

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

Ref.: Expediente No. 04-106.330
Solicitud de Patente denominada "LA
AUTENTICACIÓN DESAFIO BASADO SIN REQUERIR
CONOCIMIENTO DE DATOS DE LA
AUTENTICACIÓN CONFIDENCIAL".
Titular: Microsoft Corporation.

Darío Cárdenas Navas, identificado como aparece al pie de mi firma, atentamente me dirijo a ese Despacho dando respuesta al Oficio No. 10030 de fecha 28 de Octubre de 2004.

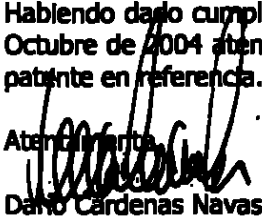
De acuerdo con lo solicitado me permito anexar copia auténtica y debidamente legalizada del documento en donde consta la cesión del derecho de la patente del inventor al solicitante junto con la Traducción Oficial correspondiente.

Igualmente, adjunto a la presente copia de los documentos de prioridad de las siguientes patentes junto con sus correspondientes traducciones:

- Patente de los Estados Unidos No. 10/917.786 de fecha 13 de Agosto de 2003.
- Patente de los Estados Unidos No. 60/515.461 de Fecha 29 de Octubre de 2003.

Habiendo dado cumplimiento a los requerimientos incluidos en el Oficio No. 10030 de fecha 28 de Octubre de 2004 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. LHO

Jag/correspo/Microsoft.patentes.La autenticación desafío basada.doc

UNITED STATES OF AMERICA

The State of



Washington

Secretary of State

APOSTILLE

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States of America

2. This public document has been
signed by:

LAURIE A. HENEGHAN

3. acting in the capacity of:

Notary Public, state of Washington

4. bears the seal/stamp of:

LAURIE A. HENEGHAN

CERTIFIED

5. at: Olympia, Washington

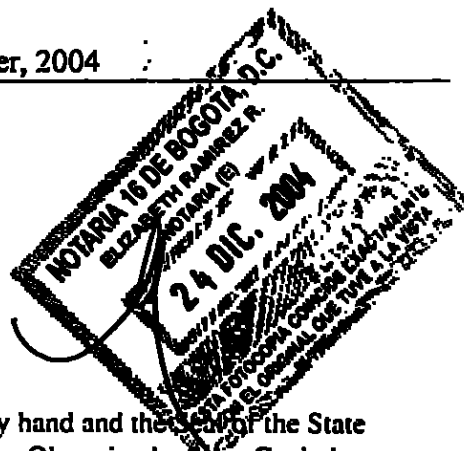
6. the: 8 day of October, 2004

7. by: Sam Reed, Secretary of State

8. No: 200424324

9. Seal/Stamp:

10. Signature:

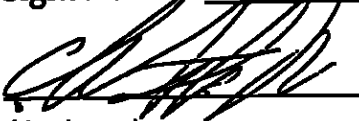


Given under my hand and the Seal of the State
of Washington at Olympia, the State Capital

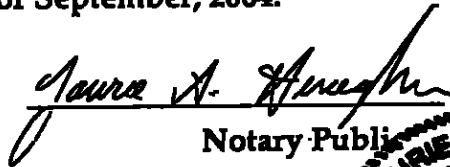
Sam Reed

Sam Reed, Secretary of State

77
72
Signed on the 30 day of September of 2004, by

 (Christopher G. Kaler)
(Assignor)

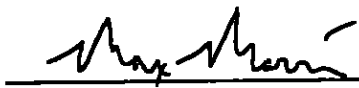
Subscribed and sworn to before me, Laurie A. Heneghan,
a Notary Public, this 30 day of September, 2004.


Notary Public

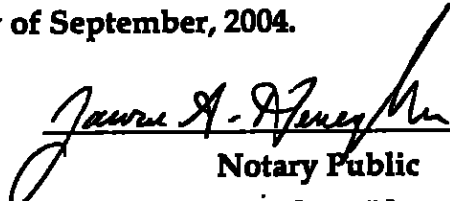
[SEAL]



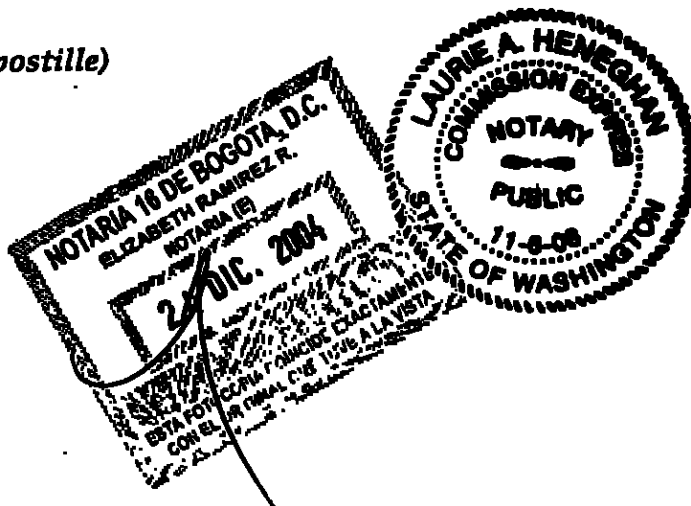
Signed on the 28 day of September of 2004, by

 (Max G. Morris)
(Assignor)

Subscribed and sworn to before me, Laurie A. Heneghan,
a Notary Public, this 28 day of September, 2004.


