovery secret and include version information for the source domain server and include in the functions supported by the source domain server.

[0036] In one embodiment the invention comprises a data structure for the discovery secret to be transmitted from the source domain server to the correspondent domain computer (e.g., server). As noted above, this discovery secret is used to establish compatibility between the source domain server and the correspondent domain computer (e.g., server). Alternatively, it could be used for other purposes between the two domains. For example, it could be used for them to agree that they will send proprietary TNEF formats rather than text or HTML which would have nothing to do with encryption or security. The data structure includes a message and its usual header relating to the message. Additionally, the data structure includes an additional header attached to the message and message header and including a data element specific to the correspondent domain computer (e.g., server). The header also includes a source domain server address to which the correspondent domain computer (e.g., server) is permitted to send a message to the source domain server in order to establish compatibility between the source domain server and the correspondent domain computer (e.g., server). As noted above, the additional header should include an expiration date, although this is optional.

[0037] Alternatively or in addition, the discovery secret may be a message with a single correspondent domain and/or a message to a correspondent domain which is an operator. The single message to the correspondent domain may be for each key and it may be sent on a time-based determination (e.g., one message per hour). For example, the user action may be NDRs or return receipts. In particular, the choice of sending a separate message or attaching to an already being sent message is independent of whether you do it on every message or only occasionally. One crossover case is attaching the discovery secret to a message that has recipients at a single domain (the correspondent domain) rather than attaching the discovery secret to a message that has recipients at multiple domains.



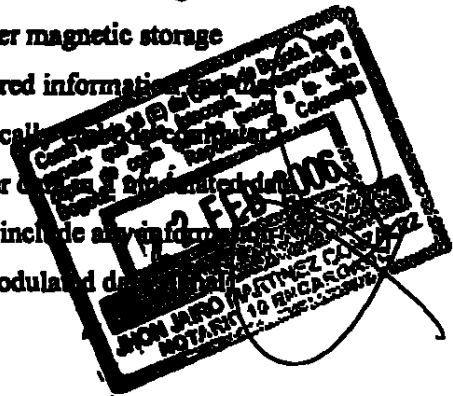
96

259

one implementation, the message is split so that the copy going to the recipients at the correspondent domain has the discovery secret for that domain.

[0038] FIG. 8 shows one example of a general purpose computing device in the form of a computer 130. In one embodiment of the invention, a computer such as the computer 130 is suitable for use in the other figures illustrated and described herein. Computer 130 has one or more processors or processing units 132 and a system memory 134. In the illustrated embodiment, a system bus 136 couples various system components including the system memory 134 to the processors 132. The bus 136 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0039] The computer 130 typically has at least some form of computer readable media. Computer readable media, which include both volatile and nonvolatile media, removable and non-removable media, may be any available medium that may be accessed by computer 130. By way of example and not limitation, computer readable media comprise computer storage media and communication media. Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. For example, computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that may be used to store the desired information. Communication media typically include any medium that facilitates the transfer of a computer readable signal such as a carrier wave or other transport mechanism and include any information delivery media. Those skilled in the art are familiar with the modulated data carrier and



72

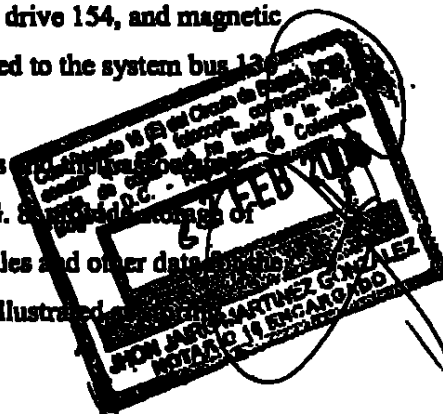
260

which has one or more of its characteristics set or changed in such a manner as to encode information in the signal. Wired media, such as a wired network or direct-wired connection, and wireless media, such as acoustic, RF, infrared, and other wireless media, are examples of communication media. Combinations of any of the above are also included within the scope of computer readable media.

[0040] The system memory 134 includes computer storage media in the form of removable and/or non-removable, volatile and/or nonvolatile memory. In the illustrated embodiment, system memory 134 includes read only memory (ROM) 138 and random access memory (RAM) 140. A basic input/output system 142 (BIOS), containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is typically stored in ROM 138. RAM 140 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 132. By way of example, and not limitation, FIG. 8 illustrates operating system 144, application programs 146, other program modules 148, and program data 150.

[0041] The computer 130 may also include other removable/non-removable, volatile/nonvolatile computer storage media. For example, FIG. 8 illustrates a hard disk drive 154 that reads from or writes to non-removable, nonvolatile magnetic media. FIG. 8 also shows a magnetic disk drive 156 that reads from or writes to a removable, nonvolatile magnetic disk 158, and an optical disk drive 160 that reads from or writes to a removable, nonvolatile optical disk 162 such as a CD-ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that may be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 154, and magnetic disk drive 156 and optical disk drive 160 are typically connected to the system bus 136 by a non-volatile memory interface, such as interface 166.

[0042] The drives or other mass storage devices are connected to the system bus 136 by a non-volatile memory interface, such as interface 166. The drives or other mass storage devices store computer storage media discussed above and illustrated in FIG. 8, such as computer readable instructions, data structures, program modules and other data for use by computer 130. In FIG. 8, for example, hard disk drive 154 is illustrated.



28

261

operating system 170, application programs 172, other program modules 174, and program data 176. Note that these components may either be the same as or different from operating system 144, application programs 146, other program modules 148, and program data 150. Operating system 170, application programs 172, other program modules 174, and program data 176 are given different numbers here to illustrate that, at a minimum, they are different copies.

[0043] A user may enter commands and information into computer 130 through input devices or user interface selection devices such as a keyboard 180 and a pointing device 182 (e.g., a mouse, trackball, pen, or touch pad). Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to processing unit 132 through a user input interface 184 that is coupled to system bus 136, but may be connected by other interface and bus structures, such as a parallel port, game port, or a Universal Serial Bus (USB). A monitor 188 or other type of display device is also connected to system bus 136 via an interface, such as a video interface 190. In addition to the monitor 188, computers often include other peripheral output devices (not shown) such as a printer and speakers, which may be connected through an output peripheral interface (not shown).

[0044] The computer 130 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 194. The remote computer 194 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to computer 130. The logical connections depicted in FIG. 8 include a local area network (LAN) 196 and a wide area network (WAN) 198, but may also include other networks. LAN 136 and/or WAN 138 may be a wired network, a wireless network, a combination thereof, and so on. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and global computer networks (e.g., the Internet).

[0045] When used in a local area networking environment, computer 130 is connected to the LAN 196 through a network interface or adapter. When used in a wide area networking environment, computer 130 typically includes a modem 150 or other means for establishing communications over the WAN 198, such as a network interface or adapter.



29

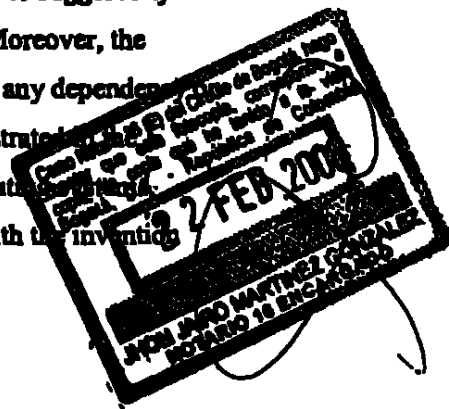
262

The modem 178, which may be internal or external, is connected to system bus 136 via the user input interface 184, or other appropriate mechanism. In a networked environment, program modules depicted relative to computer 130, or portions thereof, may be stored in a remote memory storage device (not shown). By way of example, and not limitation, FIG. 8 illustrates remote application programs 192 as residing on the memory device. The network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0046] Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described below in conjunction with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described herein.

[0047] For purposes of illustration, programs and other executable program components, such as the operating system, are illustrated herein as discrete blocks. It is recognized, however, that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.

[0048] Although described in connection with an exemplary computing system environment, including computer 130, the invention is operational with numerous other general purpose or special purpose computing system environments or configurations. The computing system environment is not intended to suggest any limitation as to the scope of use or functionality of the invention. Moreover, the computing system environment should not be interpreted as having any dependence requirement relating to any one or combination of components illustrated in the exemplary operating environment. Examples of well known computing environments, and/or configurations that may be suitable for use with the invention



107

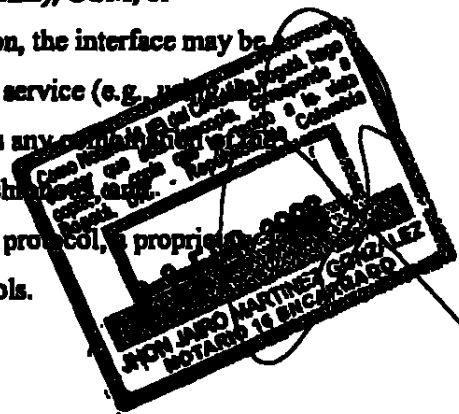
263

include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0049] The invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0050] An interface in the context of a software architecture includes a software module, component, code portion, or other sequence of computer-executable instructions. The interface includes, for example, a first module accessing a second module to perform computing tasks on behalf of the first module. The first and second modules include, in one example, application programming interfaces (APIs) such as provided by operating systems, component object model (COM) interfaces (e.g., for peer-to-peer application communication), and extensible markup language metadata interchange format (XMI) interfaces (e.g., for communication between web services).

[0051] The interface may be a tightly coupled, synchronous implementation such as in Java 2 Platform Enterprise Edition (J2EE), COM, or distributed COM (DCOM) examples. Alternatively or in addition, the interface may be loosely coupled, asynchronous implementation such as in a web service (e.g., using a simple object access protocol). In general, the interface includes any of the following characteristics: tightly coupled, loosely coupled, synchronous, asynchronous. Further, the interface may conform to a standard protocol, a proprietary protocol, or any combination of standard and proprietary protocols.



101

264

[0052] The interfaces described herein may all be part of a single interface or may be implemented as separate interfaces or any combination therein. The interfaces may execute locally or remotely to provide functionality. Further, the interfaces may include additional or less functionality than illustrated or described herein.

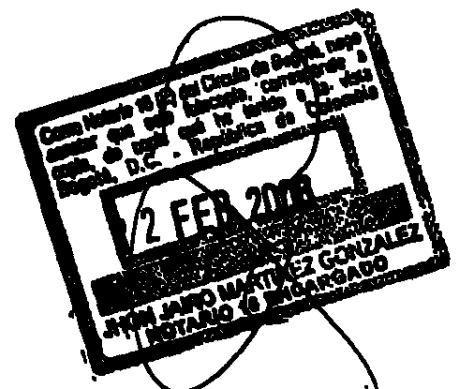
[0053] In operation, computer 130 operates as either the source domain server or the correspondent domain computer (which may be a server) to execute computer-executable instructions as noted above, such as those illustrated in Figs. 2-7.

[0054] The order of execution or performance of the methods illustrated and described herein is not essential, unless otherwise specified. That is, elements of the methods may be performed in any order, unless otherwise specified, and that the methods may include more or less elements than those disclosed herein. For example, it is contemplated that executing or performing a particular element before, contemporaneously with, or after another element is within the scope of the invention.

[0055] When introducing elements of the present invention or the embodiment(s) thereof, the articles "a," "an," "the," and "said" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0056] In view of the above, it will be seen that the several objects of the invention are achieved and other advantageous results attained.

[0057] As various changes could be made in the above constructions, products, and methods without departing from the scope of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.



102

265

What is claimed is:

1. A method for determining that a potential correspondent domain has compatible secure email technology in order to establish a link between a source domain and a correspondent domain comprising:

Transmitting a discovery secret from the source domain to the correspondent domain wherein the discovery secret includes a data element specific to the correspondent domain and wherein the discovery secret includes a source domain address to which the correspondent domain is permitted send a message in order to establish compatibility between the source domain and the correspondent domain; and

Receiving by the source domain via the source domain address an invitation from the correspondent domain wherein the invitation includes the data element or an element corresponding to the data element which may be used by the correspondent domain to initiate a process to establish compatibility with the correspondent domain.

2. The method of claim 1 further comprising transmitting an acceptance from the source domain to the correspondent domain to establish that the correspondent and source domains have compatible secure email technology or other email or communication technology.

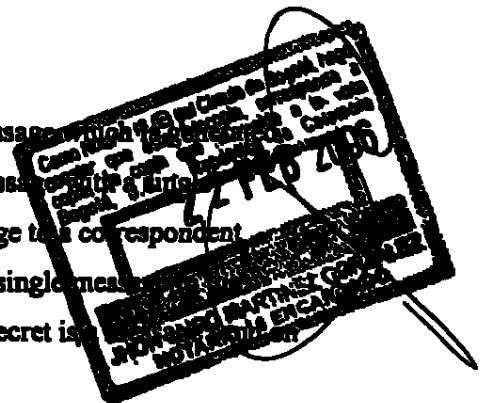
3. The method of claim 1 wherein the discovery secret is selectively transmitted to at least one of the following:

Correspondent domains from which the source domain has received a message;

Correspondent domains specifically identified in advance; and

Correspondent domains via randomly selected messages.

4. The method of claim 1 wherein the discovery secret is a message in response to user action; wherein the discovery secret is a message to a correspondent domain; wherein the discovery secret is a message to a correspondent domain which is an operator; wherein the discovery secret is a single message to a correspondent domain for each key; or wherein the discovery secret is a time-based determination.



103

266

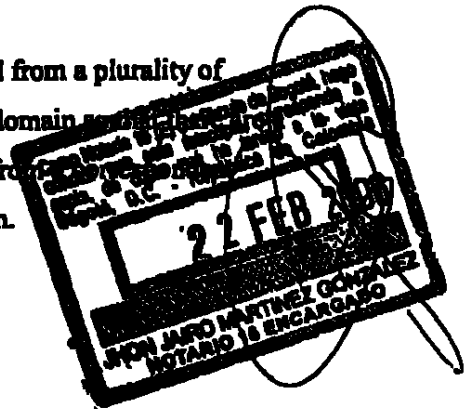
5. The method of claim 1 wherein the discovery secret comprises an additional header which includes the data element and the source domain address.

6. The method of claim 1 wherein the discovery secret comprises an expiration date and wherein the source domain does not establish that the correspondent and source domains have compatible secure email technology when receipt by the source domain of the invitation is after the expiration date.

7. The method of claim 1 wherein the data element is at least one of the following:
a per domain secret including a random or pseudorandom number for each correspondent domain;
a secret generated via hashing the correspondent domain and a secret seed that is used to generate per-domain secrets for more than one domain; and
a per-domain secret generated encrypting the correspondent domain and an expiration date of the secret.

8. The method of claim 1 wherein the data element comprises a secret and wherein the source domain verifies the secret received from the correspondent domain by re-computing and then comparing the current secret for the correspondent domain with the secret included in the discovery secret whereby the source domain only corresponds with potential correspondent domains which provide the secret so that denials of service attacks from correspondence domains is mitigated.

9. The method of claim 1 wherein the data element is selected from a plurality of multiple simultaneously valid secrets for each correspondent domain so that a plurality of valid secrets that can be used for communicating from the correspondent domain to the administrative address of the originating domain.



64

267

10. The method of claim 1 further comprising imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of service attacks using a correct data element are mitigated.

11. The method of claim 1 further comprising including the ability to override the requirement for a data element for a given correspondent domain to enable out-of-band authorization to send invitation messages from a particular domain.

12. The method of claim 1 wherein the data element is a token in the discovery secret message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server.

13. The method of claim 1 further comprising supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the correspondent domain by verifying the incoming token against tokens for the correspondent domain.

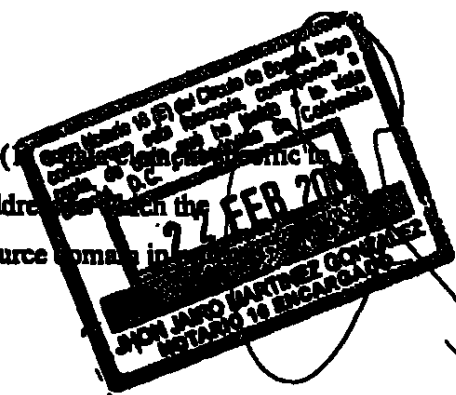
14. The method of claim 1 wherein the data element is a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

15. A data structure for a discovery secret to be transmitted from a source domain to a correspondent domain for establishing that the correspondent and source domains have compatible secure email technology comprising:

A message;

A header relating to the message; and

An additional header attached to the message and including (1) a version number for the correspondent domain and including a source domain address to which the correspondent domain is permitted send a message to the source domain in



101

268

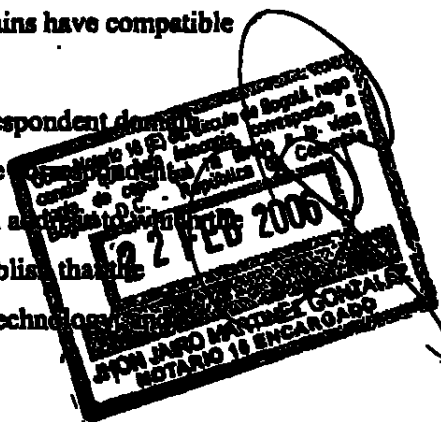
establish that the correspondent and source domains have compatible secure email technology, (2) a discovery secret and (3) an expiration date.

16. The data structure of claim 15 wherein the data element is at least one of the following:

- a per domain secret including a random or pseudo-random number for each correspondent domain,
- a secret generated via hashing the correspondent domain and a secret seed that is used to generate per-domain secrets for more than one domain;
- a per-domain secret generated encrypting the correspondent domain and an expiration date of the secret;
- a secret and wherein the source domain verifies the secret received from the correspondent domain by re-computing and then comparing the current secret for the correspondent domain with the secret included in the discovery secret;
- a data element is selected from a plurality of multiple overlapping secrets for each correspondent domain so that there are a plurality of valid secrets that can be used for communicating from a correspondent domain to the administrative address of the originating domain;
- a token in the discovery secret message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server; and
- a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

17. A system for establish that the correspondent and source domains have compatible secure email technology, comprising:

- A source domain server transmitting a discovery secret to the correspondent domain wherein the discovery secret includes a data element specific to the domain and wherein the discovery secret includes a source domain address;
- wherein the correspondent domain is permitted send a message in order to establish that the correspondent and source domains have compatible secure email technology;



105

269

A correspondent domain computer receiving the discovery secret including the data element and the source domain address wherein the correspondent domain computer transmits an invitation from the correspondent domain to the source domain address wherein the invitation includes the data element or an element corresponding to the data element.

18. The system of claim 17 wherein the source domain server transmits an acceptance from the source domain to the correspondent domain to establish that the correspondent and source domains have compatible secure email technology and wherein the source domain server initiates a process to establish a link with the correspondent domain computer upon receipt by the source domain server of the invitation; and further comprising at least one of the following:
 imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of Service attacks using a correct data element are mitigated;
 overriding the requirement for a data element for a given correspondent domain to enable out-of-band authorization to send invitation messages from a particular domain; and
 supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the correspondent domain by verifying the incoming discovery secret against discovery secrets for the correspondent domain.

19. The system of claim 17 wherein the discovery secret transmitted by the source domain service comprises at least one of the following:

- A discovery secret selectively transmitted to correspondent domains from which the source domain has received a message;
- a discovery secret selectively transmitted to correspondent domains specifically identified in advance or randomly selected correspondent domains;
- a message which is generated in response to user action;
- a message with a single correspondent domain;
- a message to a correspondent domain which is a server's operator address;
- a single message to the correspondent domain for each key;

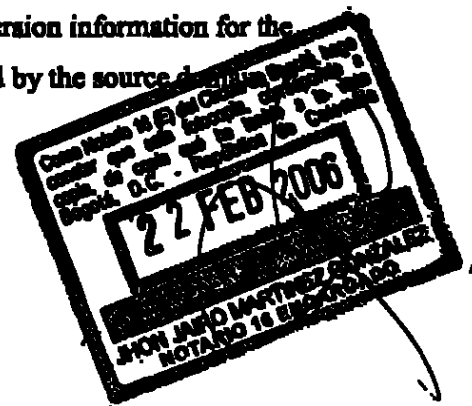


107

270

a message send on a time-based determination;
 an additional header which includes the data element and the source domain address; and
 an expiration date and wherein the source domain does not initiate the process to
 establish a link with the correspondent domain when receipt by the source domain of the
 invitation is after the expiration date.

20. The system of claim 17 wherein the data element is at least one of the following:
 a per domain secret including a random or pseudorandom number for each correspondent
 domain,
 a secret generated via hashing the correspondent domain and a secret seed that is used to
 generate per-domain secrets for more than one domain;
 a per-domain secret generated encrypting the correspondent domain and an expiration
 date of the secret;
 a secret and wherein the source domain verifies the secret received from the
 correspondent domain by re-computing and then comparing the current secret for the
 correspondent domain with the secret included in the discovery secret;
 a data element is selected from a plurality of multiple overlapping secrets for each
 correspondent domain so that there are a plurality of valid secrets that can be used for
 communicating from a correspondent domain to the administrative address of the
 originating domain;
 a token in the discovery secret message in a mail header or embedded in the body of a
 message or wherein the data element is a token in a mail header and the body of the
 message remains encrypted when passing through a mail server; and
 a mention and further comprising including in the mention of version information for the
 source domain and including in the mention functions supported by the source domain

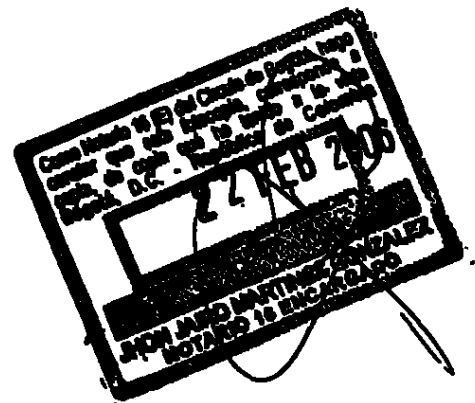


108

271

ABSTRACT

A discovery secret is transmitted from the source domain to the correspondent domain. The discovery secret includes a data element specific to the correspondent domain and. The discovery secret includes a source domain address to which the correspondent domain is permitted send a message in order to determine that a potential correspondent has compatible secure email technology so that a link between the source domain and the correspondent domain may be established. The discovery secret is received by the correspondent domain including receiving the data element and the source domain address. An invitation is transmitted from the correspondent domain to the source domain address. The invitation includes the data element or an element corresponding to the data element. The source domain initiates a process to establish a link with the correspondent domain upon receipt by the source domain of the invitation.



109

PATENT APPLICATION

DECLARATION AND POWER OF ATTORNEY

ATTORNEY DOCKET NO. MSFT 8189.1

MS DOCKET NO. 311610.02

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL

the specification of which is filed herewith unless the following box is checked:

☐ was filed on _____ as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claims of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: _____ NO: _____
			YES: _____ NO: _____

POWER OF ATTORNEY

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) associated with

Continuation No. 000000779

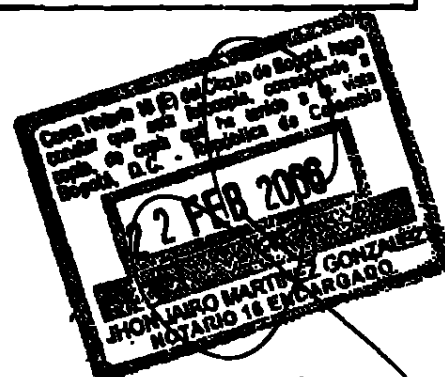
to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Send Correspondence to:

Frank R. Agovino
Senniger, Powers, Lawitt & Rosdal
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63103

Direct Telephone Calls To:

Frank R. Agovino
(314) 231-5400



BEST AVAILABLE COPY

273

DECLARATION AND POWER OF ATTORNEY
ATTORNEY DOCKET NO. MSPT 5169.1 **MS DOCKET NO. 311610.02**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: Eric D. Tribble

Citizenship: US

Residence: Redmond, Washington

Post Office Address: One Microsoft Way, Redmond, Washington 98052-6399


Inventor's Signature

4/14/05
Date

Full Name of Inventor: Trevor W. Freeman

Citizenship: Great Britain

Residence: Redmond, Washington

Post Office Address: One Microsoft Way, Redmond, Washington 98052-6399


Inventor's Signature

4/14/05
Date

FRACwa



BEST AVAILABLE COPY

111

FIG. 1

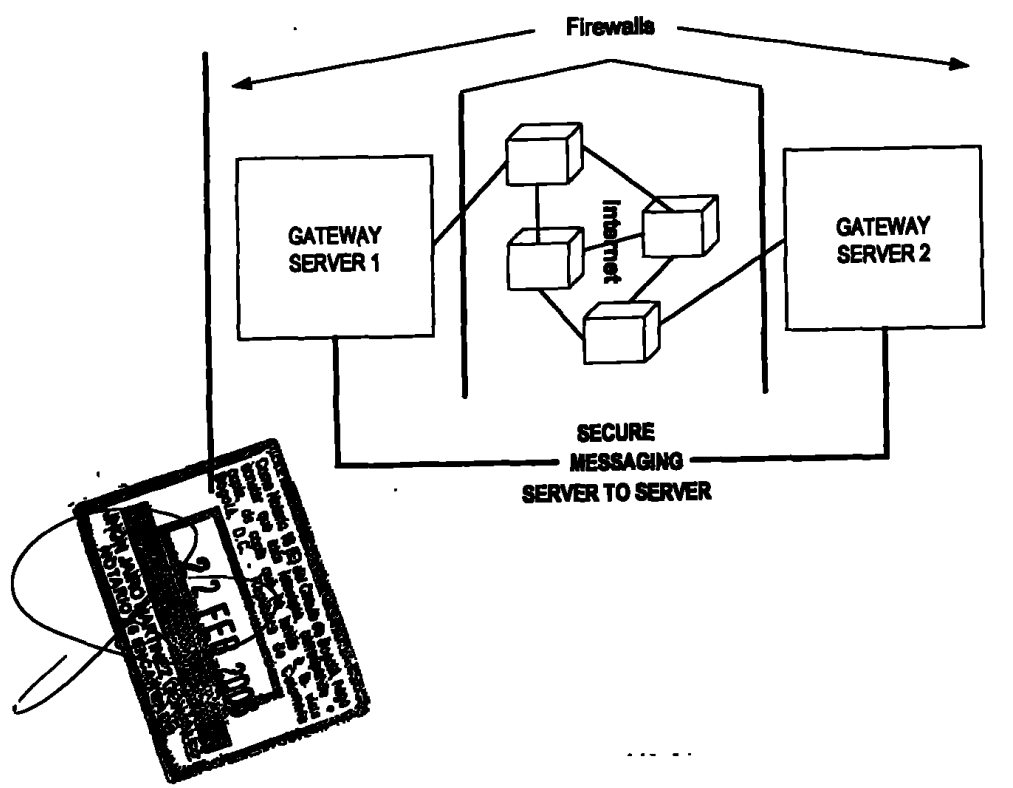
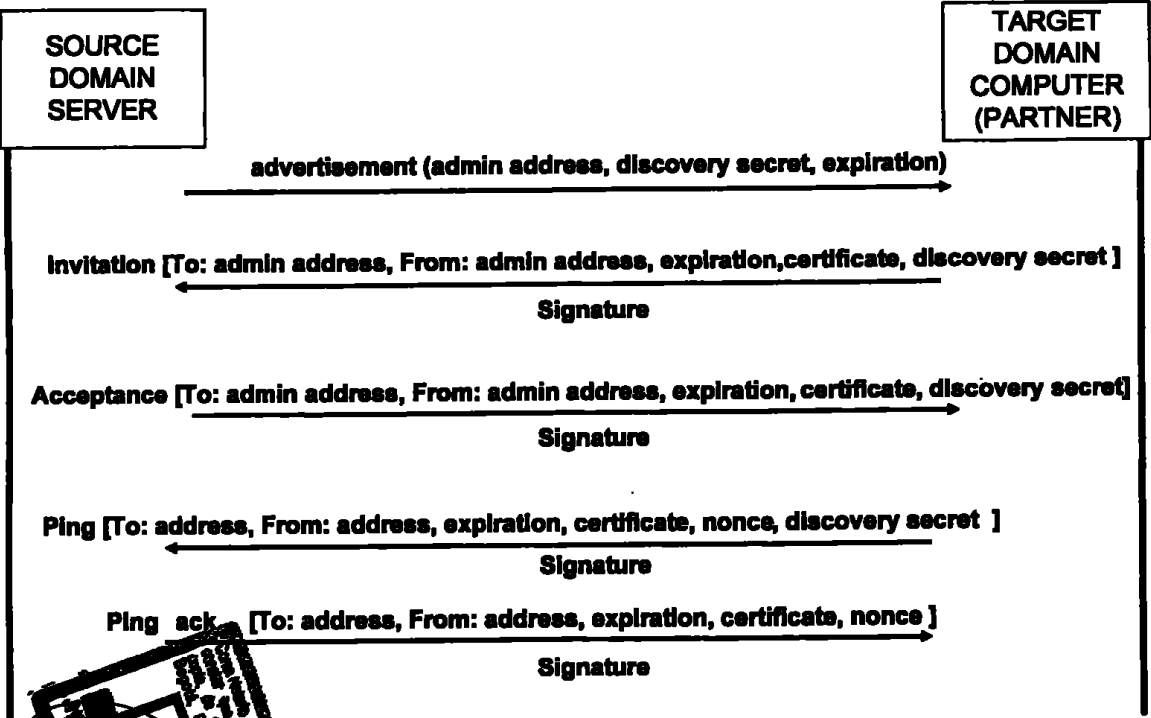


FIG. 2



2/8

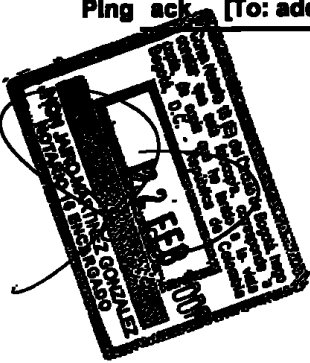


FIG. 3

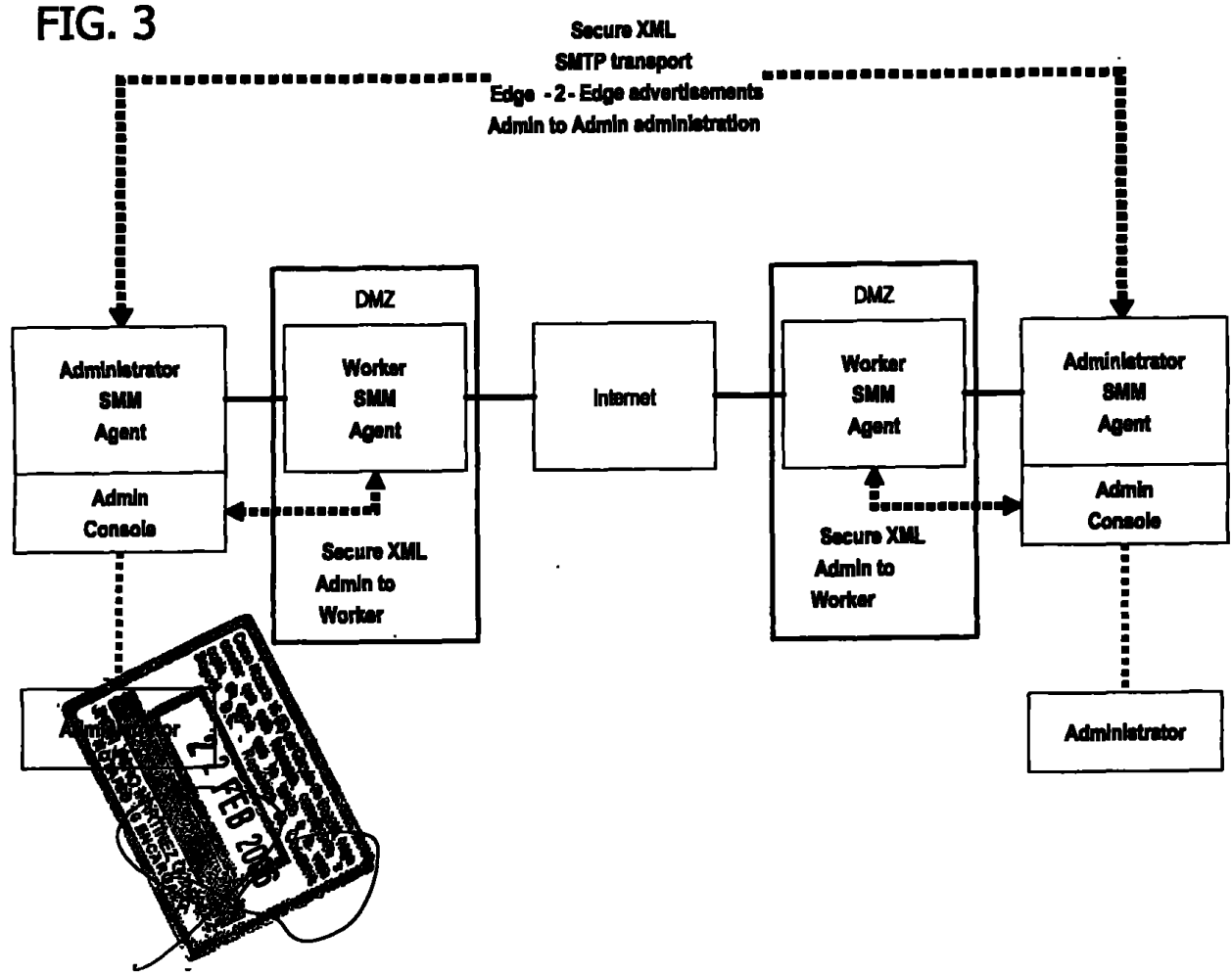


FIG. 4

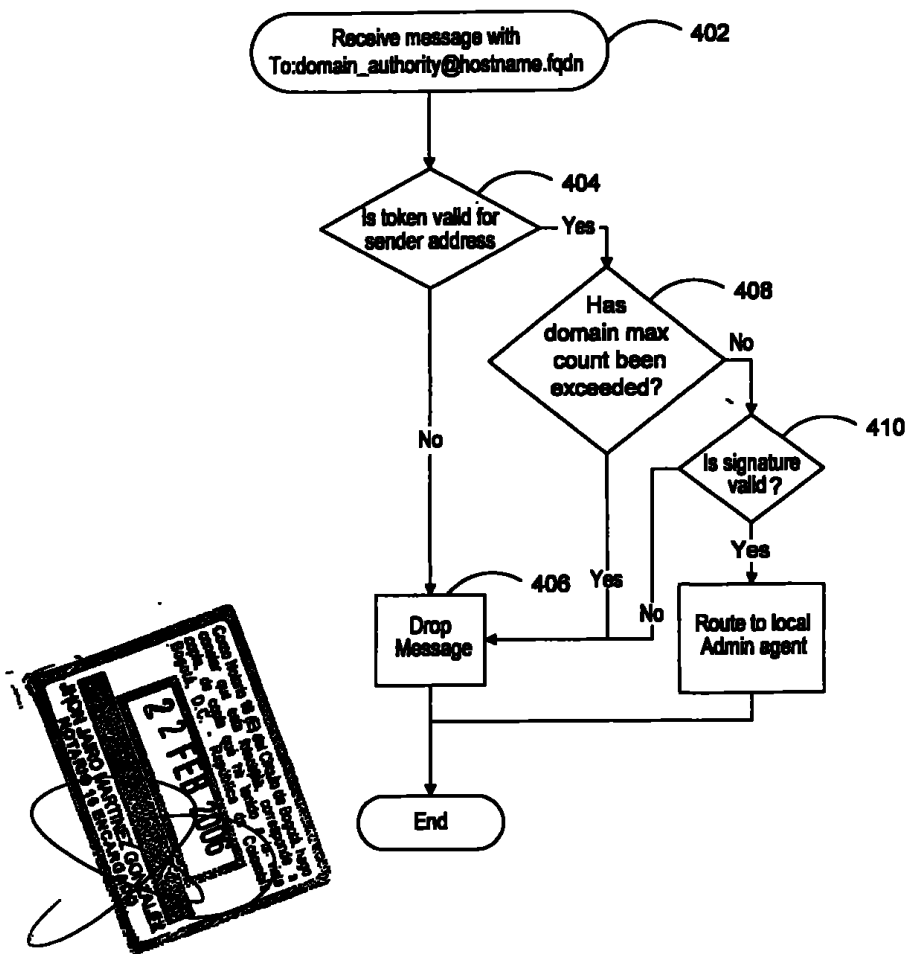


FIG. 5

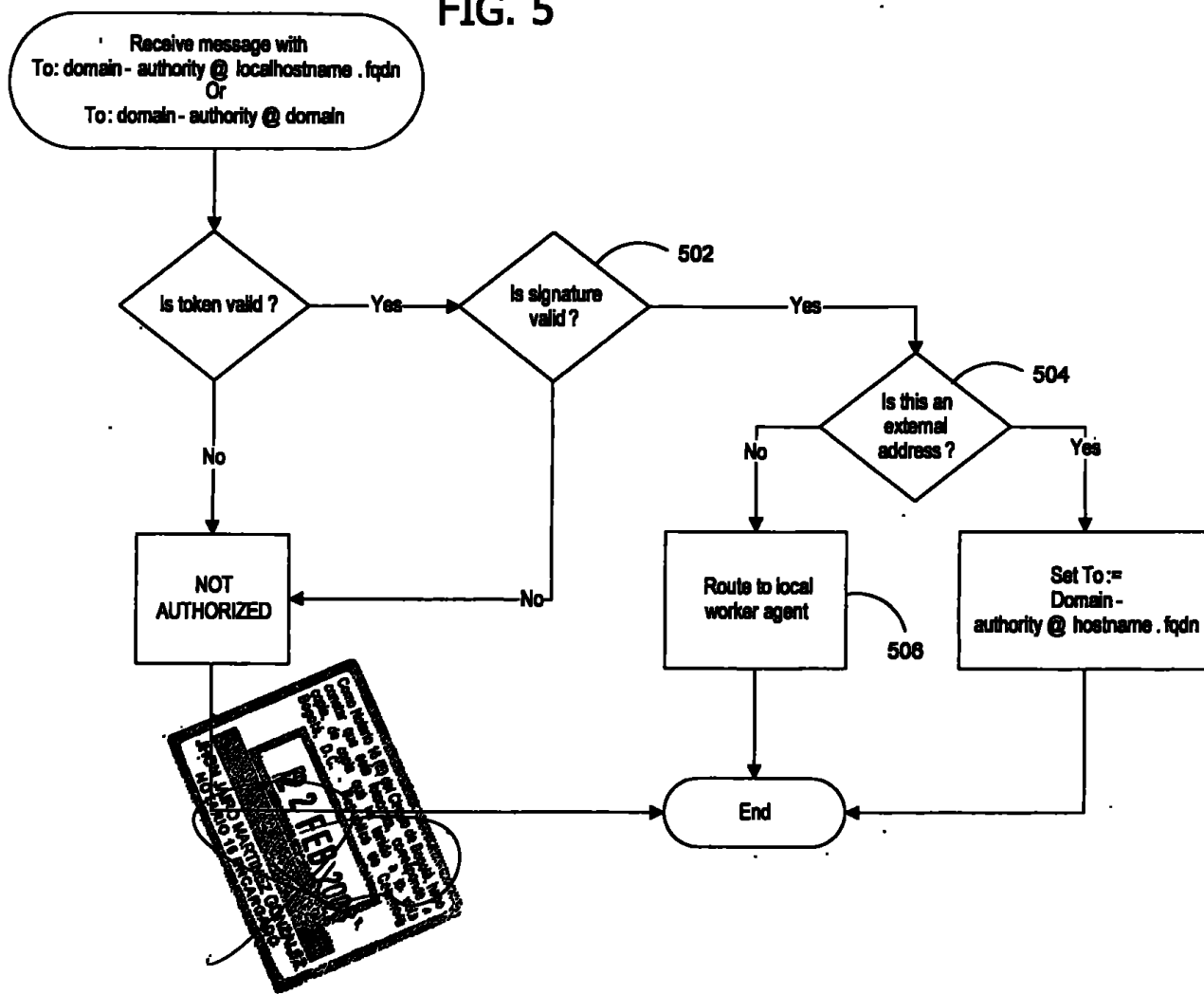


FIG. 6

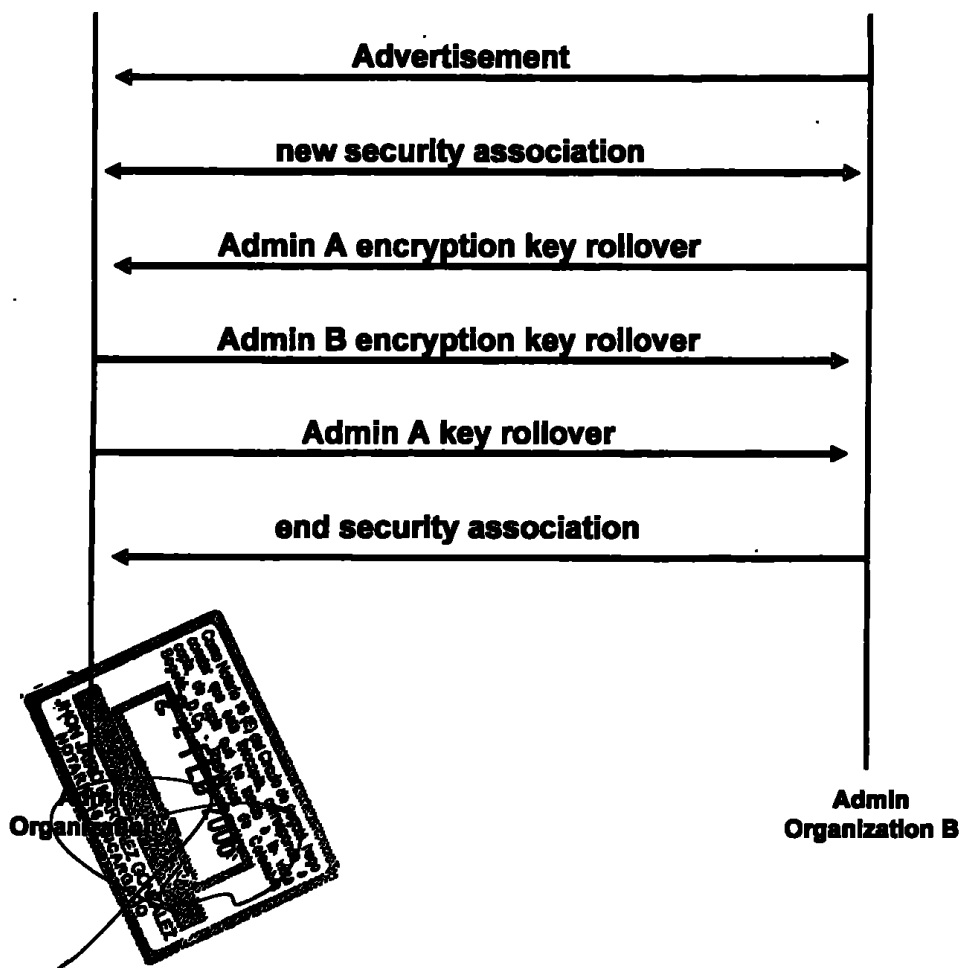
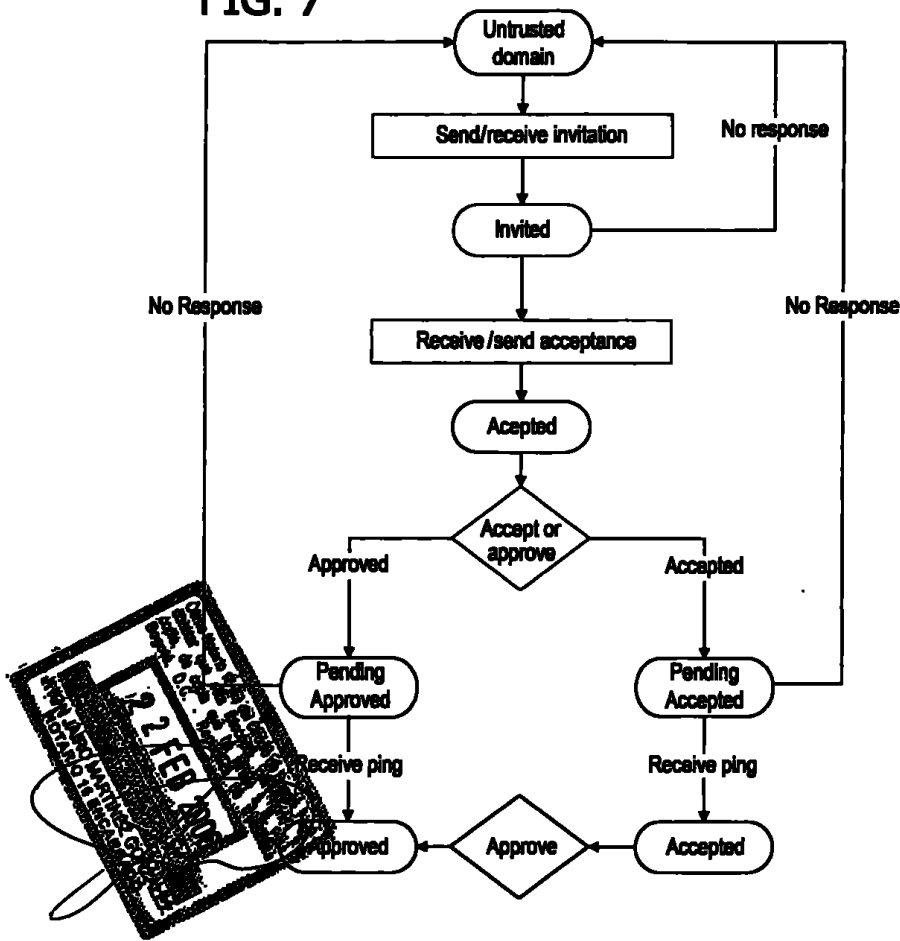
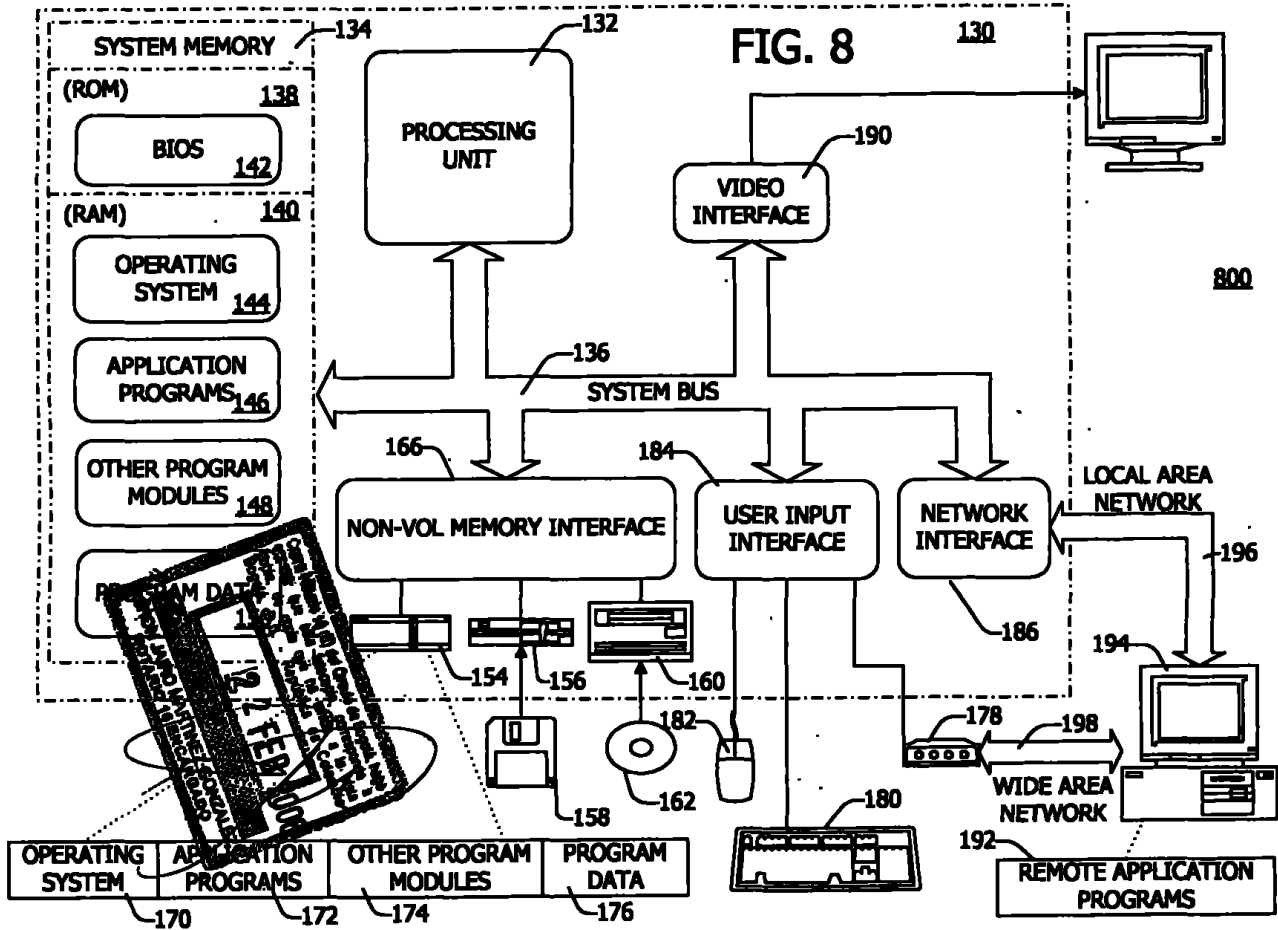


FIG. 7



112



282

APPLICATION DATA SHEET

Application Information

Application Type:: Regular
Subject Matter:: Utility
Suggested Classification::
Suggested Group Art Unit::
Title:: SYSTEM AND METHOD FOR
ESTABLISHING THAT A SERVER AND
A CORRESPONDENT HAVE COMPATIBLE
SECURE EMAIL
Attorney Docket Number:: MS#311610.02 (5169.1)
Request for Early Publication?:: No
Request for Non-Publication?:: No
Suggested Drawing Figure:: 1
Total Drawing Sheets:: 8
Small Entity?:: No
Petition Included?:: No

Applicant Information

Applicant Authority Type:: Inventor
Primary Citizenship Country:: US
Status:: Full Capacity
Given Name:: Eric
Middle Name:: D.
Family Name:: Tribble
City of Residence:: Redmond
State or Province of Residence:: WA
Country of Residence:: US
Street of Mailing Address:: 15600 NE 8th Street
City of Mailing Address:: Bellevue
State or Province of Mailing
Address:: WA
Country of Mailing Address:: US
Postal Code of Mailing Address:: 98008



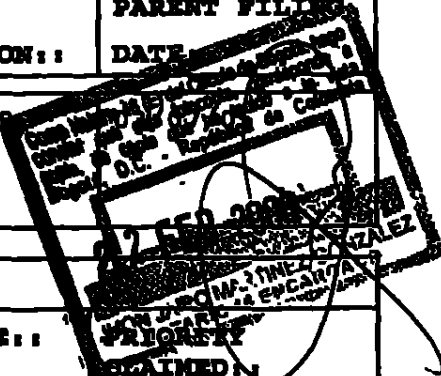
120

283

Applicant Authority Type:: Inventor
Primary Citizenship Country:: Great Britain
Status:: Full
Given Name:: Trevor
Middle Name:: W.
Family Name:: Freeman
City of Residence:: Sammamish
State or Province of Residence:: WA
Country of Residence:: US
Street of Mailing Address:: 2022 236th Avenue SE
City of Mailing Address:: Sammamish
State or Province of Mailing Address:: WA
Country of Mailing Address:: US
Postal Code of Mailing Address:: 98075

Correspondence Information
Correspondence Customer Number:: 000038779

Representative Information
Representative Customer Number:: 000038779

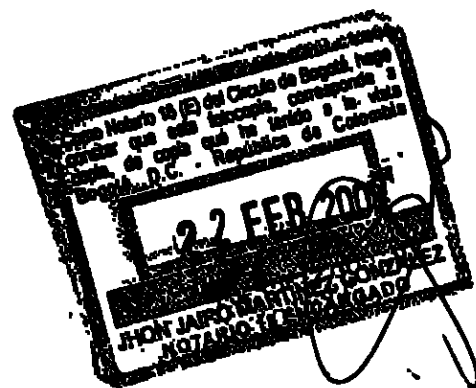
Domestic Priority Information			
APPLICATION::	CONTINUITY TYPE::	PARENT APPLICATION::	PARENT FILING DATE
This application	An application claiming the benefit under 35 USC 119(e)	60/659,279	
Foreign Priority Information			
COUNTRY::	APPLICATION NUMBER::	FILING DATE::	

121

284

Assignee Information

Assignee Name::	Microsoft Corporation
Street of Mailing Address::	One Microsoft Way
City of Mailing Address::	Redmond
State or Province of	
Mailing Address::	WA
Country of Mailing Address::	US
Postal or Zip Code of	
Mailing Address::	98052



122

295

TRADUCCIÓN DEL INGLÉS AL ESPAÑOL DE UNA PORCIÓN DE UN DOCUMENTO ORIGINAL ENTREGADO EN UNA CARPETA DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DEL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS, CON COBERTURA DE PLÁSTICO TRANSPARENTE, REALIZADA POR NORA JIMÉNEZ DE ADAM, TRADUCTORA E INTÉRPRETE OFICIAL. TEL: 571-2572804; FEBRERO 8 DE 2006

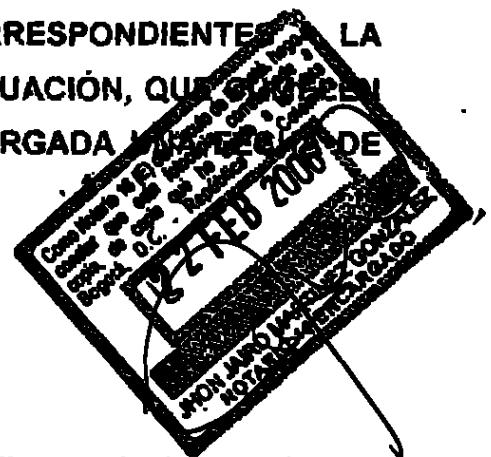
Emitido en papelería especial con reborde negro-gris con el número PA 1409083 en la parte superior izquierda del documento: "ESTADOS UNIDOS DE AMÉRICA - A TODOS LOS BENEFICIARIOS DE ESTE DOCUMENTO: EL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS Oficina de Patentes y Marcas Registradas de los Estados Unidos

Diciembre 28 de 2005

ESTE DOCUMENTO CERTIFICA QUE LOS ANEXOS SON COPIA FIEL DE LOS DOCUMENTOS REGISTRADOS EN LA OFICINA DE PATENTES Y MARCAS REGISTRADAS DE LOS ESTADOS UNIDOS CORRESPONDIENTES A LA SOLICITUD DE PATENTE IDENTIFICADA A CONTINUACIÓN, QUE SE ADECUAN CON LOS REQUISITOS PARA QUE LES SEA OTORGADA LA MARCA DE REGISTRO DE ACUERDO CON 35 USC 111.

NÚMERO DE SOLICITUD: 60/659,279

FECHA DE REGISTRO: 7 de marzo de 2005



EL CÓDIGO DE PAÍS Y EL NÚMERO DE SOLICITUD DE PRIORIDAD A SER UTILIZADO PARA SU REGISTRO EN EL EXTRANJERO SEGÚN LA CONVENCION DE PARÍS ES EL US60/659.279

123

286

Estampilla dorada del Departamento de Comercio - Oficina de Patentes y Marcas Registradas de los Estados Unidos

Bajo la potestad del SUBSECRETARIO DE COMERCIO PARA LA PROPIEDAD INTELECTUAL Y DIRECTOR DE LA OFICINA DE PATENTES Y MARCAS REGISTRADAS

(Firma)

M. BASSFORD

Funcionario de Certificaciones

SEGUNDA PÁGINA: Papel blanco con lo siguiente: SELLADO CON LOS NÚMEROS 112935 DEL U.S. PTO - 60/659279. CÓDIGO DE BARRAS 030705. A LA IZQUIERDA: SELLO CON EL NÚMERO 22713 U.S. PTO SEGUIDO DEL CÓDIGO DE BARRAS CON EL NÚMERO 030705.

Comisionado de Patentes

P.O. Box 1450

Alexandria, Virginia 22313 - 1450

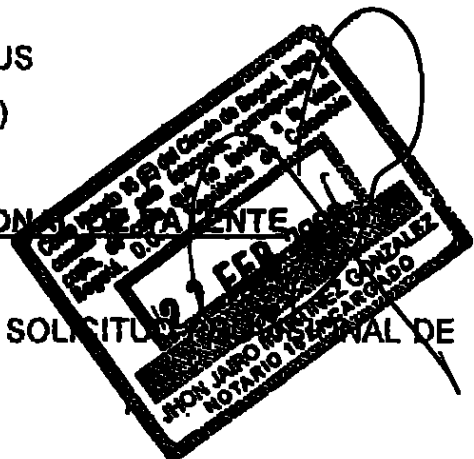
No. de Etiqueta de Correo Expreso EV453251602US

Expediente de Abogado No. MS#311610.01 (5169)

CUBIERTA DE SOLICITUD PROVISIONAL

Esta es una solicitud para la presentación de una SOLICITUD DE PATENTE según 37 CFR 1.53 (c).

INVENTOR (ES):



124

287

1. Tribble, Eric D.

APELLIDO NOMBRE INICIAL DEL SEGUNDO NOMBRE

Redmond, WA

RESIDENCIA (CIUDAD Y YA SEA ESTADO O PAÍS EXTRANJERO)

2. Freeman, Trevor W.

APELLIDO NOMBRE INICIAL DEL SEGUNDO NOMBRE

Redmond, WA

RESIDENCIA (CIUDAD Y YA SEA ESTADO O PAÍS EXTRANJERO)

3. _____

APELLIDO NOMBRE INICIAL DEL SEGUNDO NOMBRE

RESIDENCIA (CIUDAD Y YA SEA ESTADO O PAÍS EXTRANJERO)

_ Se nombran inventores adicionales en las _ hoja (s) numeradas separadas que se encuentran anexas.

Título del Invento: SISTEMA Y MÉTODO PARA ESTABLECER UN VÍNCULO ENTRE UN SERVIDOR Y UN OBJETIVO

Dirección de Correspondencia: Número de cliente 006

1

Copia suministrada por USPTO de la Base de Datos de Patentes IFW el
12/23/2005



125

248

TERCERA PÁGINA:

PARTES DE LA SOLICITUD ADJUNTAS:

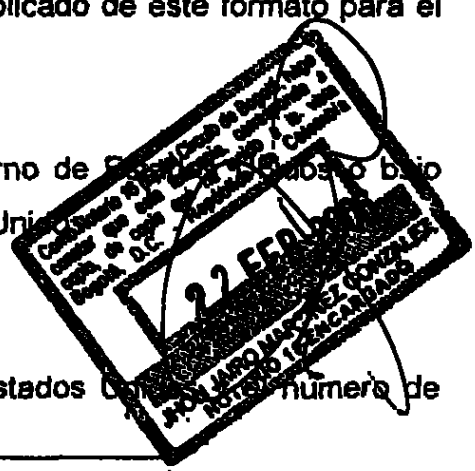
- ☒ Especificación (No. de páginas 24)
- ☒ Gráficas (No. de páginas 8)
- ☒ Ficha técnica de la solicitud
- ☐ CD (s), Número
- ☒ Carta de acuse de recibo
- ☐ Otros (especifique) _____

MÉTODO DE PAGO DE GASTOS DE PRESENTACIÓN

- ☐ El solicitante reivindica su condición de pequeña entidad.
- ☐ Se anexa un cheque por valor de \$_____ para cubrir los gastos de presentación (y los gastos por tamaño de la solicitud, si aplican). El Comisionado queda autorizado por el presente para debitar cualquier pago o acreditar cualquier exceso de pago a la Cuenta de Depósito No. 19-1345.
- ☒ El Comisionado queda autorizado por el presente a debitar los gastos indicados (y los gastos por tamaño de la solicitud, si aplican) de la cuenta de Depósito No. 19-1345. Se anexa una copia en duplicado de este formato para el procesamiento de gastos.

El invento fue creado por una agencia del gobierno de Estados Unidos o bajo contrato con una agencia del gobierno de Estados Unidos.

- ☒ No
- ☐ Sí, el nombre de la agencia del gobierno de Estados Unidos y el número de contrato con el Gobierno son: _____



128

289

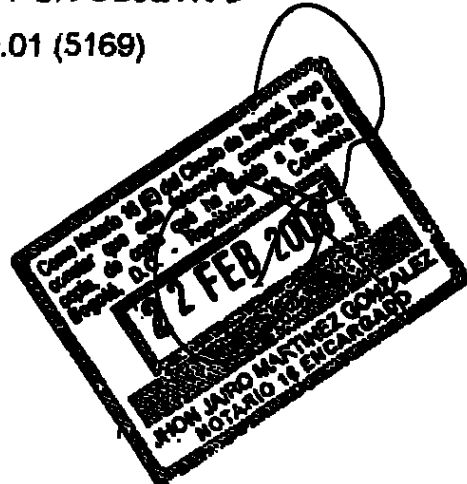
Respetuosamente,
(Firma)
Frank R. Agovino -Reg. No. 27,416
Fecha: marzo 7 de 2005
FRA/dep

Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el
12/23/2005

CUARTA PÁGINA:

FICHA TÉCNICA DE LA SOLICITUD
INFORMACIÓN DE LA SOLICITUD

Tipo de solicitud:	Provisional
Asunto:	Utilidad
Clasificación Propuesta:	En blanco
Unidad de Grupo de Arte Propuesta:	En blanco
Título:	SISTEMA Y MÉTODO PARA ESTABLECER UN VÍNCULO ENTRE UN SERVIDOR Y UN OBJETIVO
Expediente del Abogado:	MS#311610.01 (5169)
Solicitud de Publicación Anticipada:	En blanco
Solicitud de No publicación:	En blanco
Figura Gráfica Propuesta:	En blanco
Total Hojas de Gráficas:	8
Pequeña Entidad:	NO
Petición incluida:	NO
Tipo de Petición:	En blanco



127

290

Agencia Lic. del Gob. De USA: En blanco
No. De Contrato o Adjudicación: En blanco
Orden de Confid. En Sol. Principal: En blanco

INFORMACIÓN DEL SOLICITANTE

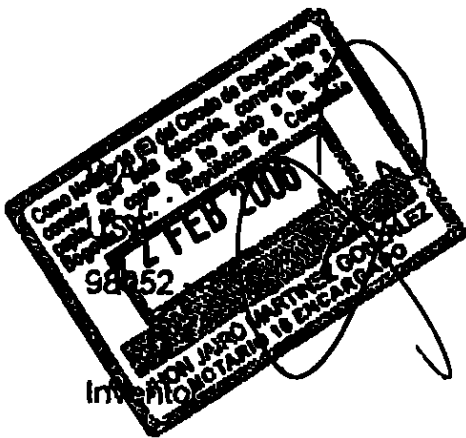
Tipo de Autoridad del Solicitante: Inventor
País de Ciudadanía Principal: USA
Condición: Plena capacidad
Primer Nombre: Eric
Segundo Nombre: D.
Apellido: Tribble
Sufijo del Nombre: En blanco
Ciudad de Residencia: Redmond
Estado o Provincia de residencia: WA
País de Residencia: USA
Calle de la Dirección Postal: One Microsoft Way
Ciudad de la Dirección Postal: Redmond

Copia suministrada por USPTO de la Base de Datos de Imágenes IFW el 12/23/2005

QUINTA PÁGINA:

Estado o Provincia de la Dirección Postal:
País de la Dirección Postal:
Código Postal de la Dirección Postal:

Tipo de Autoridad del Solicitante:



128

291

País de Ciudadanía Principal: US
Condición: Plena capacidad
Primer Nombre: Trevor
Segundo Nombre: W.
Apellido: Freeman
Sufijo del Nombre: En blanco
Ciudad de Residencia: Redmond
Estado o Provincia de residencia: WA
País de Residencia: USA
Calle de la Dirección Postal: One Microsoft Way
Ciudad de la Dirección Postal: Redmond
Estado o Provincia de la Dirección Postal: WA
País de la Dirección Postal: USA
Código Postal de la Dirección Postal: 98052 - 6399

Información de Correspondencia

No. de Correspondencia del Cliente: 000038779

Información de Representación

No. de Representante del Cliente: 000038779

Página 2 Inicial 3/7/05

Copla suministrada por USPTO de la Base de Datos de Inven. y M. del 12/23/2005



SEXTA PÁGINA:

Información de Prioridad Doméstica			
Solicitud	Tipo de	Solicitud	Fecha de

129

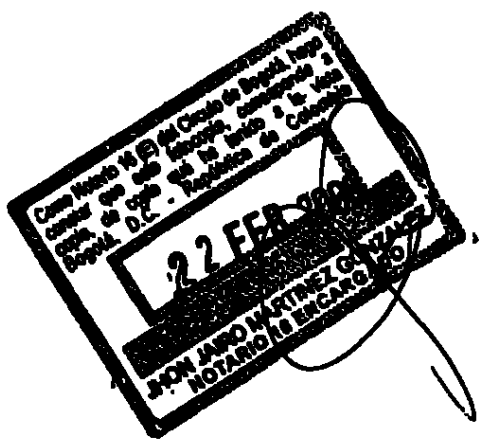
292

	C ntinuidad	Principal	Radicación de Sol. Principal
En blanco	En blanco	En blanco	En blanco

Información de Prioridad Extranjera			
País:	No. de Solicitud:	Fecha de Presentación:	Prioridad Reivindicada:
En blanco	En blanco	En blanco	En blanco

INFORMACIÓN DEL CESIONARIO:

Nombre del Cesionario:	MICROSOFT CORPORATION
Calle de la Dirección Postal:	One Microsoft Way
Cuidad de la Dirección Postal:	Redmond
Estado o Provincia la Dirección Postal:	Washington
País la Dirección Postal:	Estados Unidos de A.
Código Postal la Dirección Postal:	98052



150

SISTEMA Y METODO PARA ESTABLECER UN VINCULO ENTRE UN SERVIDOR Y UN OBJETO

CAMPO TÉCNICO

[0001] Implementaciones del presente invento se relacionan con el campo de establecer una interconexión compatible entre los terminos. En particular, implementaciones de este invento se relacionan con un sistema y método para revelar / descubrir servicios de curso con capacidades avanzadas.

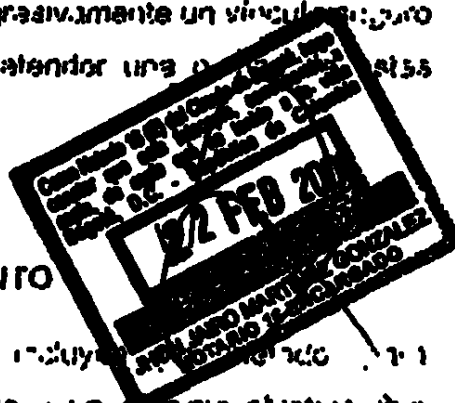
ANTECEDENTES DEL INVENTO

[0002] Algunos sistemas anteriores intentan identificar colegas potenciales comunicándose directamente. Sin embargo, estos sistemas a menudo vulnerables cuando se comunican y, en particular, crean una vulnerabilidad al SPAM.

[0003] De esta manera, se desea un sistema para identificar un colega discreto a un colega potencial y establecer progresivamente un vínculo seguro entre el servidor y el colega potencial para atender una o más de estas necesidades.

RESUMEN DEL INVENTO

[0004] Implementaciones del presente invento incluyen un sistema y método para establecer un vínculo seguro entre un servidor y un colega potencial para atender una o más de estas necesidades.



[0005] Transmitir un anuncio desde el dominio fuente al dominio objetivo, donde el anuncio incluye un elemento de datos específicos al dominio objetivo, y donde el anuncio incluye la dirección de la que el dominio fuente con el cual el dominio objetivo enviar un mensaje para establecer un vínculo entre el dominio fuente es dominio objetivo. /

[0006] Recibir del dominio fuente a través de la dirección del dominio donde una invitación de dominio objetivo donde la invitación incluye el elemento de datos o un elemento de datos correspondientes al elemento de datos donde el dominio fuente inicia el proceso para establecer el vínculo con el dominio objetivo una vez se recibe la indicación del dominio fuente

[0007] Un anuncio se transmite del dominio fuente al dominio objetivo. El anuncio incluye un elemento de datos específico al dominio objetivo. El anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se permite enviar un mensaje para establecer el vínculo entre dominio fuente y dominio objetivo. El anuncio lo recibe el dominio objetivo en incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio objetivo a la dirección del dominio fuente. La invitación incluye el elemento de datos o un elemento de datos correspondiente al elemento de datos. El Dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo en pronto se recibe la indicación del dominio fuente

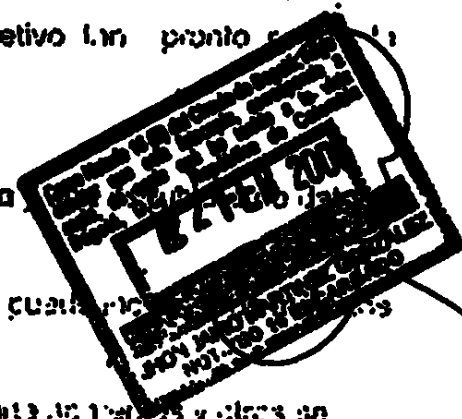
[0008] El invento también incluye un sistema

[0009] Alternativamente al invento también puede incluir

Fig. 1

[0010] Otros aspectos del invento se describen en los ejemplos y figuras de

Fig. 2



DESCRIPCION BREVE DE LOS DIBUJOS

[0011] La figura 1 es un diagrama de bloque ejemplar de los servidores 1 y 2 dentro del DMZ y que tienen una mensajería segura entre los dos. Los servidores están conectados a través de un firewall y que hace puente entre 1 y 2 que son parte de un sistema de mensajería seguro separado. Los servidores 1 y 2 forman una subred que está localizada entre una red interna confiable, tal como un sistema de mensajería seguro que vincula los puertos 1 y 2, y una red externa no confiable (tal como la Internet pública). En forma crítica, el DMZ contiene dispositivos accesibles al tráfico de Internet, tales como servidores web (http) servidores FTP servidores SMTP(e-mail) y servidores DNS a través de firewalls.

[0012] La figura 2 es, de acuerdo con el invento, un diagrama ejemplar que muestra el flujo de trabajo entre el servidor dominio fuente y un colega potencial (por ejemplo, un servidor de dominio objetivo).

[0013] La figura 3 es un diagrama de bloque ejemplar que muestra una administradora de mensajes segura de acuerdo con el invento.

[0014] La figura 4 es un diagrama de flujo que muestra las operaciones de rutado administrativo SMM de acuerdo con el invento.

[0015] La figura 5 es un diagrama de flujo que muestra las operaciones de rutado SMM de acuerdo con el invento.

[0016] La figura 6 es un diagrama de bloque ejemplar que muestra un flujo de trabajo inter-organización entre un servidor de administración de la



296

organización A) y un colega (administración de la organización B) de acuerdo con el invento

[0017] La figura 7 es un diagrama de flujo que muestra un diagrama de estado luego de que una asociación de seguridad nueva se implementa entre el servidor y un colega de acuerdo con el invento

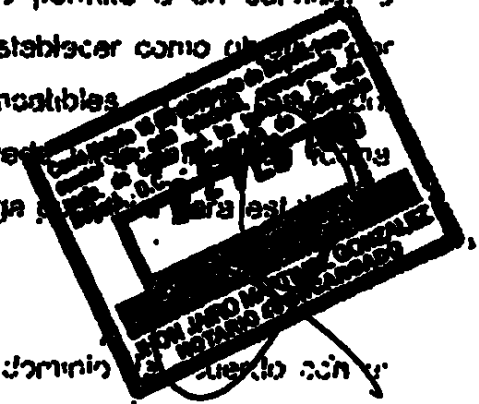
[0018] La figura 8 es un diagrama de bloque que muestra un ejemplo de un ambiente de sistema de computación alteruado en el cual el invento se puede implementar.

[0019] Caracteres de referencia correspondientes indican partes correspondientes a través de los dibujos

DESCRIPCIÓN DETALLADA DEL INVENTO

[0020] El invento se relaciona con un sistema y método para establecer un vínculo entre un servidor y un objetivo. En particular, el invento se relaciona con un sistema y métodos para establecer un vínculo seguro para desplegar un e-mail seguro. El invento le permite a un servidor determinar que un colega potencial se puede establecer como objetivo por qué tienen tecnologías de e-mail seguras y compatibles. Cuando el colega potencial se identifica, el servidor puede generar una clave material clave de información con el colega para establecer un vínculo seguro.

[0021] El objetivo de firmar y validar el dominio de un correo electrónico con el invento es suministrar un mecanismo de transporte para información de seguridad de materiales y métodos para el servidor entre los servidores.



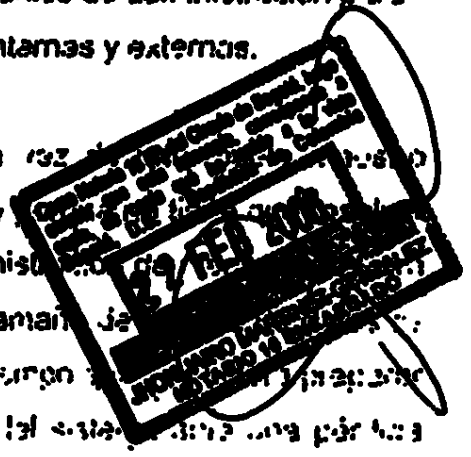
134

297

La figura 1 es un diagrama de bloques simplificado del servidor limitrofe 1 y 2 dentro de la zona desmilitarizada (DMZ). Los servidores 1 y 2 forman un anillo de mensajería segura entre ellos. Los servidores están separados por un firewall a través del cual están conectados para hacer puente entre los servidores 1 y 2. Los servidores puente son parte de un sistema de mensajería segura. Los servidores limitrofes 1 y 2 forman una sub-red que está localizada entre una red confiable interna, tal como un sistema de mensajería segura que incluye los servidores puente 1 y 2 y la red externa no confiable, tal como la Internet pública. Los firewalls también están configurados entre los servidores limitrofes y la Internet. En esta ilustración de la figura 1, el servidor limitrofe 1 puede intercambiar correo firmado y codificado con el servidor limitrofe 2 y el servidor puente 1 puede intercambiar correo firmado y codificado con el servidor puente 2. Adicionalmente, el servidor puente 1 puede reenviar a su servidor limitrofe 1 DMZ ya sea correo firmado o firmado y codificado donde el recipiente de decodificación es el servidor puente 2. Los servidores limitrofes tratan todo el correo como texto claro y codifican todo el correo punto a punto. Si los servidores limitrofes y de puente no comparten la misma clave de codificación, los servidores limitrofes no pueden decodificar el correo puente codificado.

[0022] Existe la necesidad para un punto único de administración para los datos autoritarios para todas las relaciones internas y externas.

Adicionalmente, un modelo maestro único en vez de un modelo de réplicas se implementa porque es más sencillo y evita los conflictos de réplicas. Las operaciones de administración de datos (CRUD) son generalmente poco frecuentes y el tamaño de los datos es relativamente pequeño. La implementación de un modelo maestro único evita la necesidad de mantener una copia de los datos en cada servidor. En una implementación de un modelo maestro único, los datos son mantenidos en un solo lugar y se replican en los servidores que necesitan acceder a los datos.



150

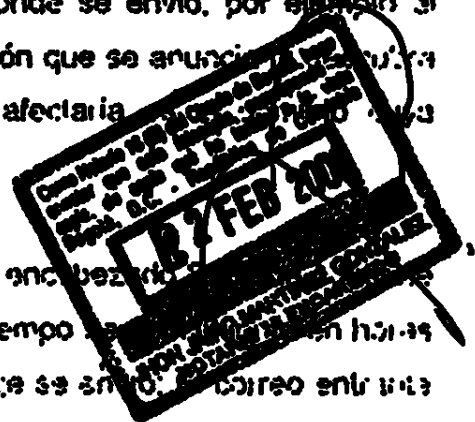
298

replican en otro servidor limitrofo. Como no hay un punto único de administración, no todos los datos se replican y los datos replicados son únicamente de lectura.

[0023] Un servidor puede involucrarse con un número de colegas para iniciar unos vínculos de correo seguros para un proyecto específico. Sin embargo, la administración de la coordinación de tal proyecto generalmente no escala. Para que la mensajería segura haga un impacto, el correo seguro se habilita con la mayoría de los colegas de negocios en la organización. Esto requiere la habilidad para descubrir qué colegas tienen servidores limitrofes instalados y tienen un flujo de trabajo organización-organización simple para facilitar el establecimiento de un vínculo de correo seguro.

[0024] El invento permite descubrir los servidores limitrofes instalados en la organización colega de tal manera que una conexión segura se pueda iniciar. Para facilitar el descubrimiento, el servidor anuncia su presencia con un correo saliente. Para minimizar la vulnerabilidad a ser atacado el proceso de anuncio, el sistema y método del invento no utiliza una dirección codificada en duro en su anuncio. Por lo tanto, la dirección anunciada es un nombre de casilla de correo aleatoria que puede rotar con intervalos razonables, por ejemplo cada semana. Para asegurar que la vulnerabilidad se minimice, el anuncio también está fijado al dominio de donde se envió, por ejemplo al dominio objetivo. En el caso de que la dirección que se anuncia fuera una dirección parte del único dominio que se afectaría, la dirección de invitación estaba comprometida.

[0025] En una forma, el anuncio es una encuesta enviada a la dirección aleatoria 322 con invitaciones y el tiempo de la dirección 322 relativa a cuando el mensaje se envió. El correo entrante a la hora de ser forzado por el servidor objetivo o colega para un

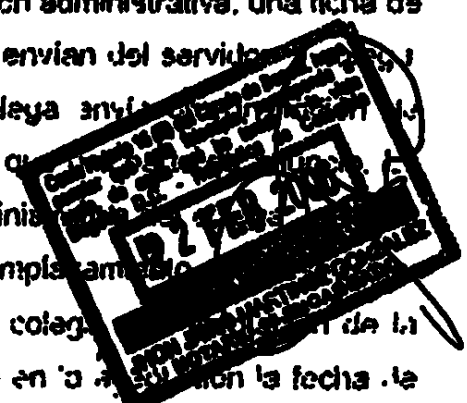


136

299

anuncio del servidor limitrofe y lo compara contra una lista de servidores limitrofes conocidos. Cualquier admisión a estas listas se comunica al administrador local SMM. Cuando se descubre un nuevo servidor limitrofe, el SMM puede enviar un mensaje de prueba (por ejemplo, una invitación) al otro servidor SMM para ofrecer un turno de firma y codificación de dominio. Tan pronto se recibe la invitación o el anuncio de otro administrador SMM, si el mensaje se puede verificar bajo la política actual de confiabilidad del SMM local entonces puede invocar una política para aceptar automáticamente la invitación. En forma alterna, el administrador SMM puede requerir una aprobación manual antes de aceptar la invitación. Tan pronto se recibe la aceptación de la invitación por el servidor, si el mensaje es verificable intrínsecamente, entonces el SMM receptor puede invocar una política para iniciar automáticamente las firmas y codificación del dominio. La configuración de dominio nuevo y seguro es un proceso no sincronizado y no se utiliza para todos los roles hasta que el vínculo se confirma operativamente con la recepción del reconocimiento.

[0026] Figura 2 es un diagrama ejemplar que muestra el flujo de trabajo entre el servidor de dominio fuente y un colega potencial (por ejemplo, un computador que es el dominio objetivo) de acuerdo con el invento. Inicialmente, un anuncio que incluye una dirección administrativa, una fecha de emplazamiento y una fecha de vencimiento se envían del servidor de dominio fuente. Cuando el colega reconoce el anuncio, el colega envía una invitación de vuelta a la dirección administrativa del servidor de dominio fuente. La invitación del colega incluye una dirección administrativa, una fecha de vencimiento, un certificado y la fecha de emplazamiento. El servidor de dominio fuente envía a la dirección administrativa del colega una invitación de vuelta a la dirección administrativa del servidor de dominio fuente que incluye en la invitación la fecha de vencimiento, el certificado, la fecha de emplazamiento y una firma. Luego de recibir la aceptación, el colega envía una invitación al servidor de dominio fuente.



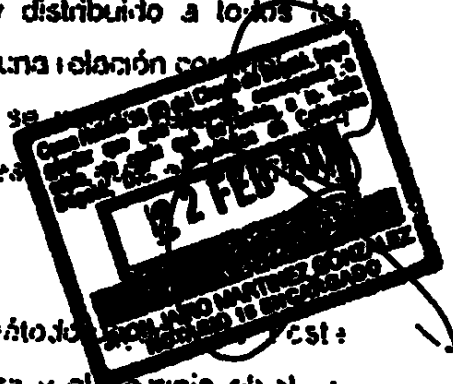
157

300

indicación la reconoce al servidor para establecer la conexión. Si el mensaje de invitación no se puede verificar utilizando la política de confiabilidad como se mostró en la figura 2 y entonces la petición se puede poner en cola en espera de una aprobación manual.

[0027] En referencia a la figura 3, un diagrama de bloque de ejemplo muestra una administradora de mensajes segura de acuerdo con el invento. La aceptación de la invitación por el colega crea unos certificados cruzados en el agente administrativo SMM que luego se envía a los agentes trabajadores SMM que codifican el certificado. La certificación cruzada restringe el conjunto de nombres que la nueva confiabilidad acepta y la restricción a la comunicación de dominio del servidor limítrofe. Para facilitar una ejecución separada al SMM que envía asigna una clave de sesión y reutiliza ésta clave a través de mensajes múltiples a un recipiente SMM. La clave de la sesión también se puede distribuir en este caso del administrador SMM al trabajador SMM de tal manera que todos los trabajadores utilicen la misma clave para el envío al tamaño de la memoria caché. Para permitir el escalamiento, la clave privada de decodificación correspondiente para el certificado codificado debe estar disponible en todo el Internet enfrentado a los servidores limítrofes para permitir la decodificación de correo entrante. Esto se puede generar en un solo sitio, por ejemplo, el agente administrativo y distribuido a todos los trabajadores de servidor. Una vez que se establece una relación con el sitio debe mantener. Por ejemplo, el certificado original se puede mantener en el sitio de renovación enviarse a otro SMM antes de la expiración.

[0028] Desde la perspectiva del servidor, el método de acuerdo con el invento establece un vínculo entre el dominio fuente y el dominio objetivo. El servidor fuente transmite un anuncio a un dominio objetivo. El servidor objetivo le devuelve los datos tales como se proporcionó a

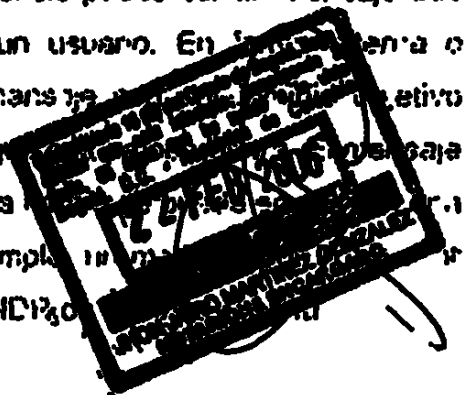


138

una fecha u otro secreto que está designado específicamente al dominio objetivo. Adicionalmente, el anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el servidor de dominio fuente y el computador objetivo. El servidor de dominio fuente recibe una invitación del dominio objetivo cuya invitación está dirigida a la dirección del dominio fuente que suministró previamente. La invitación incluye un elemento de datos en el anuncio o un elemento de datos que corresponde al elemento de datos en el anuncio. Esto permite que el servidor fuente inicie un proceso para establecer un vínculo entre el servidor de dominio objetivo y el servidor de dominio fuente tan pronto recibe el servidor de dominio fuente la invitación del servidor de dominio objetivo. Como se anotó en la figura 2, el servidor de dominio fuente transmite al servidor de dominio objetivo una aceptación para establecer el vínculo entre ellos.

[0029] En una implementación, el dominio fuente transmite en forma selectiva el anuncio al dominio objetivo, la donde el dominio fuente ha recibido el mensaje en forma alterna o adicionalmente, el dominio fuente puede enviar un anuncio al dominio objetivo que se ha identificado específicamente. En forma alterna o adicionalmente, el dominio fuente puede enviar un anuncio a dominios objetivos seleccionados en forma aleatoria.

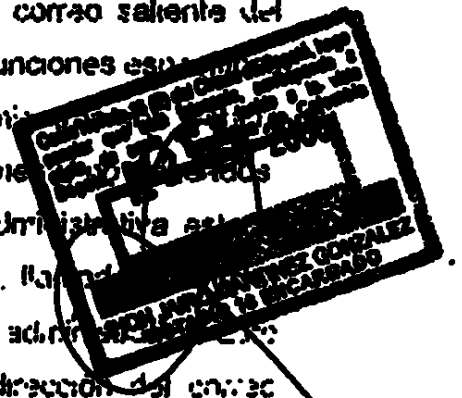
[0030] En una implementación, el anuncio puede ser un mensaje que se genera en respuesta a la acción de un usuario. En forma alterna o adicionalmente el anuncio puede ser un mensaje que se genera en respuesta a la acción de un usuario o un mensaje a un dominio objetivo que se genera en respuesta a la acción de un usuario. El dominio objetivo puede ser para cada mensaje una determinación basada en el tiempo (por ejemplo, un mensaje que se genera en respuesta a la acción de un usuario puede ser un mensaje que se genera en respuesta a la acción de un usuario).



302

[0031] En una implementación del invento, un servidor de correo ocasionalmente añade un encabezado adicional (como un 'x-header') a un mensaje que se entrega a otro dominio email. Los datos en el encabezado incluyen un secreto que es específico al dominio objetivo y la dirección de correo al donde el mensaje administrativo del dominio objetivo se puede dirigir de vuelta al servidor de correo. Si el correo en el dominio objetivo también es dirigido a través del servidor que implementa esta implementación del invento, entonces detectará el encabezado adicional y determinará que debe haber un servidor compatible en el dominio de origen. El dominio objetivo luego dirige el tráfico administrativo, tal como las peticiones para establecer una conexión segura, a la dirección de correo administrativa contenida. Como se anotó anteriormente, tales mensajes administrativos deben contener el secreto que le fue suministrado al dominio objetivo. El que acepta el correo administrativo en el dominio de origen puede entonces descartar cualquier correo que no parece ser del dominio objetivo pero que no contiene el secreto correspondiente al dominio objetivo. Aunque esto no suministra una seguridad absoluta de que el correo administrativo recibido es del dominio que origina, minimiza la vulnerabilidad al SPAM.

[0032] En una implementación, el invento se implementa utilizando un encabezado, llamado una mención, que se anexa a un correo saliente del dominio fuente. Esta mención revela la disponibilidad de funciones especializadas en el servidor de correo que origina el correo saliente minimizando la necesidad para generar mensajes adicionales y posiblemente reducir costos. Como se anotó anteriormente, la dirección de correo administrativa está incluida en la mención y habría un secreto por dominio. El invento se utiliza para mitigar los riesgos del SPAM a la dirección de correo administrativa al referenciar el secreto a los mensajes del flujo de trabajo en la dirección del correo administrativo.

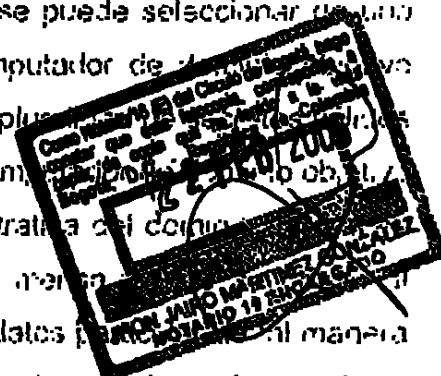


140

305

lante la re-transmisión. En general, los dominios que buscan la aprobación se marcan y si la marca se ha recibido el dominio se aprueba. Los dominios que buscan aceptación se marcan en forma similar.

[0037] Otros rasgos opcionales del invento incluyen lo siguiente que se puede incrementar en forma separada o en combinación. El anuncio puede incluir una fecha de vencimiento y en tal caso el servidor fuente no inicia el proceso para establecer un vínculo con el computador de dominio objetivo (por ejemplo, el servidor) cuando el servidor de dominio fuente recibe la invitación luego de la fecha de vencimiento. El elemento de datos puede ser uno de los siguientes: un secreto por dominio incluyendo un número pseudo-aleatorio para cada computador de dominio objetivo (por ejemplo, el servidor), un secreto generado a través de selecciones del computador de dominio objetivo (por ejemplo, el servidor) y una semilla secreta que se utiliza para generar los secretos por dominio para más de un dominio; y un secreto por dominio generado codificando el computador de dominio objetivo (por ejemplo el servidor) y una fecha de terminación para el secreto. Los el elemento de datos puede incluir un secreto y en tal caso el servidor de dominio fuente verifica el secreto recibido del computador de dominio objetivo (por ejemplo el servidor) re-computando y luego comparando el secreto actual para el computador de dominio objetivo (por ejemplo, el servidor) con el secreto incluido en el anuncio. El elemento de datos se puede seleccionar de una pluralidad de secretos múltiples para cada computador de dominio objetivo (por ejemplo el servidor) de tal manera que una pluralidad de secretos se pueden utilizar para la comunicación de un computador de dominio objetivo (por ejemplo, el servidor) a la dirección administrativa del dominio. Se puede imponer un límite en el número de anuncios que un computador de dominio fuente con un elemento de datos particular puede recibir de solicitudes de ataques de servicio utilizando un elemento de datos particular se asignizan. El servidor de dominio fuente puede incluir la habilidad

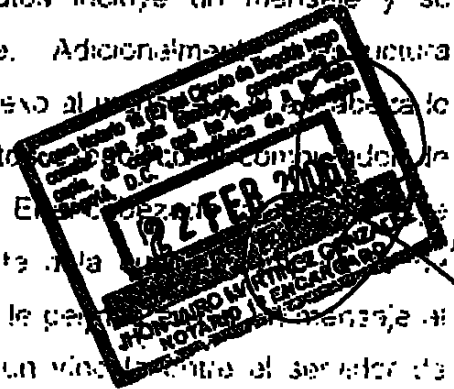


443

306

para sobrepasar los requerimientos para un elemento de datos para el computador de dominio objetivo dado (por ejemplo, el servidor) para permitir una autorización fuera-de-banda para enviar mensajes de invitación de un dominio particular. El elemento de datos puede ser una ficha en el mensaje de anuncio en un encabezado de correo o incrustada en el cuerpo de un mensaje o el elemento de datos puede ser una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando pasa a través del servidor de correo. El servidor de dominio fuente puede dar soporte a múltiples fichas válidas simultáneamente para el mismo dominio y verificar los mensajes de invitación de sub-dominios del computador de dominio objetivo (por ejemplo, el servidor) verificando la ficha de entrada contra las fichas para el computador de dominio objetivo (por ejemplo, el servidor). El elemento de datos puede ser una mención e incluir en la mención información de la versión para el servidor de dominio fuente e incluir en la mención funciones apoyadas por el servidor de dominio fuente.

[0038] En una implementación el invento comprende una estructura de datos para que el aviso se pueda transmitir del servidor de dominio fuente al computador de dominio objetivo (por ejemplo, el servidor). Como se anotó anteriormente, esta estructura de datos se utiliza para establecer un vínculo entre el servidor de dominio fuente y el computador de dominio objetivo (por ejemplo, el servidor). La estructura de datos incluye un mensaje y su encabezado usual relacionarlo con el mensaje. Adicionalmente la estructura de datos incluye un encabezado adicional previo al mensaje y el encabezado del mensaje que incluye un elemento de datos para el computador de dominio objetivo (por ejemplo, el servidor). El elemento de datos incluye una dirección del servidor de dominio fuente a la que el computador de dominio objetivo (por ejemplo, el servidor) se le permite enviar mensajes al servidor de dominio fuente para establecer un vínculo entre el servidor de dominio fuente y el computador de dominio objetivo (por ejemplo, el servidor).



144

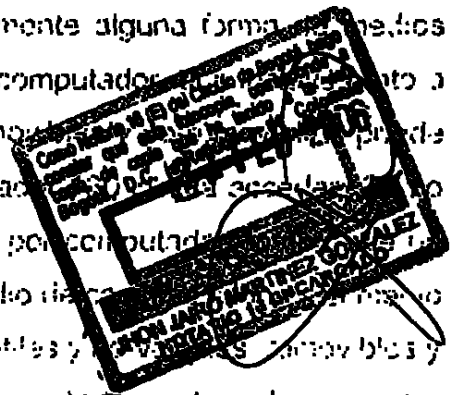
307

Como se anotó anteriormente, el encabezado adicional debe incluir una fecha de vencimiento, aunque esto es opcional.

[0030] Una implementación representativa ejemplar

[0040] La figura 3 muestra un ejemplo de un dispositivo de cómputo de propósito general en la forma de un computador 130. En una implementación del invento, un computador tal como el computador 130 es adecuado para uso en las otras figuras que se muestran y se describen acá. El computador 130 tiene uno o más procesadores o unidades procesadoras 132 y una memoria de sistema 134. Tiene en la implementación que se muestra, un bus de sistema 136 que conecta los componentes varios del sistema incluyendo la memoria del sistema 134 con el procesador 132. El bus 136 representa uno o más de varios tipos de estructuras de bus, incluyendo un bus de memoria o controladora de memoria, un bus periférico, un puerto de gráficos acelerado, y un procesador de bus local utilizando cualquiera de varias arquitecturas de bus. Como ejemplo, y no como limitante, estas arquitecturas incluyen el bus Industry Standard Architecture (ISA), el bus Micro Channel Architecture (MCA), el bus Enhanced ISA (EISA), el bus local Video Electronics Standards Association (VESA), y el bus Peripheral Component Interconnect (PCI) también conocido como el bus Mezzanine.

[0041] El computador 130 tiene típicamente alguna forma de medios legibles por computador. El medio legible por computador puede ser uno o más de los medios volátiles y no-volátiles, medios removibles y no-removibles, o cualquier medio disponible que el computador pueda leer. Como ejemplo y no como limitante, el medio legible por computador puede ser un medio de almacenamiento de computador y un medio de almacenamiento de computador incluye los medios volátiles y no-volátiles y los medios implementados en cualquier método o tecnologías para

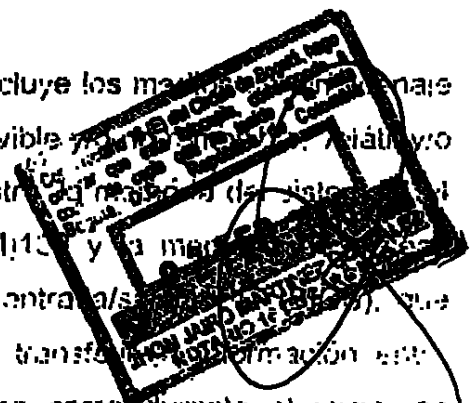


145

308

almacenar información tal como instrucciones legibles por computador, estructuras de datos, módulos de programa o cualquier otro tipo de datos. Los medios legibles por computador incluyen RAM, ROM, EPROM, memoria flash o cualquier otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) o cualquier otro almacenaje en disco óptico, casetes magnéticos, cintas magnéticas, almacenaje en discos magnéticos o cualquier otro dispositivo de almacenaje magnético, o cualquier otro medio que se pueda utilizar para almacenar la información deseada que el computador 130 pueda acceder. Los medios de comunicación encarnan instrucciones legibles por computador, estructuras de datos, módulos de programa, u otros tipos de datos en señal de datos modulada tales como ondas transportadoras y otros mecanismos de transporte e incluyen cualquier medio de suministro de información. Aquellos diestros en el arte están familiarizados con las señales de datos moduladas, que tienen una o más de sus características fijas o alteradas de tal manera que codifican la información en la señal. Medios alambrados, tales como redes alambradas o conexiones alambradas directas, y medios inalámbricos, tales como acústicos, RF, infrarrojos y otros medios inalámbricos, son ejemplos de medios de comunicación. Combinaciones de cualquier tipo de los anteriores también se incluyen dentro del alcance de medios legibles por computador.

[0042] La memoria del sistema 134 incluye los medios de almacenamiento en computador en la forma de memoria removible 136 y memoria no-removible. En la implementación que se muestra, la memoria 134 incluye a la memoria de sólo lectura (ROM) 138 y la memoria de acceso aleatorio (RAM) 140. Un sistema básico de entrada/salida (BIOS) 142, que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del computador 130 tales como durante el inicio, se almacenan típicamente en ROM 138. La RAM 140 contiene típicamente los módulos de programa que son accesibles inmediatamente al sistema.



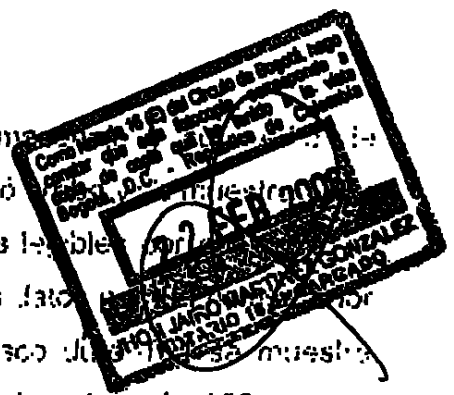
146

309

operados actualmente por la unidad de procesamiento 132. Como ejemplo, y no como limitante, la figura 8 muestra el sistema operativo 144, programas de aplicación 146 y otros módulos de programas 148, y datos de programas 150.

[0043] El computador 130 también puede incluir otros medios de almacenaje en computador removibles y/o no-removibles, volátiles y/o no-volátiles. Por ejemplo, la figura 8 muestra un drive de disco duro 154 que lee o escribe a medios magnéticos no-removibles y no-volátiles. La figura 8 también muestra un drive de disco magnético 156 que lee o escribe a el disco magnético removible, no-volátil 158, y un drive de disco óptico 160 que lee o escribe a el disco óptico removible, no-volátil 162 tal como un CD-ROM o cualquier otro medio óptico. Otros tipos de medios de almacenaje en computador removibles/no-removibles, portátiles/no-volátiles que se pueden utilizar en el ambiente operativo ejemplar incluyen, pero no están limitadas a, cintas de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cintas de videos digitales, RAM de estado sólido, ROM de estado sólido, y cosas parecidas. El drive de disco duro 154, y el drive de disco magnético 156 y el drive de disco óptico 160 están conectados en forma típica al bus del sistema 136 a través de una interfase de memoria no-volátil, tal como la interfase 166.

[0044] El drive u otros dispositivos de almacenamiento en computador asociado que se discutió en la figura 8, administra el almacenaje de instrucciones legibles 170, estructuras de datos, módulos de programa y otros datos de programa 172. En la figura 8, por ejemplo, el drive de disco duro 154 muestra almacenando el sistema operativo 170, programas de aplicación 172, y otros módulos de programa 174, y datos de programa 176. Nótese que estos componentes pueden ser los mismos o diferentes al sistema operativo 132.

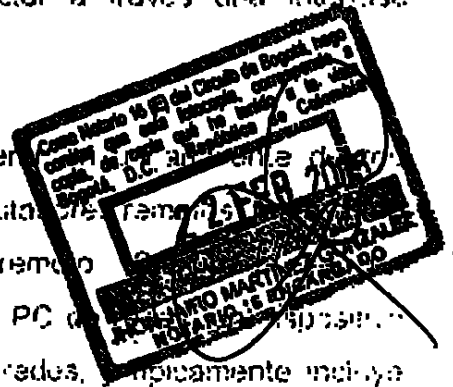


149

programas de aplicación 146 u otros módulos de programa 148 y 149, el programa 150, al sistema operativo 170, programas de aplicación 172, otros módulos de programas 174 y datos de programas 176 se les dan distintos números para mostrar que, por lo menos, son copias diferentes.

[0045] Un usuario puede ingresar un comando de información al computador 130 a través de dispositivos de entrada o dispositivos de selección en la interfase del usuario tales como un teclado 180 y un dispositivo de señalamiento 182 (por ejemplo, un ratón, un trackball, una pluma o una almohadilla táctil). Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, un joystick, un panel de juegos, un disco digital, escáner, y demás. Estos y otros dispositivos de entrada se conectan a la unidad procesadora 132 a través de una interfase de usuario de entrada 184 que se conecta al bus del sistema 136, pero que pueda estar conectada por otras interfases o estructuras de bus, tales como puertos paralelos, puertos de juego o el Bus Serial Universal (USB). Un monitor 188 u otro tipo de dispositivo de visualización también se conecta al bus del sistema 136 a través de una interfase, tal como la interfase de video 190. Adicionalmente al monitor 188, los computadores frecuentemente incluyen otros dispositivos de salida periféricos (que no se muestran) tales como una impresora y parlantes, que se pueden conectar a través una interfase periférica de salida (que no se muestran).

[0046] El computador de 130 puede operar utilizando conexiones lógicas a uno o mas computadores. El computador remoto 194. El computador remoto puede ser un computador personal, un servidor, un router, un PC de un colega o cualquier otro nodo común de redes, típicamente incluye muchos o todos de los elementos descritos arriba relativos al computador 130. Las conexiones lógicas que se muestran en la figura 3 incluyen una conexión

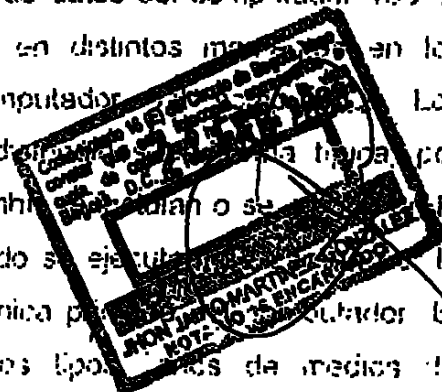


311

área local (LAN) 196 y una red de área amplia (WAN) 198 pero también pueden incluir otras redes. La LAN 196 y/o la WAN 198 pueden ser una red alámbrica, una red inalámbrica, o una combinación, y demás. Estos ambientes de redes son comunes en oficinas, redes de computadores de negocios, intranets, y redes globales de computadores (por ejemplo Internet).

[0047] Cuando se utilizan en un ambiente de red local, el computador 130 está conectado a la LAN 196 a través de una interfase de red o adaptador 186. Cuando se utiliza en un ambiente de red de área amplia, el computador 130 incluye típicamente un modem 178 u otros medios para establecer comunicación con la WAN 198, tal como Internet. El modem 178, que puede ser interno o externo, se conecta al bus del sistema 136 a través de una interfase de entrada del usuario 184, u otros mecanismos apropiados. En un ambiente de red, los módulos de programa que se muestran relativos al computador 130, o porciones de él, se pueden almacenar en un dispositivo de almacenaje de memoria remoto (que no se muestran). Como ejemplo, y no como limitante, la figura 8 muestra programas de aplicación remotos 192 como residiendo en el dispositivo de memoria. Las conexiones de red que se muestran son ejemplares y otros medios para establecer un vínculo de comunicación entre computadores se puede utilizar.

[0048] Generalmente, el procesador de datos del computador 130 se programa con instrucciones almacenadas en distintos medios en los medios de almacenaje legibles por computador. Los programas y el sistema operativo están almacenados en la memoria, por ejemplo, en discos floppy o CD ROMs. De ahí, se cargan o se transfieren a la memoria secundaria del computador. Cuando se ejecutan, se cargan o se transfieren a la memoria electrónica principal del computador. El presente documento incluye estos y otros tipos de medios de almacenaje legibles por computador cuando estos medios contienen



149

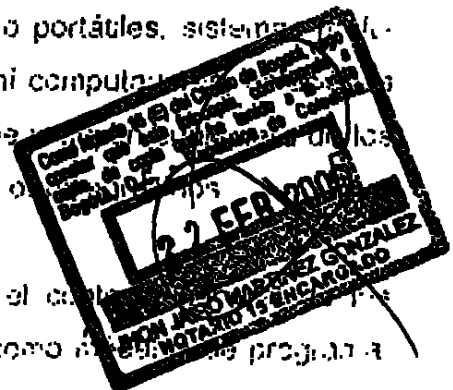
3/2

instrucciones o programas para cumplir entre los pasos descritos más abajo, conjunto con un micro procesador u otro procesador de datos. El invento también incluye al computador en sí mismo cuando se programa de acuerdo a los métodos y técnicas descritos acá.

[0049] Con un propósito ilustrativo, los programas y otros componentes de programas ejecutables, tales como el sistema operativo, se muestran como bloques discretos. Se reconoce, sin embargo, que tales programas y componentes residan, en varios momentos, en distintos componentes de almacenamiento del computador, y los ejecuta el procesador(es) del computador.

[0050] Aunque se describe en relación con el ambiente de sistema de computación ejemplar, incluyendo a los computadores 130, el invento es funcional con otros ambientes de sistema de computación de propósito general o especial y otras combinaciones. El ambiente de sistema de computación no tiene la intención de sugerir ninguna limitación en cuanto al alcance, uso o funcionalidad del invento. Aún más, el ambiente de sistema de computación no se debe interpretar como teniendo algunas dependencias o requerimiento relacionado con uno o varios componentes o combinación de ellos ilustrados en el ambiente operativo ejemplar. Ejemplos de sistemas de cómputo, ambientes, y/o configuraciones que son adecuadas para uso con el invento incluyen, pero no están limitados a, computadores personales, computadores servidores, dispositivos de mano o portátiles, sistemas de telefonía, teléfonos móviles, PDA, la red, mini computadores, dispositivos de trabajo, ambientes de cómputo distribuidos que incluyen los sistemas anteriores o dispositivos mencionados y otros.

[0051] El aparato de puente descrito en el contexto de los sistemas ejecutables por computador tales como el sistema operativo, programas de aplicación u otros programas, tales como los dispositivos de almacenamiento.



(80

33

los módulos de programa incluyen, pero no están limitados a, rutinas programadas, objetos, componentes, estructuras de datos que ejecutan tareas particulares o implementan tipos de datos abstractos particulares. En cuanto también se puede practicar en ambientes de cómputo distribuidos donde las tareas las ejecuta un procesador remoto que está vinculado a través de una red de comunicaciones. En un ambiente de cómputo distribuido los módulos de programa pueden estar localizados tanto en los medios de almacenamiento del computador local y en el computador remoto incluyendo a los dispositivos de almacenamiento de memoria.

[0052] Una interfase en el contexto de la arquitectura de software incluye módulos de software, componentes, porciones de código, u otras secuencias de instrucciones ejecutables por computador. La interfase incluye por ejemplo, un primer módulo que accede a un segundo módulo para ejecutar tareas de cómputo en beneficio del primer módulo. El primero y segundo módulo incluyen en un ejemplo aplicaciones de interfases de programación (API) tales como las suministradas por el sistema operativo, interfaces de modelo de objetos (COM) (por ejemplo, para aplicaciones de comunicación colega-colega) y las interfaces de formato de intercambio de meta datos del lenguaje de marcación extensible (XML) (por ejemplo, para la comunicación entre servicios de red).

[0053] La interfase puede ser una implementación de la interfase y acoplada fuertemente como la Java 2 Platform (J2P) o la Java 2 Platform, Enterprise Edition (J2EE), COM, o COM distribuido (DCOM). En forma alternativa o en adición a la interfase puede ser una implementación no-síncrona de la interfase tal como un servicio de red (por ejemplo, un servicio de red de objetos simple). En general la interfase incluye cualquier combinación de las siguientes características: acoplada fuertemente o acoplada suelta, síncrona o no-síncrona. Aún más la interfase puede



151

315

[0059] Como se pueden hacer varios cambios en la construcción mencionada productos, y métodos sin alterarse del alcance del invento se entiende que todo el material descrito en la anterior descripción y que se muestra en los dibujos acompañantes se debe interpretar como ilustrativo y no limitante en ningún sentido



153

316

LO QUE SE REIVINDICA ES.

1. Un método para establecer un vínculo entre un dominio fuente y un dominio objetivo que comprende:

transmitir un anuncio del dominio fuente al dominio objetivo donde el anuncio incluye un elemento de datos específico para el dominio objetivo y donde el aviso incluye una dirección del dominio fuente a la cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo; y

recibir por el dominio fuente, a través de la dirección del dominio fuente una invitación del dominio objetivo donde la invitación incluye un elemento de datos o un elemento de datos correspondiente al elemento de datos donde el dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo tan pronto recibe el dominio fuente la invitación.

2. El método de la reivindicación 1 comprende además la transmisión de una adaptación del dominio fuente al dominio objetivo para establecer el vínculo entre ellos.

3. El método de la reivindicación 1 donde el anuncio se transmite en forma selectiva a por lo menos uno de los siguientes:

dominios objetivos de donde el dominio fuente ha recibido un mensaje

dominios objetivo específicamente identificados anteriormente; y

dominios objetivos seleccionados en forma aleatoria

4. El método de la reivindicación 1 donde el anuncio es un mensaje que se genera en respuesta a una acción de usuario, donde el anuncio es un mensaje

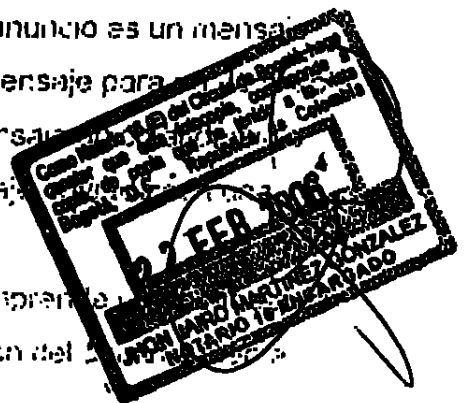
con un dominio objetivo único; donde el anuncio es un mensaje para un dominio objetivo que es un operador; donde el anuncio es un mensaje

dirigido para cada clave; o donde el anuncio es un mensaje

de programación basada en el tiempo

5. El método de la reivindicación 1 donde el anuncio comprende

un anuncio que incluye los elementos de datos y la dirección del



154

318

mensaje o donde el elemento de datos es una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando se pasa a través del servidor de correo.

13. El método de la reivindicación 1 comprende además el soporte de múltiples fichas válidas para el mismo dominio y la verificación de mensajes de invitación de sub-dominios del dominio fuente verificando las fichas de entrada contra fichas para el dominio objetivo.

14. El método de la reivindicación 1 donde el elemento de datos es una mención y comprende además incluir en la mención información sobre la versión para el dominio fuente e incluir en la mención funciones soportadas por el dominio fuente.

15. Una estructura de datos para un anuncio se transmite de un dominio fuente a un dominio objetivo para establecer un vínculo entre el dominio fuente y el dominio objetivo que comprende:

Un mensaje;

Un encabezado relacionado con el mensaje; y

Un encabezado adicional anexo al mensaje y que incluye un elemento de datos específico al dominio objetivo que incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje al dominio fuente para establecer un vínculo entre el dominio fuente y el dominio objetivo, una ficha de emplazamiento y una fecha de vencimiento.

16. La estructura de datos de la reivindicación 15 donde el elemento de datos es por lo menos uno de los siguientes:

Un secreto por dominio que incluye un número pseudo aleatorio para el dominio objetivo.

Un secreto generado a través del dominio objetivo y un código de verificación que se utiliza para generar secretos por-dominio para más dominios o un secreto por dominio generado codificando el dominio objetivo con un código de verificación del secreto.



186

Comprende adicionalmente uno de los siguientes:

Imponer un límite en el número de mensajes que se pueden pasar a la dirección

del dominio fuente con un elemento de datos particular donde se mitiga la

negación de ataques de Servicio utilizando un elemento de datos correcto

Sobrepasando los requerimientos para un elemento de datos para un dominio

objetivo dado para permitir las autorizaciones fuera de banda para enviar un

mensaje de invitación de un dominio particular y soportando simultáneamente

hojas múltiples válidas para el mismo dominio y verificando el mensaje de

invitación de sub-dominios del dominio objetivo verificando la ficha entrante contra

fichas para el dominio objetivo

19 El sistema de la reivindicación 17 donde un anuncio transmitido por un servidor

dominio fuente comprende por lo menos uno de los siguientes:

Un anuncio transmitido en forma selectiva al dominio objetivo de donde el dominio

fuentes ha recibido un mensaje;

Un anuncio transmitido en forma selectiva al dominio objetivo específicamente

identificado anteriormente o seleccionado en forma pseudo-aleatoria del dominio

objetivo;

Un mensaje que se genera en respuesta a una acción de usuario (por ejemplo,

clic, recibes).

Un mensaje con un dominio objetivo único,

Un mensaje para el dominio objetivo que es un operador;

Un mensaje único para el dominio objetivo y para cada llave;

Un mensaje enviado en determinación hechas en base al tiempo (por ejemplo, un

mensaje cada hora).

Un encabezado adicional que incluye un elemento de datos y una dirección

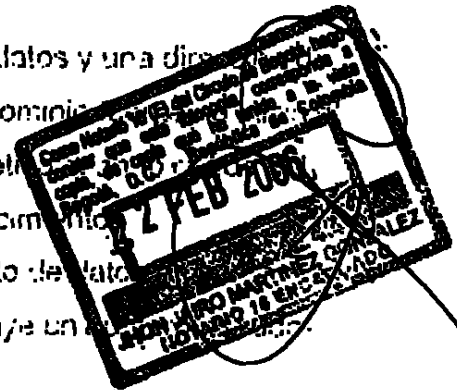
dominio fuente y una fecha de vencimiento donde el dominio

fuente usa para establecer un vínculo con el dominio objetivo

fuente una invitación luego de la fecha de vencimiento

20 El sistema de la reivindicación 17 donde el elemento de datos

comprende los siguientes: un secreto por dominio que incluye un



321

aloteno para cada dominio objetivo un secreto generado a través del dominio objetivo y una semilla de secreto que se utiliza para generar secretos por dominio para más de un dominio;

Un secreto por dominio generado codificando al dominio objetivo y una fecha de vencimiento del secreto;

Un secreto donde el dominio fuente verifica el secreto recibido del dominio objetivo re-computando y luego comparando el secreto actual para el dominio objetivo con el secreto incluido en el anuncio;

Un elemento de datos se seleccionado de una pluralidad de secretos múltiples que se sobrepone para cada dominio objetivo de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación del dominio objetivo a la dirección administrativa del dominio que origina;

Una ficha en el mensaje de anuncio en el encabezado del correo o incrustado en el cuerpo del mensaje o donde el elemento de datos es una ficha en un encabezado del correo y el cuerpo del mensaje permanece codificado cuando pasa a través del servidor de correo y

Una mención que comprende adicionalmente incluir en la mención información la versión para el dominio fuente e incluyendo en la mención soluciones soportadas por el dominio fuente.



139

322

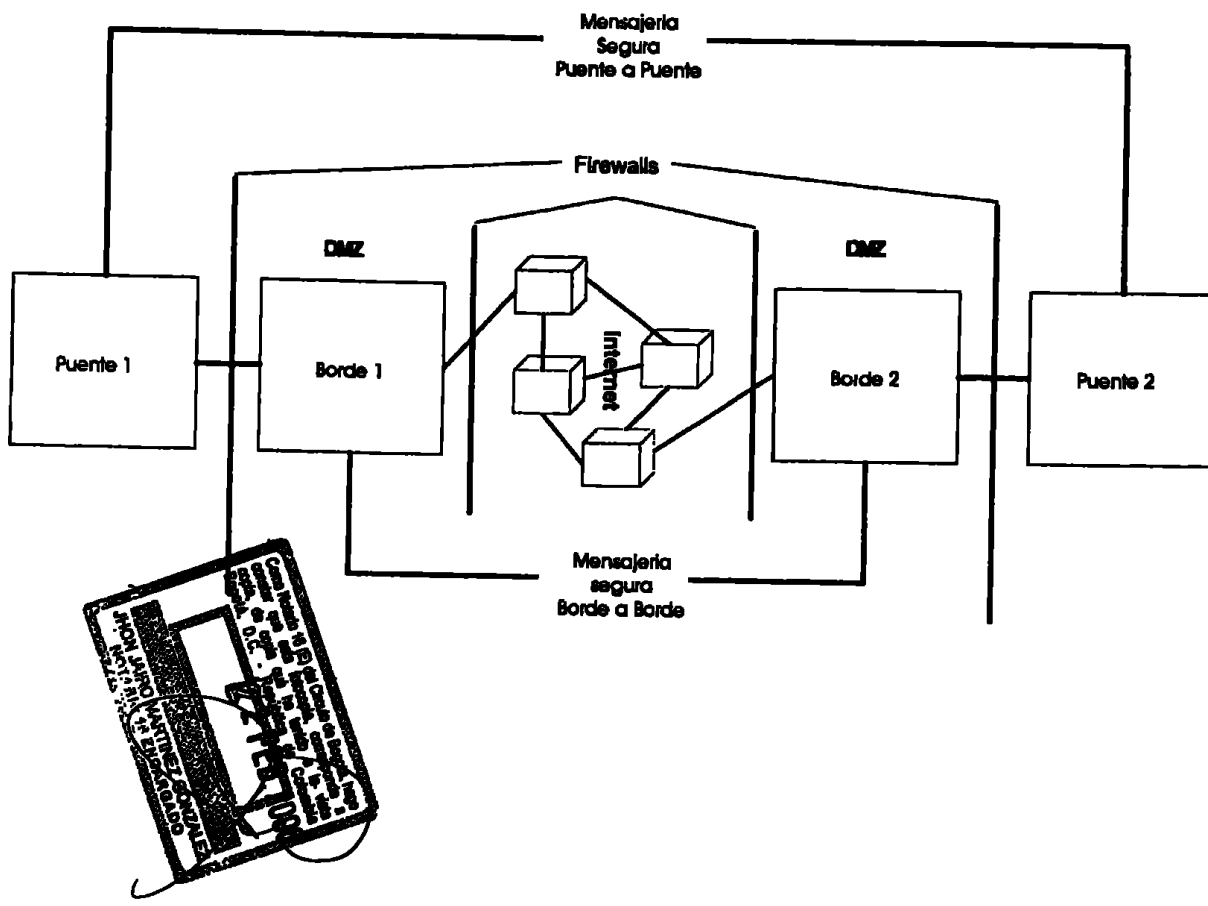
RESUMEN

Un anuncio se transmite de un dominio fuente a un dominio objetivo. El anuncio incluye elementos de datos específicos al dominio objetivo y. El anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo. El anuncio lo recibe en dominio objetivo incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio objetivo a la dirección del dominio fuente. La invitación incluye el elemento de datos o elemento de datos correspondiente al elemento de datos. El dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo tan pronto recibe del dominio fuente la invitación.



160

FIG. 1



1/8

1/61

FIG. 2

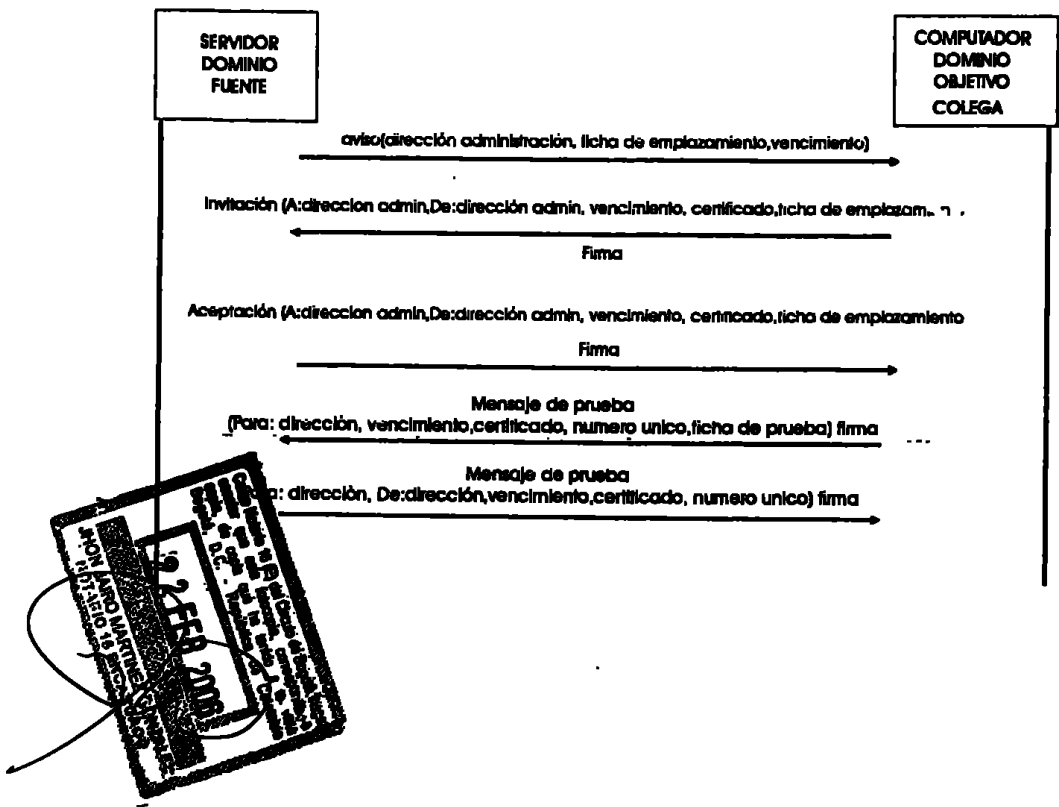
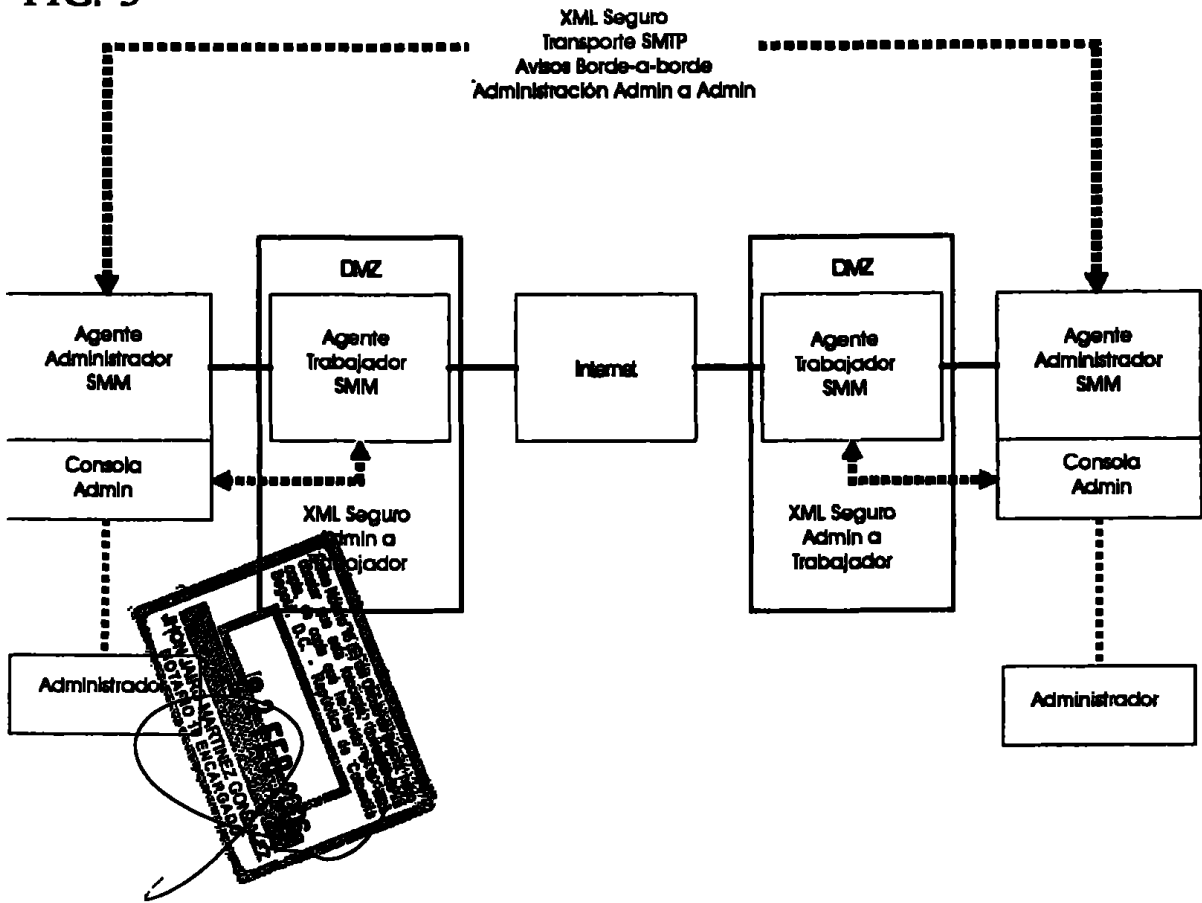
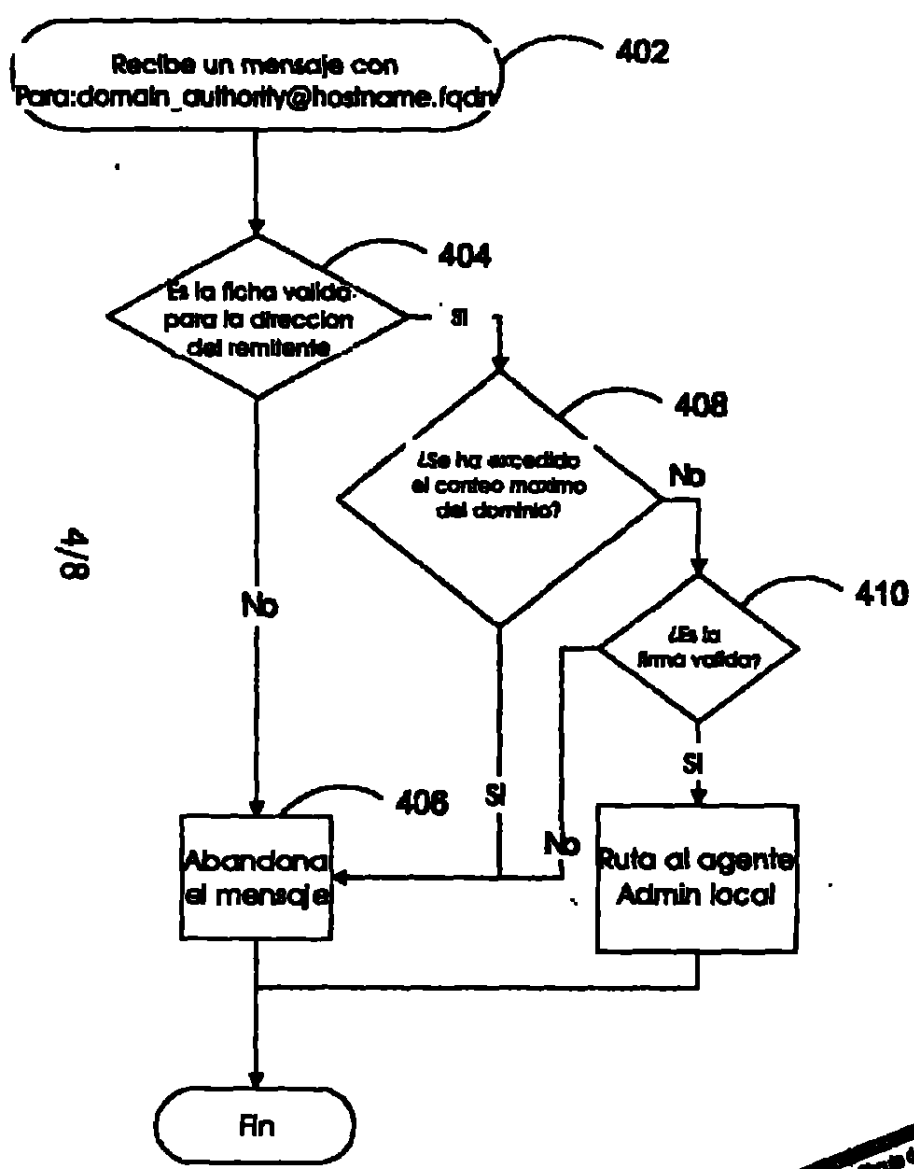


FIG. 3



326

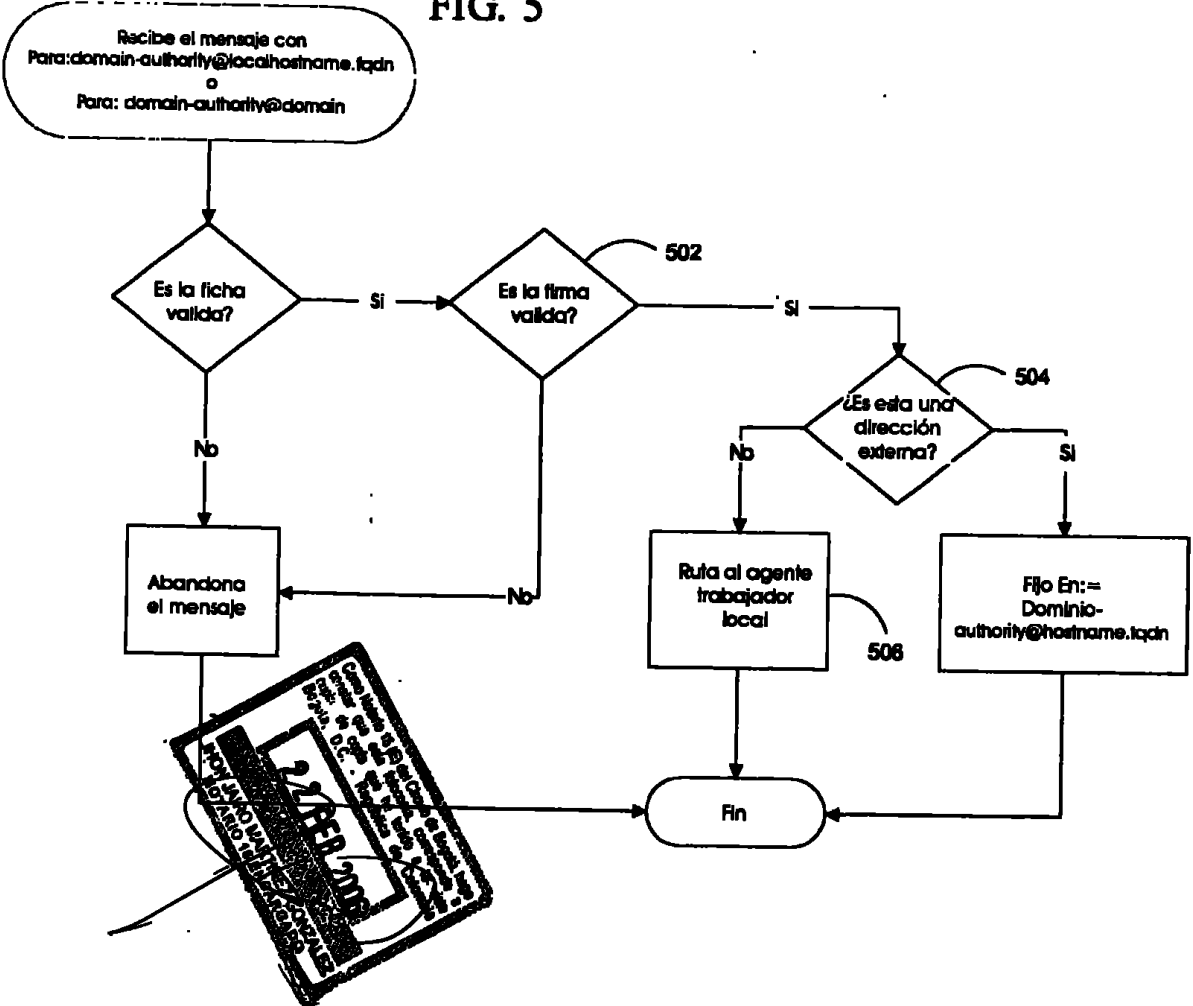
FIG. 4



164

FIG. 5

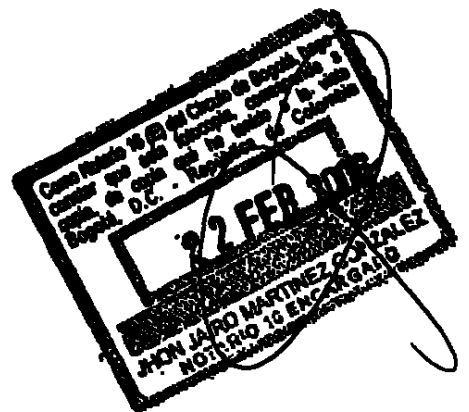
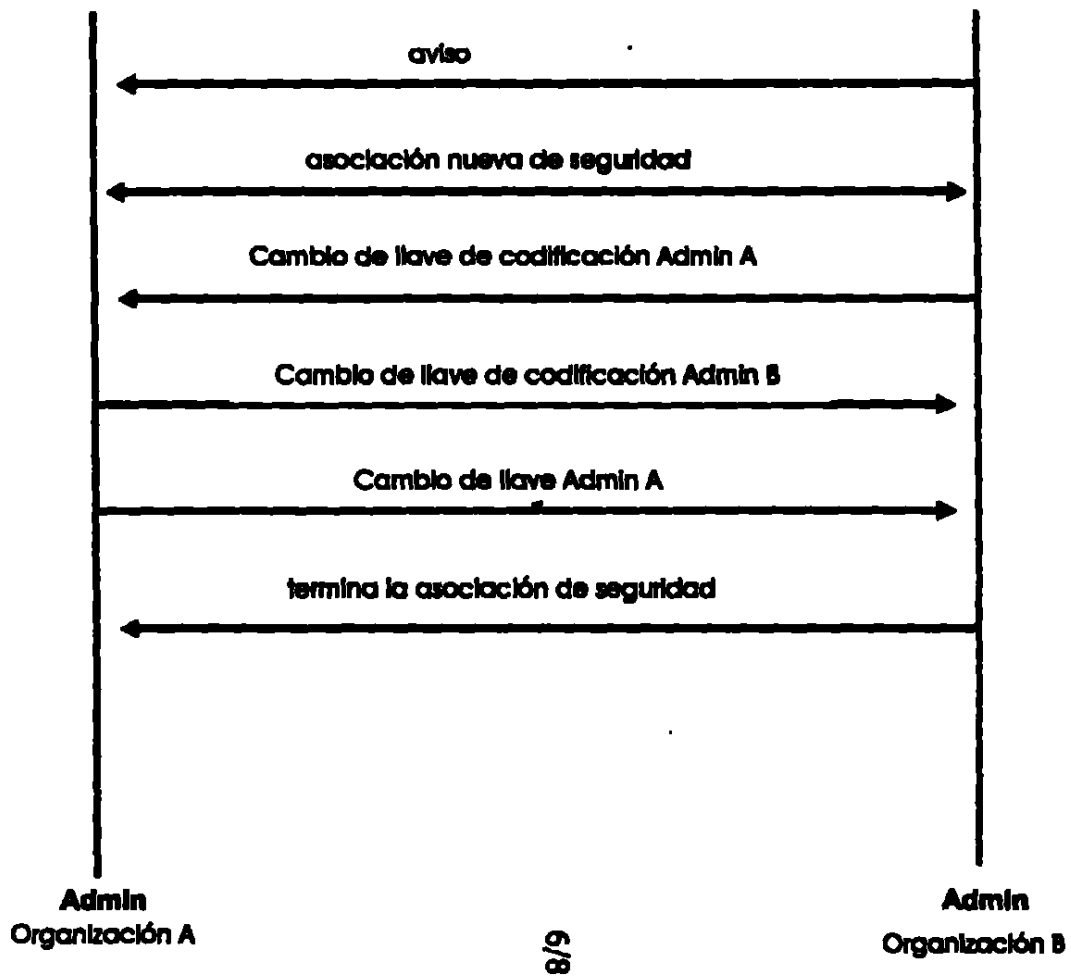
8/5



105

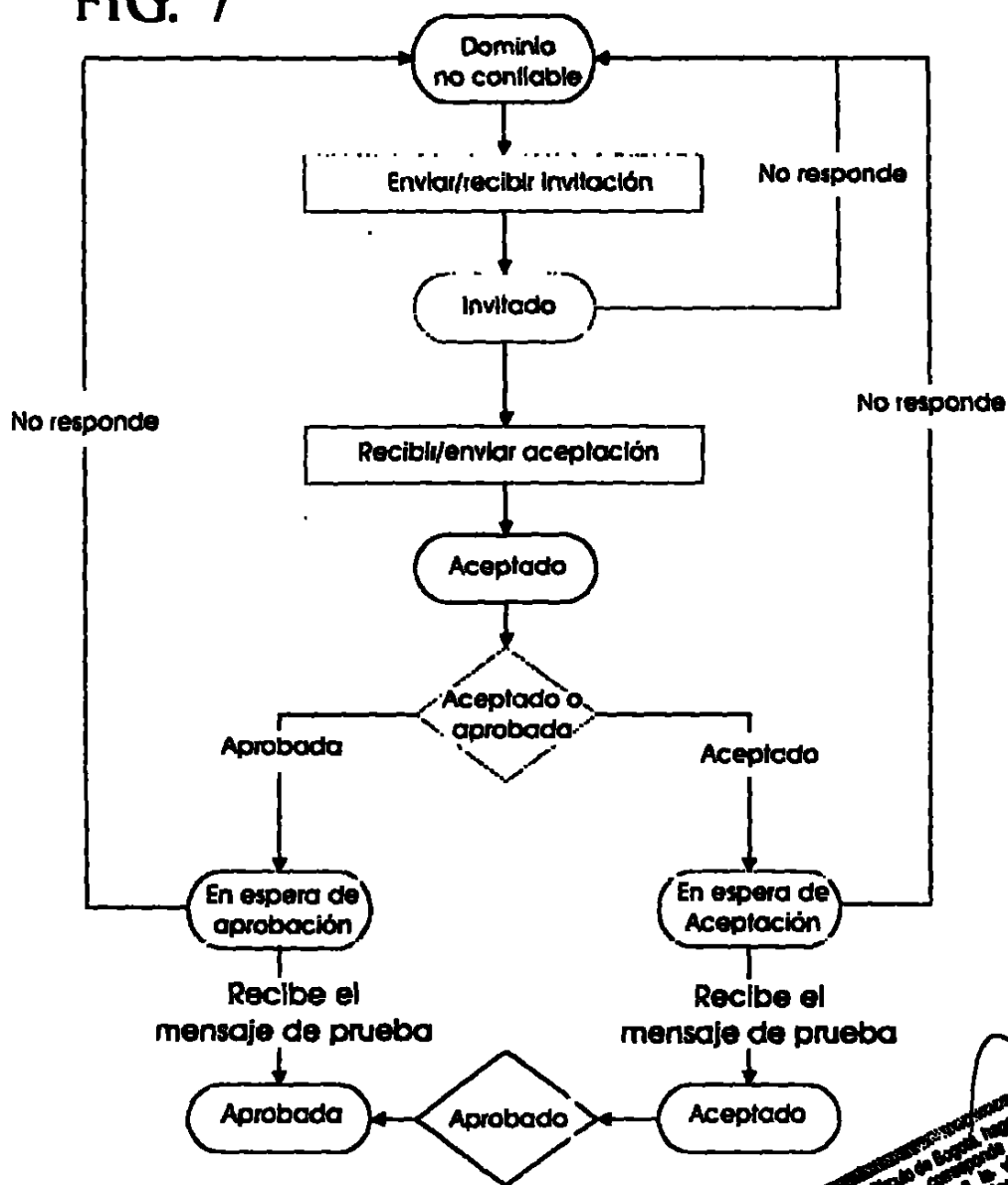
318

FIG. 6

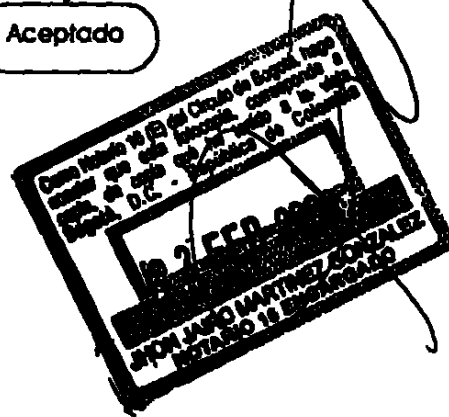


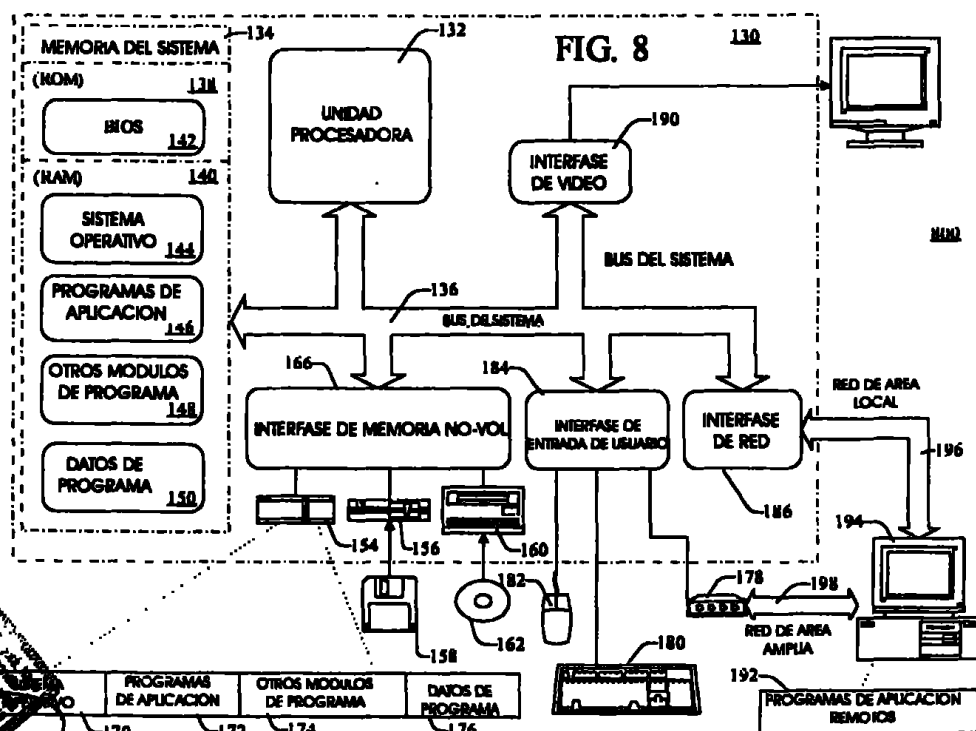
166

FIG. 7

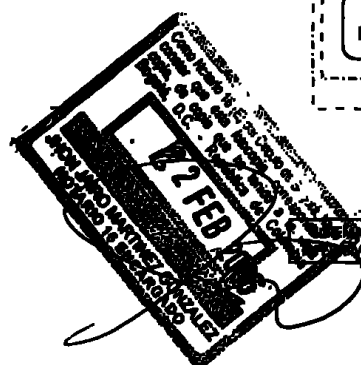


7/8





8/8



168

331

PA 1489003



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

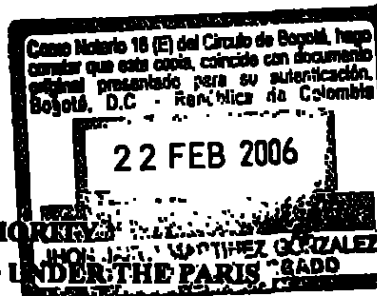
December 28, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 60/659,279

FILING DATE: March 07, 2005

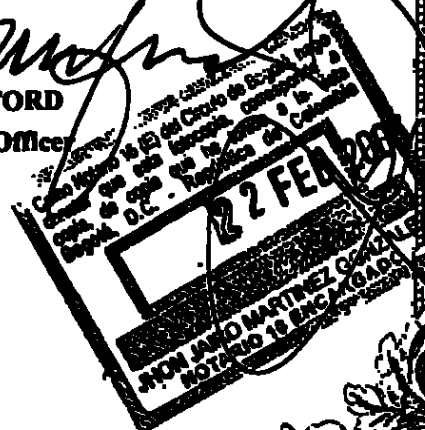
THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS US60/659,279



By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office



[Signature]
M. BASSFORD
Certifying Officer

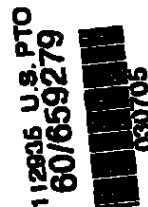


109



Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Express Mail Label No. EV453251602US
Attorney Docket No. MS#311610.01(5169)



332

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S):

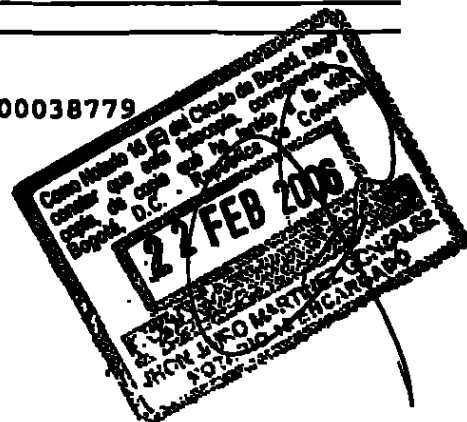
1. Tribble, Eric D.
LAST NAME FIRST NAME MIDDLE INITIAL
Redmond, WA
RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
2. Freeman, Trevor W.
LAST NAME FIRST NAME MIDDLE INITIAL
Redmond, WA
RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
3. _____
LAST NAME FIRST NAME MIDDLE INITIAL

RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)

[] Additional inventors are being named on the _____
separately numbered sheet(s) attached hereto.

Title of the Invention: SYSTEM AND METHOD FOR ESTABLISHING A
LINK BETWEEN A SERVER AND A TARGET

Correspondence Address: Customer Number 000038779



120

ENCLOSED APPLICATION PARTS:

- ☒ Specification - Number of Pages 24
- ☒ Drawings - Number of Sheets 8
- ☒ Application Data Sheet
- ☐ CD(s), Number
- ☒ Return Receipt Postcard
- ☐ Other (specify) _____

METHOD OF PAYMENT OF FILING FEE:

- ☐ Applicant claims small entity status
- ☐ A check in the amount of \$_____ is enclosed to cover the filing fee (and application size fee, if applicable). The Commissioner is hereby authorized to charge any underpayment or credit any overpayment to Deposit Account No. 19-1345.
- ☒ The Commissioner is hereby authorized to charge the filing fee (and application size fee, if applicable) to Deposit Account No. 19-1345. A duplicate copy of this form is enclosed for fee processing.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- ☒ No
- ☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

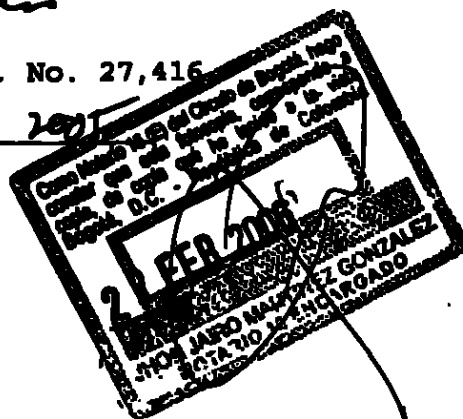
Respectfully submitted,

Frank R. Agovino

Frank R. Agovino, Reg. No. 27,416

Date: March 7, 2005

FRA/dep



334

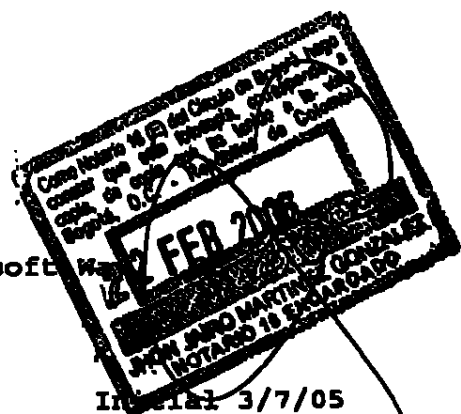
APPLICATION DATA SHEET

Application Information

Application Type:: Provisional
Subject Matter:: Utility
Suggested Classification::
Suggested Group Art Unit::
Title:: SYSTEM AND METHOD FOR
ESTABLISHING A LINK BETWEEN A
SERVER AND A TARGET
Attorney Docket Number:: MS#311610.01 (5169) ,
Request for Early Publication?:
Request for Non-Publication?:
Suggested Drawing Figure::
Total Drawing Sheets:: 8
Small Entity?: No
Petition Included?: No
Petition Type::
Licensed US Govt. Agency::
Contract or Grant Numbers::
Secrecy Order in Parent?:

Applicant Information

Applicant Authority Type:: Inventor
----- Primary Citizenship Country:: US -----
Status:: Full Capacity
Given Name:: Eric
Middle Name:: D.
Family Name:: Tribble
Name Suffix::
City of Residence:: Redmond
State or Province of Residence:: WA
Country of Residence:: US
Street of Mailing Address:: One Microsoft Way
City of Mailing Address:: Redmond



122

335

State or Province of Mailing
Address:: WA
Country of Mailing Address:: US
Postal Code of Mailing Address:: 98052-6399

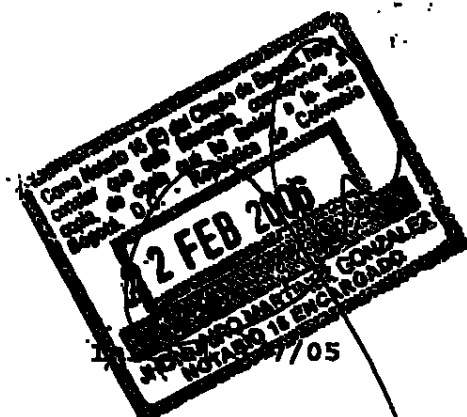
Applicant Authority Type:: Inventor
Primary Citizenship Country:: US
Status:: Full Capacity
Given Name:: Trevor
Middle Name:: W.
Family Name:: Freeman
Name Suffix::
City of Residence:: Redmond
State or Province of Residence:: WA
Country of Residence:: US
Street of Mailing Address:: One Microsoft Way
City of Mailing Address:: Redmond
State or Province of Mailing
Address:: WA
Country of Mailing Address:: US
Postal Code of Mailing Address:: 98052-6399

Correspondence Information

Correspondence Customer Number:: 000038779

Representative Information

Representative Customer Number:: 000038779



123

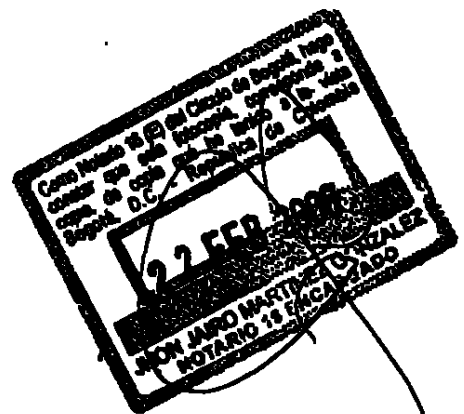
336

Domestic Priority Information			
APPLICATION::	CONTINUITY TYPE::	PARENT APPLICATION::	PARENT FILING DATE::

Foreign Priority Information			
COUNTRY::	APPLICATION NUMBER::	FILING DATE::	PRIORITY CLAIMED::

Assignee Information

Assignee Name::	Microsoft Corporation
Street of Mailing Address::	One Microsoft Way
City of Mailing Address::	Redmond
State or Province of Mailing Address::	WA
Country of Mailing Address::	US
Postal or Zip Code of Mailing Address::	98052



124

337

SYSTEM AND METHOD FOR ESTABLISHING A LINK BETWEEN A SERVER AND A TARGET

TECHNICAL FIELD

[0001] Embodiments of the present invention relate to the field of establishing a compatible interconnection between two domains. In particular, embodiments of this invention relate to a system and method to reveal and discover mail servers with advanced capabilities.

BACKGROUND OF THE INVENTION

[0002] Some prior systems attempt to identify potential partners by communicating directly. However, these systems become vulnerable when communicating and, in particular, create a vulnerability to SPAM.

[0003] Accordingly, a system for discretely identifying a potential partner and progressive establishing a secure link between a server and a potential partner is desired to address one or more of these and other disadvantages.

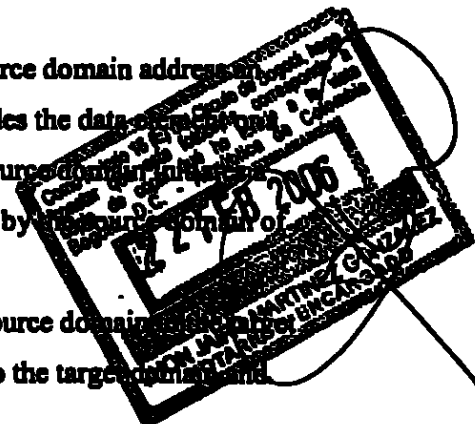
SUMMARY OF THE INVENTION

[0004] Embodiments of the invention include a method for establishing a link between a source domain and a target domain comprising:

[0005] Transmitting an advertisement from the source domain to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

[0006] Receiving by the source domain via the source domain address an invitation from the target domain wherein the invitation includes the data element corresponding to the data element wherein the source domain initiates the process to establish a link with the target domain upon receipt by the source domain of the invitation.

[0007] An advertisement is transmitted from the source domain to the target domain. The advertisement includes a data element specific to the target domain and



125

338

The advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain. The advertisement is received by the target domain including receiving the data element and the source domain address. An invitation is transmitted from the target domain to the source domain address. The invitation includes the data element or a data element corresponding to the data element. The source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

[0008] The invention also includes a system and a data structure.

[0009] Alternatively, the invention may comprise various other methods and apparatuses.

[0010] Other features will be in part apparent and in part pointed out hereinafter.

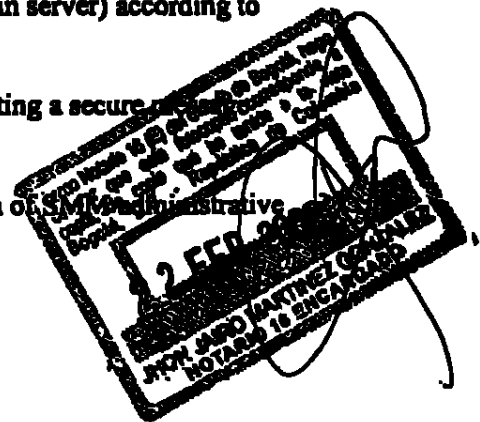
BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 is an exemplary block diagram of edge servers 1 and 2 within a DMZ and having secure messaging therebetween. The servers are connected via a firewall to bridges 1 and 2 which are part of a separate secure messaging system. Edge servers 1 and 2 form a subnetwork that is located between a trusted internal network, such as a secure messaging system linking bridges 1 and 2, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers via firewalls.

[0012] FIG. 2 is an exemplary diagram illustrating workflow between a source domain server and a potential partner (e.g., a target domain server) according to the invention.

[0013] FIG. 3 is an exemplary block diagram illustrating a secure manager according to the invention.

[0014] FIG. 4 is a flow diagram illustrating operation of SMTP administrative routing according to the invention.



128

339

[0015] FIG. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention.

[0016] FIG. 6 is an exemplary block diagram illustrating an inter-organization workflow summary between a server (admin organization A) and a partner (admin organization B) according to the invention.

[0017] FIG. 7 is a flow diagram illustrating a state diagram after a new security association implemented between a server and a partner according to the invention.

[0018] FIG. 8 is a block diagram illustrating one example of a suitable computing system environment in which the invention may be implemented.

[0019] Corresponding reference characters indicate corresponding parts throughout the drawings.

DETAILED DESCRIPTION OF THE INVENTION

[0020] The invention relates to a system and method for establishing a link between a server and a target. In particular, the invention relates to a system and method for establishing a secure link for the deployment of secure email. The invention allows a server to determine that a potential partner can be established as a target because of compatible secure email technology. As a result, once a potential partner is identified, the server can securely exchange key material information with the potential partner in order to establish the secure link.

[0021] The objective of domain signing and encryption according to the invention is to provide a transport independent mechanism to exchange confidential and server authenticated messages between servers. Fig. 1 is an exemplary block diagram of edge servers 1 and 2 within a demilitarized zone (DMZ). The servers 1 and 2 have a secure messaging link therebetween. The servers are separated by a firewall through which they are connected to bridge servers 1 and 2. The bridge servers are part of a secure messaging system. Edge servers 1 and 2 form a sub-network that is connected between a trusted internal network, such as the secure messaging system, and servers 1 and 2 and the untrusted external network, such as the public internet. Firewalls are also positioned between the edge servers and the internet. In this illustration



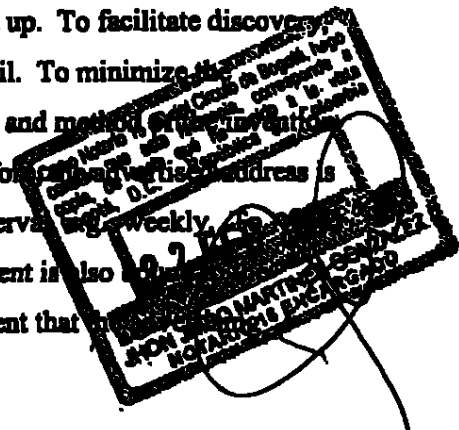
122

1, edge server 1 can exchange signed and encrypted mail with edge server 2 and bridge server 1 can exchange signed and encrypted mail with bridge server 2. In addition, bridge server 1 can forward to its DMZ edge server 1 either signed or signed and encrypted mail where the decryption recipient is bridge server 2. The edge servers treat all mail as clear text and encrypt all mail edge to edge. If the edge and bridge servers do not share the same encryption keys, the edge servers cannot decrypt bridge encrypted mail.

[0022] There is a need for a single point of administration for the authoritative data for all internal and external relationships. Optionally, a single master model rather than a multiple-master model is implemented because it is simpler and because it does not have to resolve replication conflicts. Secure message management (SMM) operations are usually infrequent and the database size is usually small so that there is sufficient time to repair or replace hardware or do a system restore before any loss of service. In one embodiment, critical data for operation is replicated to other edge servers. Since there is no single point of management, not all data is replicated and the replicated data is read only.

[0023] A server may engage with a number of its partners to set up secure mail links for a specific project. However, the management coordination of such projects does not usually scale. For secure messaging to make an impact, secure mail is enabled with the majority of the organizations business partners. This requires the ability to discover which partners have edge servers installed and have a simple organization-to-organization workflow to negotiate the establishment of a secure mail link.

[0024] The invention permits discovery of edge servers installed in a organization's partners so that a secure connection can be set up. To facilitate discovery, the server advertises the presence of itself with outbound mail. To minimize the advertisement process being vulnerable to attack, the system and method of the invention do not use a hard coded address in its advertisement. Therefore, the advertisement address is a random mailbox name which can rotate at a reasonable interval, e.g., weekly. To ensure that the vulnerabilities are minimized, the advertisement is also sent to a domain to which it is sent, e.g., the target domain. In the event that

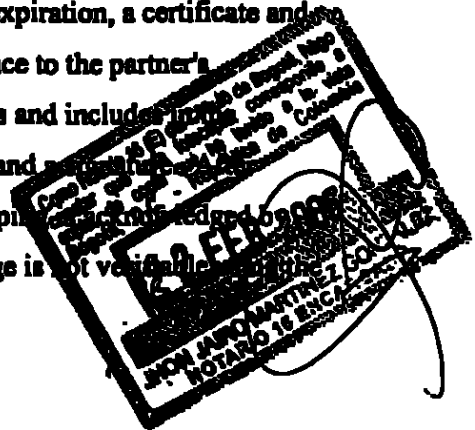


341

address is discovered by a third party the only domain that would be affected is the domain whose invitation address was compromised.

[0025] In one form, the advertisement is an 822 header containing the ephemeral 822 address for invitations and the expiration time in hours of the 822 address relative to when the message was sent. Inbound mail is filtered by the receiving server (e.g., target or partner server) for advertisements from edge servers and compared against a list of known edge servers. Any additions to that list are communicated to the local administrative SMM. On discovery of a new edge server, the SMM can send a probe message (e.g., an invitation) to the other SMM to offer a turn on domain signing and encryption. On receipt of an invitation or advertisement from another SMM administrator, if the message is verifiable under the existing trust policy then the local SMM could invoke a policy to automatically accept the invitation. Alternatively, the SMM administrator may require manual approval before accepting the invitation. On receipt of the invitation acceptance by the server, if the message is intrinsically verifiable, then the receiving SMM would invoke a policy to automatically start using domain signing and encryption. The configuration of a new secure domain is an asynchronous process and is not used for real data until the link is confirmed operationally by receipt of the ping acknowledgements.

[0026] Fig. 2 is an exemplary diagram illustrating workflow between a source domain server and a potential partner (e.g., target domain computer) according to the invention. Initially, an advertisement including an administrative address, a challenge token and an expiration date are sent from the server to the partner. When the partner recognizes the advertisement, the partner sends an invitation back to the server addressed to the administrative address that was part of the advertisement. The invitation from the partner includes an administrative address of the partner, the expiration, a certificate and the challenge token. In response, the server sends an acceptance to the partner's administrative address from the server's administrative address and includes in the acceptance the expiration, the certificate, the challenge token and a receipt of the acceptance. The partner pings the server and the ping is acknowledged by the server to establish the connection. If the invitation message is not verifiable



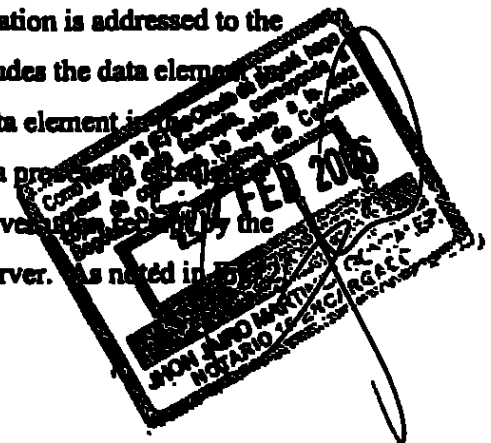
129

342

trust policy as illustrated in Fig. 2, then the request may be cued awaiting manual approval.

[0027] Referring to Fig. 3, an exemplary block diagram illustrating a secure message manager according to the invention is illustrated. The acceptance of the invitation by the partner creates a cross certificate on the administrative SMM agent which is then pushed to the worker SMM agents along with the encryption certificate. The cross certificate constrains the set of names accepted by the new trust and the restriction to domain edge server communication. In order to facilitate improved performance, the sending SMMs assign a session key and reuse the session key across multiple messages to a recipient SMM. The session key may also be distributed in this case from administration SMM to all worker SMM so all workers use the same key to reduce cache size. To allow for scaling out, the corresponding decryption private key for the encryption certificate should be available on all internet facing edge servers to allow any to decrypt inbound mail. This may be generated in a single place, i.e., the administration agent and distributed to all worker servers. Once a trust relationship is established, it should be maintained. For example, the original certificate may be retained and a renewal request sent to the other SMMs before the certificate expires.

[0028] From the server's perspective, the method according to the invention establishes a link between a source domain and a target domain. Initially a source domain server transmits an advertisement to potential target domains. The advertisement includes a data element such as a mention or a token or other secret which is specifically assigned to the target domain. In addition, the advertisement includes a source domain address to which the target domain is permitted to send a message in order to establish a link between the source domain server and the target computer. The source domain server receives an invitation from the target domain which invitation is addressed to the source domain address previously provided. The invitation includes the data element from the advertisement or a data element which corresponds to the data element in the advertisement. This allows the source domain server to initiate a process to establish a link between the target domain server and the source domain server. As noted in Fig. 3, the source domain server of the invitation from the target domain server.



100

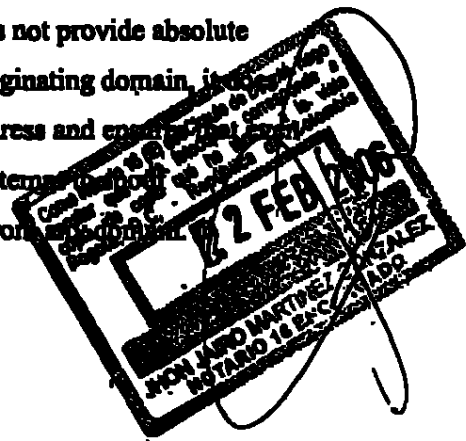
343

the source domain server transmits an acceptance to the target domain server to establish the link therebetween.

[0029] In one embodiment, the source domain selectively transmits the advertisement to target domains from which the source domain has received a message. Alternatively or in addition, the source domain may send advertisements to target domains which have been specifically identified in advance. Alternatively or in addition, the source domain may send the advertisement to randomly selected target domains.

[0030] In one embodiment, the advertisement may be a message which is generated in response to user action. Alternatively or in addition, the advertisement may be a message with a single target domain and/or a message to a target domain which is an operator. The single message to the target domain may be for each key and it may be sent on a time-based determination (e.g., one message per hour). For example, the user action may be NDRs or return receipts.

[0031] In one embodiment of the invention, an email server occasionally adds an additional header (an "x-header") to a message that will be delivered to another email domain. The data in the header includes a secret that is specific to the target domain and the email address to which the administrative messages from the target domain can be directed back to the email server. If mail at the target domain is also directed through a server that implements this embodiment of the invention, then it will detect the additional header and determine that there may be a compatible server at the originating domain. The target domain then directs administrative traffic such as requests to establish a secure connection to the contained administrative email address. As noted above, such administrative messages must also contain the secret that was provided for the target domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the target domain but that does not contain the secret corresponding to the target domain. Although this does not provide absolute assurance that the received administrative mail is from the originating domain, it does minimize the vulnerability to SPAM at the administrative address and ensure that an attacker that can see email to the target domain can only attempt to guess administrative addresses from the target domain rather than from any domain.



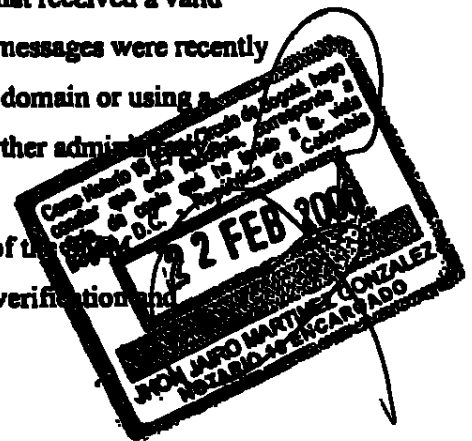
(81)

344

[0032] In one embodiment, the invention is implemented by using a header, called a mention, that is attached to an already outbound email from the source domain. This mention reveals the availability of specific functions on the mail server originating the outbound email while avoiding the need for generating additional, possibly undesirable, messages. As noted above, the administrative email address would be included in the mention and there would be a per-domain secret, called a token to mitigate risks of SPAM to the administrative email address. This would support workflow messages at the administrative email address.

[0033] The token (or secret) may be generated from a hash of the target domain and a secret seed that is kept on the originating server. This allows a single seed to be shared across multiple servers, so that each server will generate the same token unique to any target domain. When an administrative message is received at the originating server (because it is directed to the administrative address included in the mention), the token provided in the administrative messages is checked by the originating server. To check the token, the email server generates a token for the domain that sent the administrative message using the current internal seed. If the generated token is the same as the one in the administrative messages, then that message has the correct token and is passed through to the appropriate destination for administrative messages. If the token does not match, then the same process is applied to prior tokens (up to a bounded number). If none of the currently valid seeds can be used to generate a token that matches the token in the incoming message, then the message is not considered valid and is discarded or rejected, and not passed on to the eventual destination for administrative messages. This prevents unauthorized SPAM attacks against the receiver of administrative messages, which may be unable to cope with large volumes of email. Additionally, to prevent denial of service attacks from a domain that received a valid token, the verification process is able to keep track of how many messages were recently passed through to the administrative destination from a particular domain or using a particular token. When that number exceeds an allowed limit, further administrative messages using that token are discarded or rejected.

[0034] Fig. 4 is a flow diagram illustrating operation of the administrative routing according to the invention. The signature verification and



182

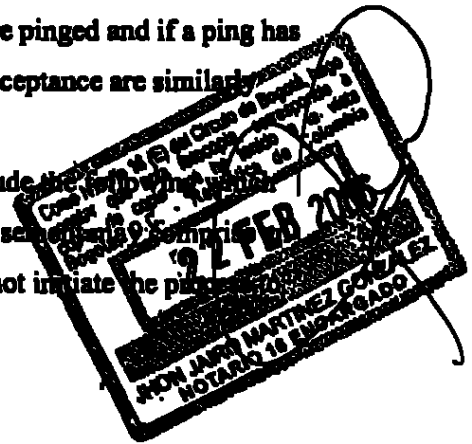
345

decryption must happen before any anti-SPAM processing because the output from the verification is necessary to set the message property flags used by the anti-SPAM agent. Signature verification should happen after the RBL and other IP address level functions. Thus, the process begins with receiving messages at the source domain address to which the target domain is permitted to send a message at 402. If it is determined at 404 that the token is not valid for the sender address, the message is dropped at 406 and the routing process ends. If the token is valid, the process proceeds to 408 to determine if the domain has a maximum account which has been exceeded. If the maximum has been exceeded, the message is dropped at 406; otherwise, if the signature is valid at 410 the message is routed to the local administrative agent.

[0035] Fig. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention. SMM signing and encryption is the last function generally. Each message going to a domain with a secure message relationship is signed and encrypted. This component also inserts the header containing the current SMM ephemeral address to all mail going to domains without a security relationship. As shown in Fig. 5, the domain looks for a valid signature at 502 and an external address at 504 after finding a valid token. If the signature is valid and there is no external address, the message is routed to the local worker agent at 506. If there is an external address, it is routed to such. Without a valid signature the message is dropped.

[0036] In one embodiment, the inter-organizational work flows as illustrated in Fig. 6 are implemented between administrative organizations. The workflow is performed by the SMM administrative agents and may include the exchange of an encryption key rollover. Fig. 7 is a state diagram illustrating the new security association. This diagram only considers the positive cases and the terminal cases. It does not include other aspects such as re-transmission of messages prior to the re-transmission limit. In general, domains looking for approval are pinged and if a ping has been received the domain is approved. Domains looking for acceptance are similarly handled.

[0037] Other optional features of the invention include the advertisement expiration date in which case the source domain server would not initiate the ping.

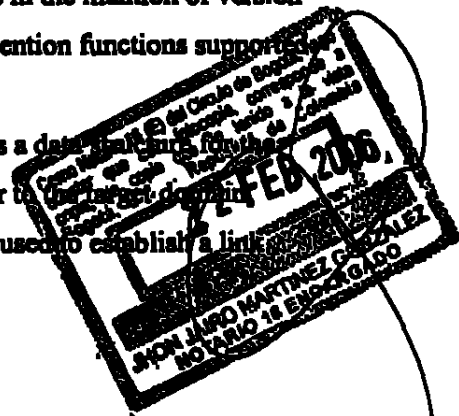


183

346

establish a link with the target domain computer (e.g., server) computer when receipt by the source domain server of the invitation is after the expiration date. The data element may be at least one of the following: a per domain secret including a pseudorandom number for each target domain computer (e.g., server), a secret generated via hashing the target domain computer (e.g., server) and a secret seed that is used to generate per-domain secrets for more than one domain; and a per-domain secret generated encrypting the target domain computer (e.g., server) and an expiration date of the secret. The data element may comprise a secret in which case the source domain server would verify the secret received from the target domain computer (e.g., server) by re-computing and then comparing the current secret for the target domain computer (e.g., server) with the secret included in the advertisement. The data element may be selected from a plurality of multiple overlapping secrets for each target domain computer (e.g., server) so that there are a plurality of valid secrets that can be used for communicating from a target domain computer (e.g., server) to the administrative address of the originating domain. A limit may be imposed on the number of messages that are passed to the source domain server address with a particular data element so that denial of service attacks using a correct data element are mitigated. The source domain server may include the ability to override the requirement for a data element for a given target domain computer (e.g., server) to enable out-of-band authorization to send invitation messages from a particular domain. The data element may be a token in the advertisement message in a mail header or embedded in the body of a message or the data element may be a token in a mail header and the body of the message remains encrypted when passing through a mail server. The source domain server may support multiple simultaneously valid tokens for the same domain and verify invitation messages from sub-domains of the target domain computer (e.g., server) by verifying the incoming token against tokens for the target domain computer (e.g., server). The data element may be a mention and include in the mention of version information for the source domain server and include in the mention functions supported by the source domain server.

[0038] In one embodiment the invention comprises a data element that is used in an advertisement to be transmitted from the source domain server to the target domain computer (e.g., server). As noted above, this data structure is used to establish a link



124

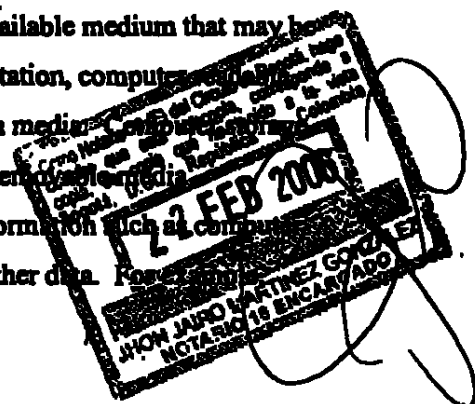
347

between the source domain server and the target domain computer (e.g., server). The data structure includes a message and its usual header relating to the message. Additionally, the data structure includes an additional header attached to the message and message header and including a data element specific to the target domain computer (e.g., server). The header also includes a source domain server address to which the target domain computer (e.g., server) is permitted to send a message to the source domain server in order to establish a link between the source domain server and the target domain computer (e.g., server). As noted above, the additional header should include an expiration date, although this is optional.

[0039] Exemplary Operating Embodiment:

[0040] FIG. 8 shows one example of a general purpose computing device in the form of a computer 130. In one embodiment of the invention, a computer such as the computer 130 is suitable for use in the other figures illustrated and described herein. Computer 130 has one or more processors or processing units 132 and a system memory 134. In the illustrated embodiment, a system bus 136 couples various system components including the system memory 134 to the processors 132. The bus 136 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0041] The computer 130 typically has at least some form of computer readable media. Computer readable media, which include both volatile and nonvolatile media, removable and non-removable media, may be any available medium that may be accessed by computer 130. By way of example and not limitation, computer readable media comprise computer storage media and communication media. Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. For example,



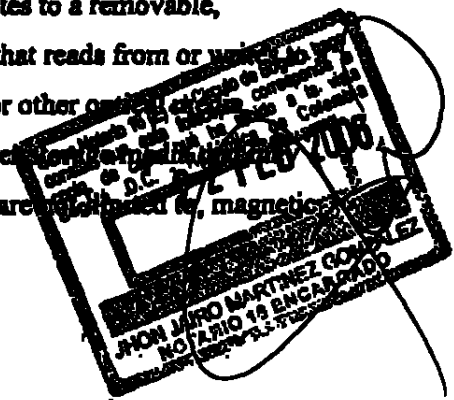
185

348

computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that may be used to store the desired information and that may be accessed by computer 130. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Those skilled in the art are familiar with the modulated data signal, which has one or more of its characteristics set or changed in such a manner as to encode information in the signal. Wired media, such as a wired network or direct-wired connection, and wireless media, such as acoustic, RF, infrared, and other wireless media, are examples of communication media. Combinations of any of the above are also included within the scope of computer readable media.

[0042] The system memory 134 includes computer storage media in the form of removable and/or non-removable, volatile and/or nonvolatile memory. In the illustrated embodiment, system memory 134 includes read only memory (ROM) 138 and random access memory (RAM) 140. A basic input/output system 142 (BIOS), containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is typically stored in ROM 138. RAM 140 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 132. By way of example, and not limitation, FIG. 8 illustrates operating system 144, application programs 146, other program modules 148, and program data 150.

[0043] The computer 130 may also include other removable/non-removable, volatile/nonvolatile computer storage media. For example, FIG. 8 illustrates a hard disk drive 154 that reads from or writes to non-removable, nonvolatile magnetic media. FIG. 8 also shows a magnetic disk drive 156 that reads from or writes to a removable, nonvolatile magnetic disk 158, and an optical disk drive 160 that reads from or writes to a removable, nonvolatile optical disk 162 such as a CD-ROM or other optical disk. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to, magnetic



126

349

[0045] A user may enter commands and information into computer 130 through input devices or user interface selection devices such as a keyboard 180 and a pointing device 182 (e.g., a mouse, trackball, pen, or touch pad). Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to processing unit 132 through a user input interface 184 that is coupled to system bus 136, but may be connected by other interface and bus structures, such as a parallel port, game port, or a Universal Serial Bus (USB). A monitor 188 or other type of display device is also connected to system bus 136 via an interface, such as a video interface 190. In addition to the monitor 188, computers often include other peripheral output devices (not shown) such as a printer and speakers, which may be connected through an output peripheral interface (not shown).

d environment using
remote comput
a power
le supply to all
connections
network

25 FEB 2006
JHON JAIRO MARTINEZ GONZALEZ
NOTARIO 18 ENCARGADO

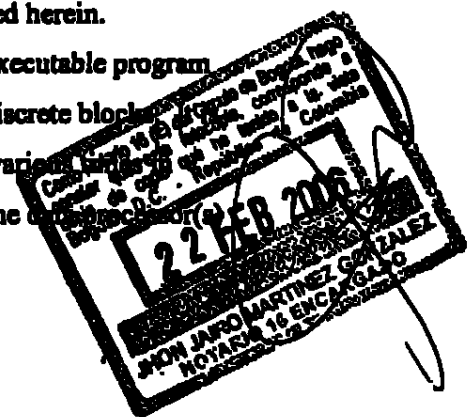
350

may also include other networks. LAN 136 and/or WAN 138 may be a wired network, a wireless network, a combination thereof, and so on. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and global computer networks (e.g., the Internet).

[0047] When used in a local area networking environment, computer 130 is connected to the LAN 196 through a network interface or adapter 186. When used in a wide area networking environment, computer 130 typically includes a modem 178 or other means for establishing communications over the WAN 198, such as the Internet. The modem 178, which may be internal or external, is connected to system bus 136 via the user input interface 184, or other appropriate mechanism. In a networked environment, program modules depicted relative to computer 130, or portions thereof, may be stored in a remote memory storage device (not shown). By way of example, and not limitation, FIG. 8 illustrates remote application programs 192 as residing on the memory device. The network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0048] Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described below in conjunction with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described herein.

[0049] For purposes of illustration, programs and other executable program components, such as the operating system, are illustrated herein as discrete blocks, recognized, however, that such programs and components reside at various times in different storage components of the computer, and are executed by the processor of the computer.



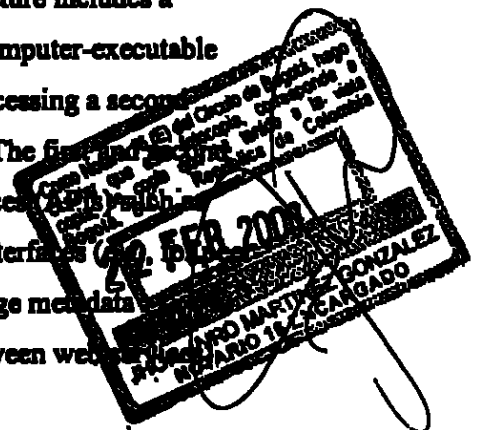
350

351

[0050] Although described in connection with an exemplary computing system environment, including computer 130, the invention is operational with numerous other general purpose or special purpose computing system environments or configurations. The computing system environment is not intended to suggest any limitation as to the scope of use or functionality of the invention. Moreover, the computing system environment should not be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the exemplary operating environment. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0051] The invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0052] An interface in the context of a software architecture includes a software module, component, code portion, or other sequence of computer-executable instructions. The interface includes, for example, a first module accessing a second module to perform computing tasks on behalf of the first module. The first and second modules include, in one example, application programming interfaces (APIs) (e.g., provided by operating systems, component object model (COM) interfaces (e.g., to-peer application communication), and extensible markup language metadata interchange format (XMI) interfaces (e.g., for communication between web



189

352

[0053] The interface may be a tightly coupled, synchronous implementation such as in Java 2 Platform Enterprise Edition (J2EE), COM, or distributed COM (DCOM) examples. Alternatively or in addition, the interface may be a loosely coupled, asynchronous implementation such as in a web service (e.g., using the simple object access protocol). In general, the interface includes any combination of the following characteristics: tightly coupled, loosely coupled, synchronous, and asynchronous. Further, the interface may conform to a standard protocol, a proprietary protocol, or any combination of standard and proprietary protocols.

[0054] The interfaces described herein may all be part of a single interface or may be implemented as separate interfaces or any combination therein. The interfaces may execute locally or remotely to provide functionality. Further, the interfaces may include additional or less functionality than illustrated or described herein.

[0055] In operation, computer 130 operates as either the source domain server or the target domain computer (which may be a server) to execute computer-executable instructions as noted above, such as those illustrated in Figs. 2-7.

[0056] The order of execution or performance of the methods illustrated and described herein is not essential, unless otherwise specified. That is, elements of the methods may be performed in any order, unless otherwise specified, and that the methods may include more or less elements than those disclosed herein. For example, it is contemplated that executing or performing a particular element before, contemporaneously with, or after another element is within the scope of the invention.

[0057] When introducing elements of the present invention or the embodiment(s) thereof, the articles "a," "an," "the," and "said" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0058] In view of the above, it will be seen that the several objects of the invention are achieved and other advantageous results attained.

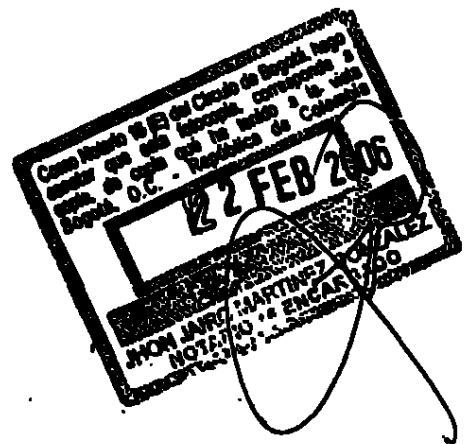
[0059] As various changes could be made in the above configurations, products, and methods without departing from the scope of the invention, it is intended that the scope of the invention be defined by the following claims.



190

353

that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.



1a1

354.

What is claimed is:

- 1. A method for establishing a link between a source domain and a target domain comprising:**

Transmitting an advertisement from the source domain to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

Receiving by the source domain via the source domain address an invitation from the target domain wherein the invitation includes the data element or a data element corresponding to the data element wherein the source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

- 2. The method of claim 1 further comprising transmitting an acceptance from the source domain to the target domain to establish the link therebetween.**

- 3. The method of claim 1 wherein the advertisement is selectively transmitted to at least one of the following:**

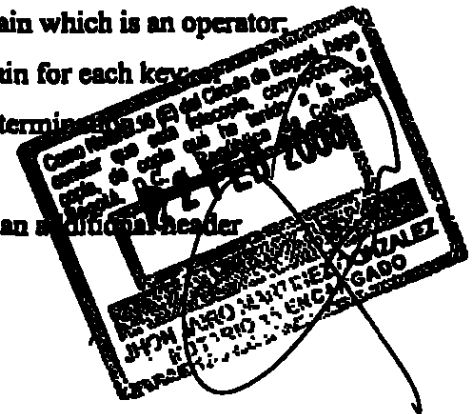
Target domains from which the source domain has received a message;

Target domains specifically-identified in advance; and

Randomly selected target domains.

4. The method of claim 1 wherein the advertisement is a message which is generated in response to user action; wherein the advertisement is a message with a single target domain; wherein the advertisement is a message to a target domain which is an operator wherein the advertisement is a single message to the target domain for each key; wherein the advertisement is a message send on a time-based determination.

5. The method of claim 1 wherein the advertisement comprises an additional header which includes the data element and the source domain address.



355

6. The method of claim 1 wherein the advertisement comprises an expiration date and wherein the source domain does not initiate the process to establish a link with the target domain when receipt by the source domain of the invitation is after the expiration date.

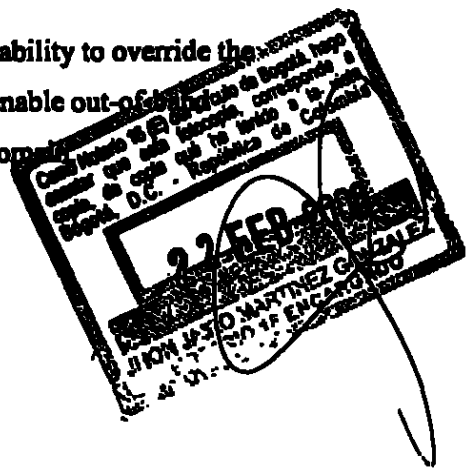
7. The method of claim 1 wherein the data element is at least one of the following:
 a per domain secret including a pseudorandom number for each target domain;
 a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain; and
 a per-domain secret generated encrypting the target domain and an expiration date of the secret.

8. The method of claim 1 wherein the data element comprises a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement.

9. The method of claim 1 wherein the data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain.

10. The method of claim 1 further comprising imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of service attacks using a correct data element are mitigated.

11. The method of claim 1 further comprising including the ability to override the requirement for a data element for a given target domain to enable out-of-band authorization to send invitation messages from a particular domain.



(a)

356

12. The method of claim 1 wherein the data element is a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server.

13. The method of claim 1 further comprising supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the target domain by verifying the incoming token against tokens for the target domain.

14. The method of claim 1 wherein the data element is a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

15. A data structure for an advertisement to be transmitted from a source domain to a target domain for establishing a link between the source domain and the target domain comprising:

A message;

A header relating to the message; and

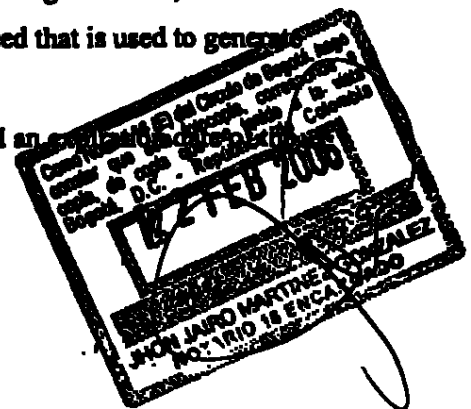
An additional header attached to the message and including a data element specific to the target domain and including a source domain address to which the target domain is permitted send a message to the source domain in order to establish a link between the source domain and the target domain, a challenge token and an expiration date.

16. The data structure of claim 15 wherein the data element is at least one of the following:

a per domain secret including a pseudorandom number for each target domain,

a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain;

a per-domain secret generated encrypting the target domain and an encryption key; and a secret;



194

357

a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement;

a data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain;

a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server; and

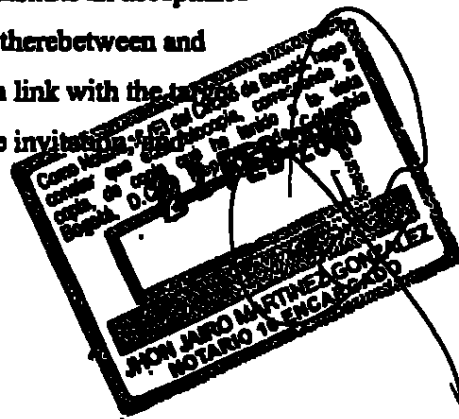
a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

17. A system for establishing a link between a source domain and a target domain comprising:

A source domain server transmitting an advertisement to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

A target domain computer receiving the advertisement including receiving the data element and the source domain address wherein the target domain computer transmits an invitation from the target domain to the source domain address wherein the invitation includes the data element or a data element corresponding to the data element.

18. The system of claim 17 wherein the source domain server transmits an acceptance form the source domain to the target domain to establish the link therebetween and wherein the source domain server initiates a process to establish a link with the target domain computer upon receipt by the source domain server of the invitation further comprising at least one of the following:



198

358

imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of Service attacks using a correct data element are mitigated;

overriding the requirement for a data element for a given target domain to enable out-of-band authorization to send invitation messages from a particular domain; and

supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the target domain by verifying the incoming token against tokens for the target domain.

19. The system of claim 17 wherein the advertisement transmitted by the source domain service comprises at least one of the following:

An advertisement selectively transmitted to target domains from which the source domain has received a message;

an advertisement selectively transmitted to target domains specifically identified in advance or randomly selected target domains;

a message which is generated in response to user action (e.g., NDRs, return receipts);

a message with a single target domain;

a message to a target domain which is an operator;

a single message to the target domain for each key;

a message send on a time-based determination (e.g., one message an hour);

an additional header which includes the data element and the source domain address; and

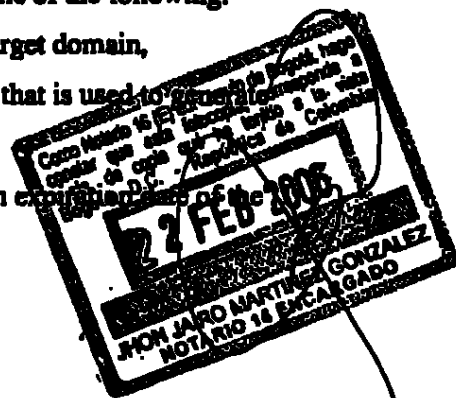
an expiration date and wherein the source domain does not initiate the process to establish a link with the target domain when receipt by the source domain of the invitation is after the expiration date.

20. The system of claim 17 wherein the data element is at least one of the following:

a per domain secret including a pseudorandom number for each target domain,

a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain;

a per-domain secret generated encrypting the target domain and an expiration date; and a secret;



176

359

a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement;

a data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain;

a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server; and

a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.



147

360

ABSTRACT

An advertisement is transmitted from the source domain to the target domain. The advertisement includes a data element specific to the target domain and. The advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain. The advertisement is received by the target domain including receiving the data element and the source domain address. An invitation is transmitted from the target domain to the source domain address. The invitation includes the data element or a data element corresponding to the data element. The source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

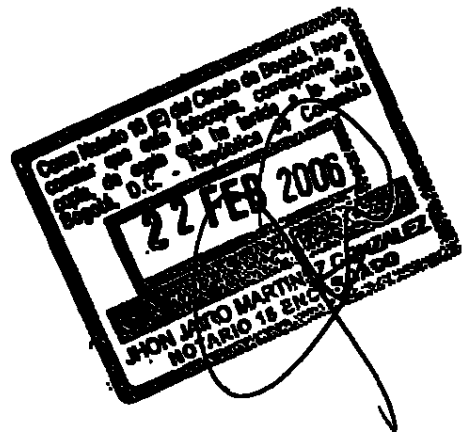


FIG. 1

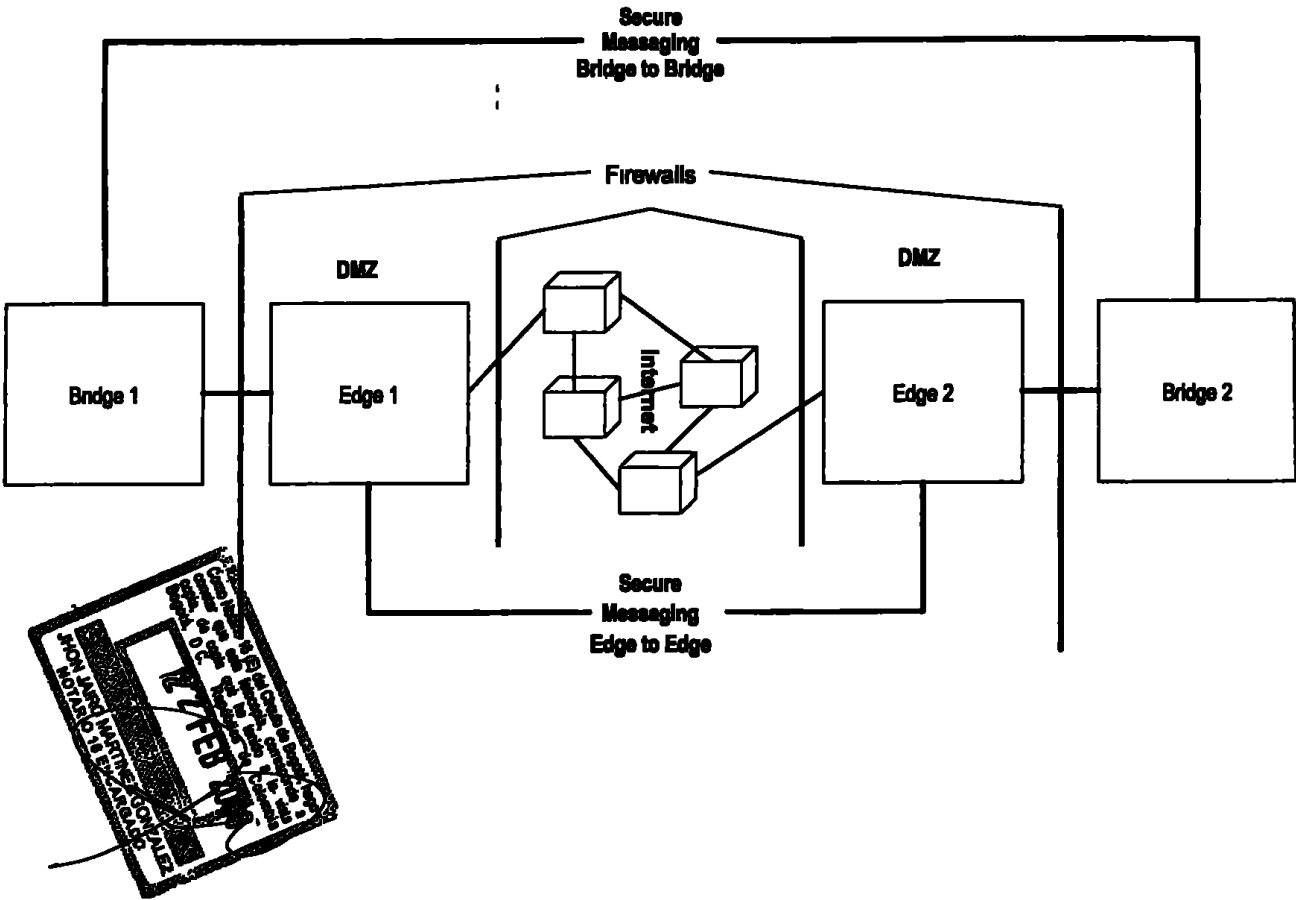
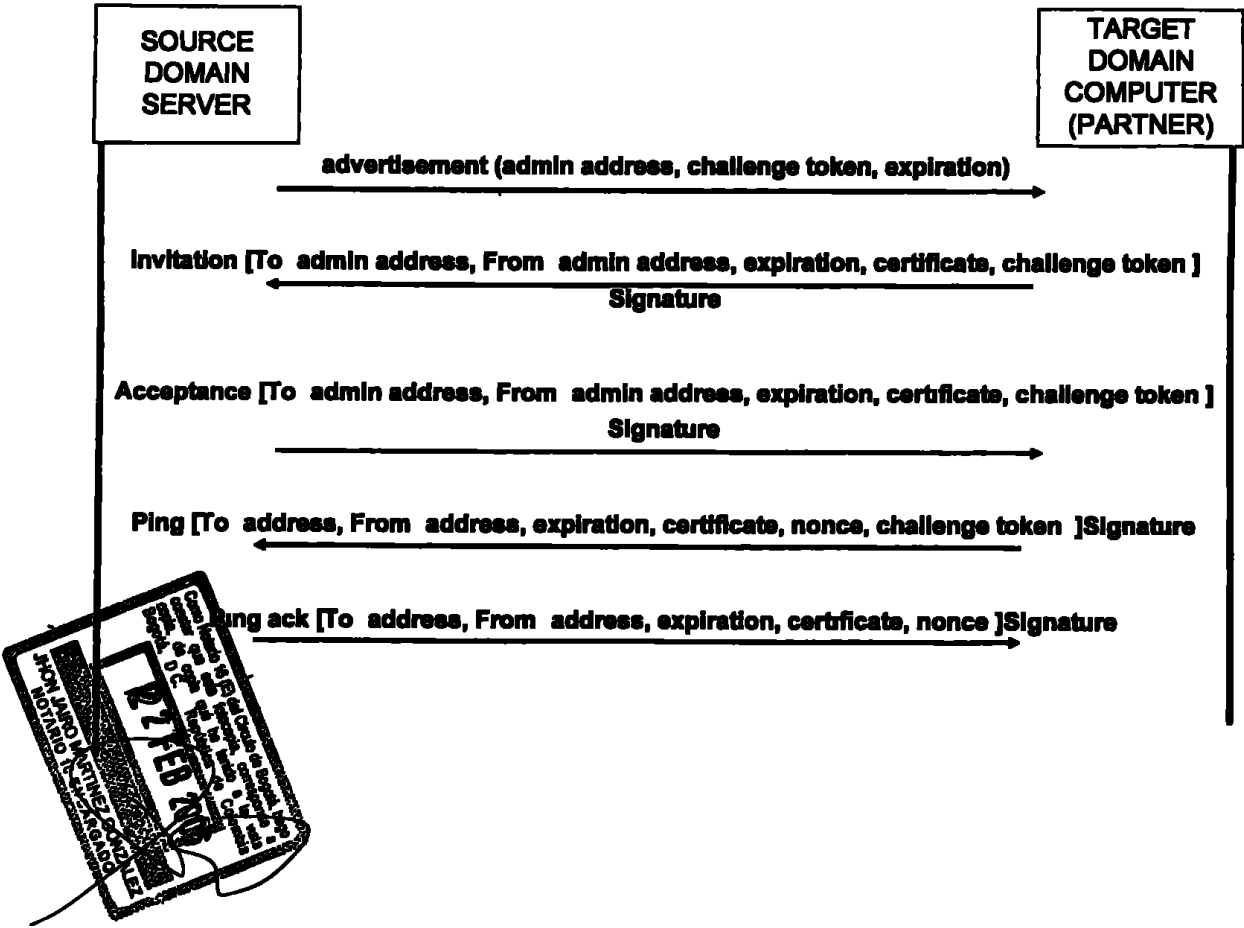


FIG. 2



200

29



FIG. 4

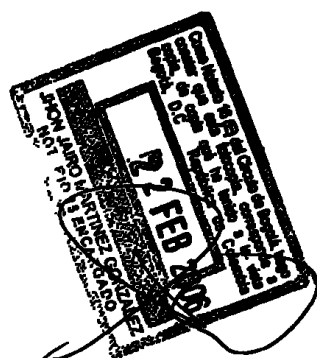
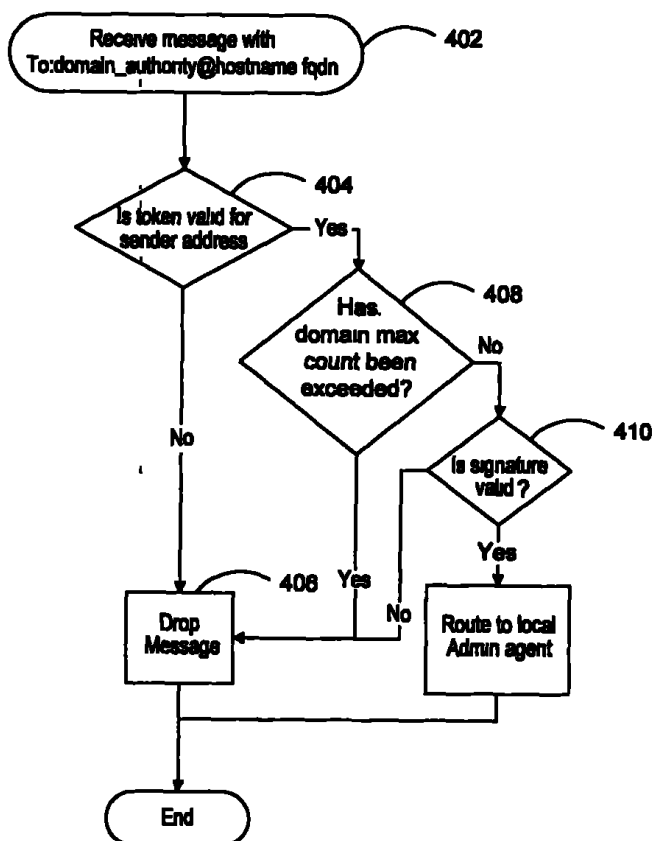


FIG. 5

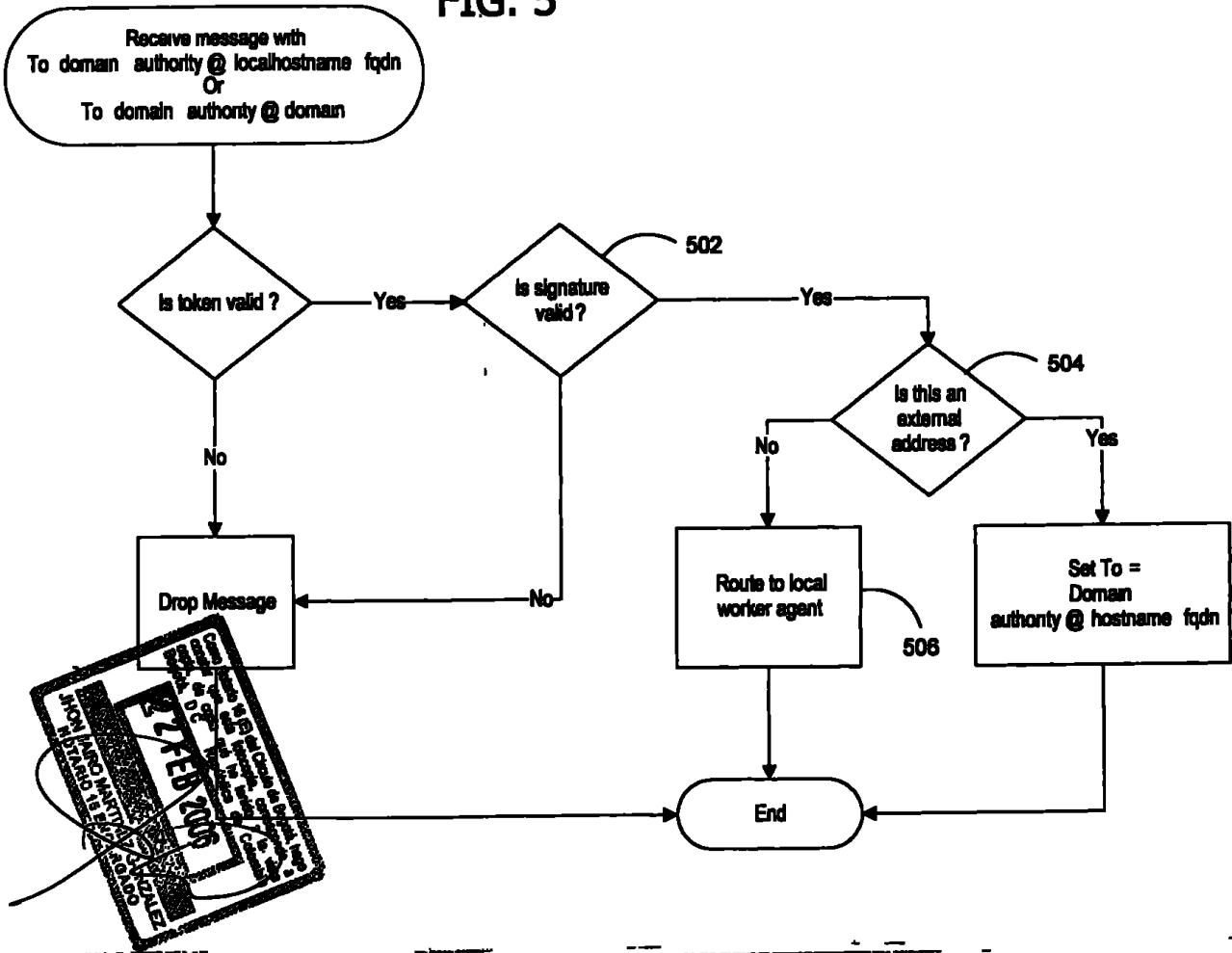


FIG. 6

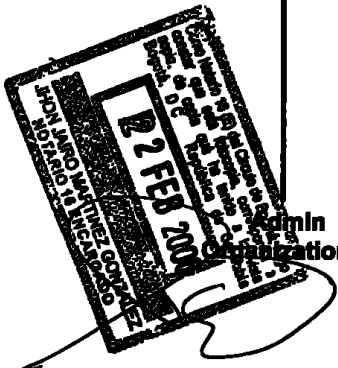
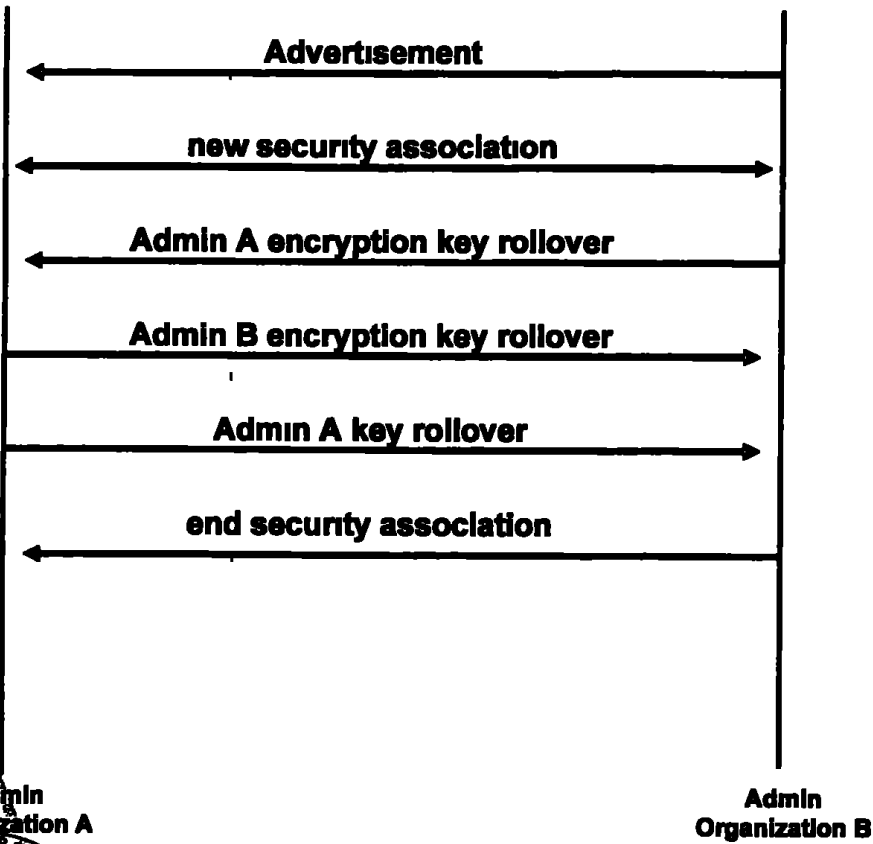
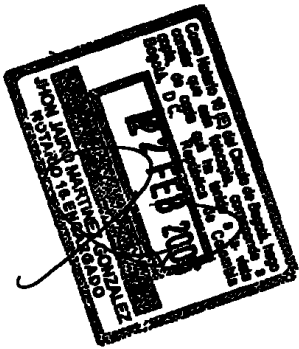
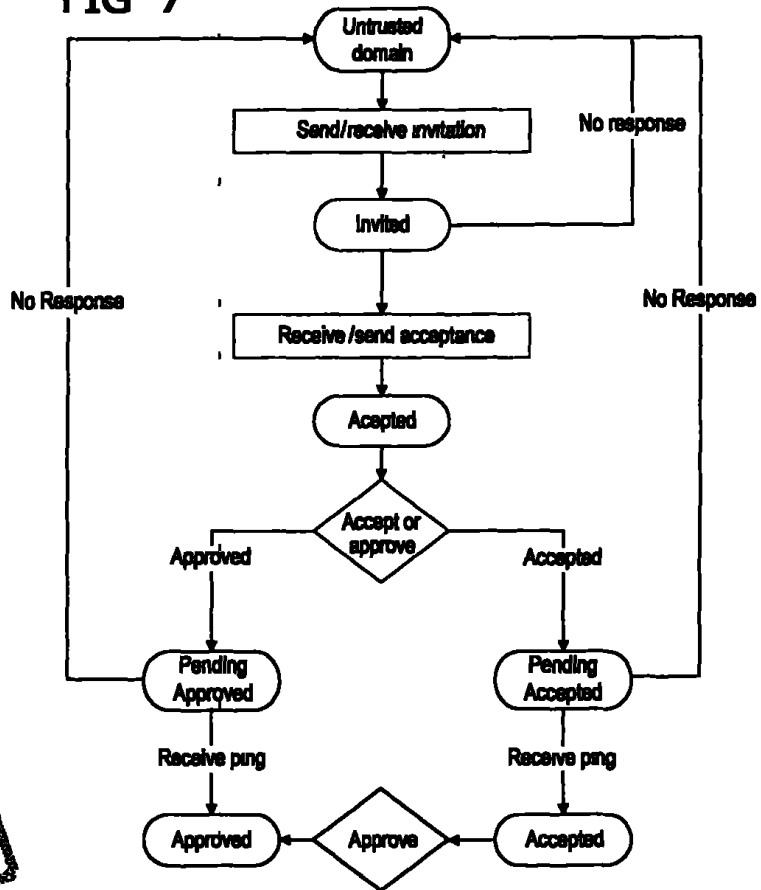
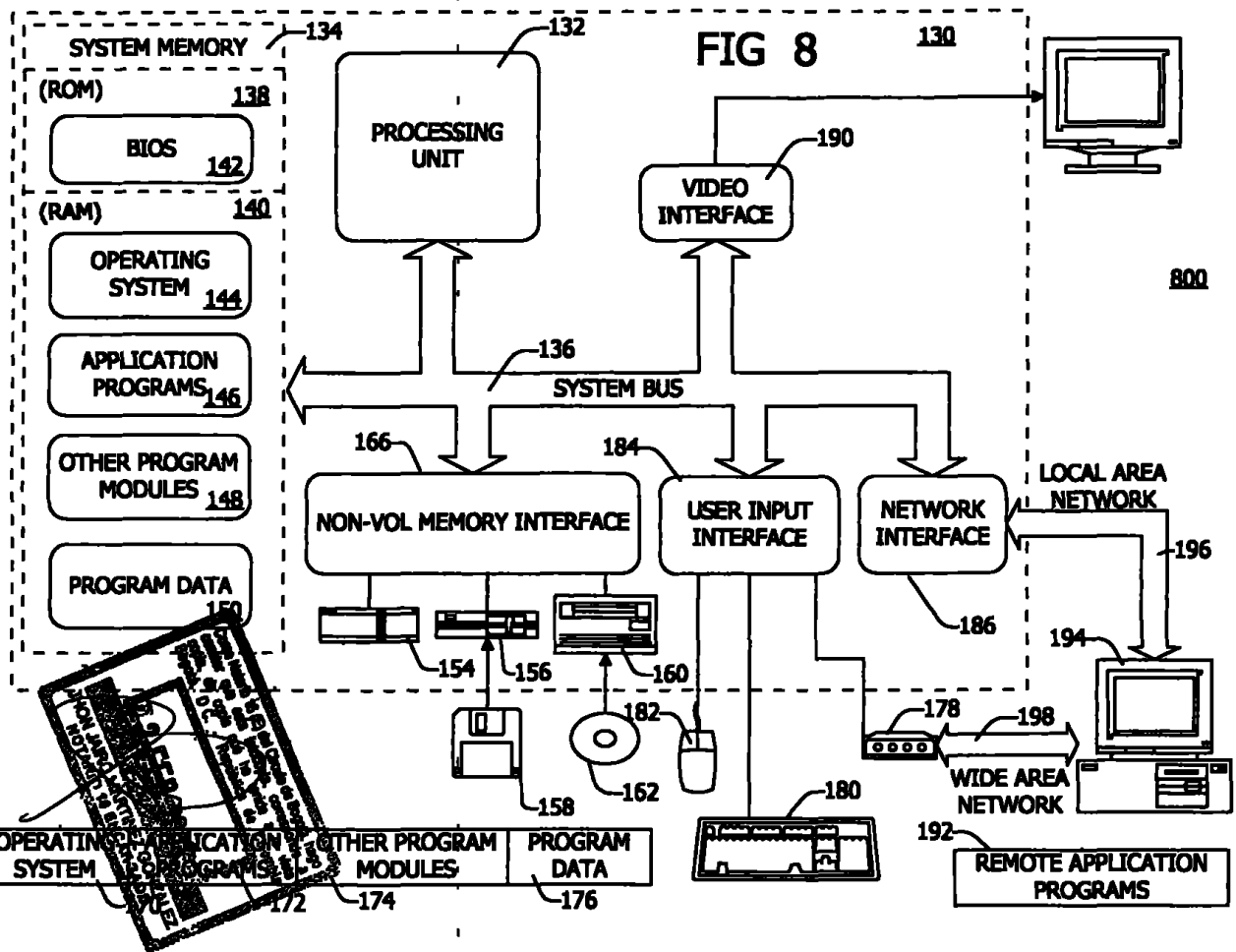


FIG 7





369

Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES EXTRACTO PARA PUBLICACIÓN SOLICITUD DE PATENTE DE INVENCION	
(21) N° de solicitud: 06-010.919 22) Fecha de solicitud: Febrero 6, 2006		(51) Int Cl: (71) Solicitante(s) MICROSOFT CORPORATION	
(30) Prioridad	(31) No. Prioridad 60/659,279 11/107,011	(32) Fecha Marzo 7, 2005 Abril 15, 2005	(33) País USA USA
		(72) Inventor(es) Eric D. Tribble Trevor W. Freeman	
		(74) Apoderado: DARIO CARDENAS NAVAS	
(54) Título: SISTEMA Y METODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE			

Resumen:

Un anuncio se transmite de un dominio fuente a un dominio objetivo. El anuncio incluye elementos de datos específicos al dominio objetivo y. El anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo. El anuncio lo recibe en dominio objetivo incluyendo la recepción del elemento de datos y la dirección de dominio fuente. Una invitación se transmite del dominio objetivo a la dirección del dominio fuente. La invitación incluye el elemento de datos o elemento de datos correspondiente al elemento de datos. El dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo tan pronto recibe del dominio fuente la invitación.

370

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCI

Folio 371

2020
Bogotá D.C.,

Doctor(a)
CARDENAS NAVAS DARIO
Apoderado(a) y/o Representante de
MICROSOFT CORPORATION

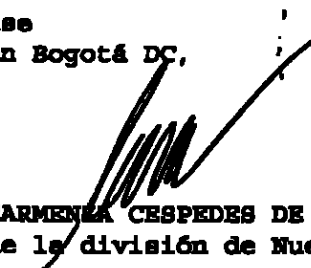
REFERENCIA	Radicación No. 06 10919
	Trámite 2
	Evento 1
	Actuación 416
	Oficio No. 3043
	Folios 1

Teniendo en cuenta que la solicitud de privilegio de patente que se tramita bajo el expediente indicado en la referencia, reúne los requisitos de forma establecidos en los artículos 26 y 27 de la Decisión 486 de la Comisión de la Comunidad Andina, y en las demás disposiciones vigentes sobre la materia, se envía el extracto de la solicitud a la Oficina de Comunicaciones para efecto de su publicación en la Gaceta de Propiedad Industrial.

De acuerdo con lo previsto por el artículo 40 de la Decisión 486/00, la publicación en este caso se hará a partir del día 06 del mes de Agosto de 2007.

Cúmplase
Dado en Bogotá DC,

11 6 MAY 2007


ALIX CARMEN CESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

adpa10