Notary Public
[SEAL]

(This document must be duly legalized by Apostille)



78
73

TRADUCCIÓN OFICIAL

ESTADOS UNIDOS DE AMERICA

El Estado de Washington

El Sello del Estado de Washington

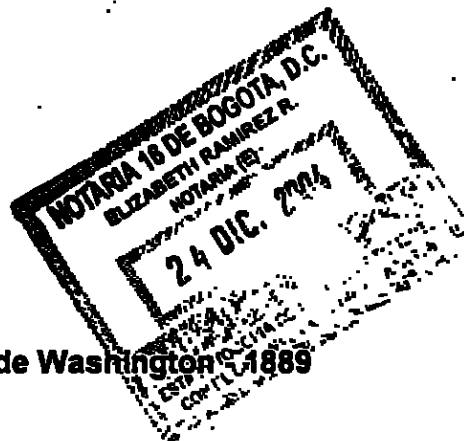
Apostilla

(Convención de La Haya, 5 de octubre de 1961)

1. País: Estados Unidos de América
2. El presente documento público ha sido firmado por: **LAURIE A. HENEGHAN**
3. actuando en calidad de Notario Público del Estado de Washington
4. Lleva el sello / estampilla de: **LAURIE A. HENEGHAN**

CERTIFICADO

5. En: Olympia, Washington
6. El: 8 de Octubre de 2004
7. Por: **Sam Reed, Secretario de Estado**
8. Bajo el número: **200424324**
9. Lleva Sello / Estampilla: El Sello del Estado de Washington
10. Firmado por: **Sam Reed**



Expedido con mi firma y el sello del Estado de Washington, en Olympia, la Capital del Estado.

Firma: Sam Reed, Secretario de Estado

Martha S. Sarmiento S.
Martha S. Sarmiento S.

**Traductora Oficial Juramentada
Resolución No. 835 Minjusticia**

4

MINISTERIO DE
RELACIONES EXTERIORES

285835

Harley S. Guzmán

CUYA FOTOCOPIA SE RECEBE EN EL
DOCUMENTO DE SEMPENA
DE LAS FUNCIONES INDICADAS

ELIZADETH RAMIREZ R.
NOTARIA (E)
24 DIC. 2004
ESTA FOTOCOPIA CONCORDA EXACTAMENTE
CON EL ORIGINAL QUE SE LE A LA VISTA

NO SE ASUME
RESPONSABILIDAD DEL TEXTO

2004 NOV 11 P 1:48

JEFE DE LEGALIZACIONES
BOGOTÁ D.C.

20
74

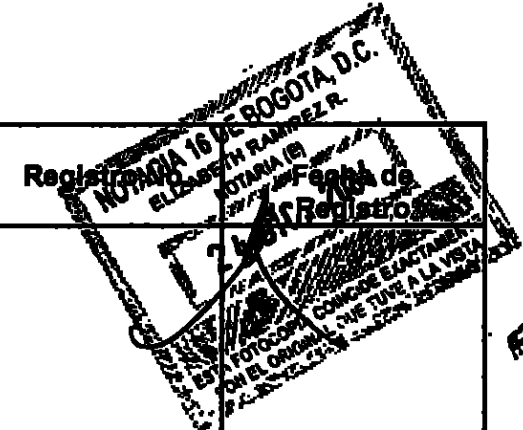
TRADUCCIÓN OFICIAL

**Colombia
307134.25**

TRASPASO DE PATENTE

Entre los suscritos, Christopher G. Kaler y Max G. Morris, ambos ciudadanos de los Estados Unidos de América, con domicilio en One Microsoft Way, Redmond, WA 98052, Estados Unidos de América, y One Microsoft Way, Redmond, WA 98052, Estados Unidos de América, respectivamente, de aquí en adelante los Cedentes, y David Bartley Eppenauer, actuando en calidad de Secretario Asistente de la Corporación Microsoft, una compañía legalmente constituida, que existe y se rige de acuerdo a las leyes del Estado de Washington, Estados Unidos de América, que se encuentra ubicada en One Microsoft Way, Redmond, WA 98052-6399, Estados Unidos de América, de aquí en adelante el Cesionario, en virtud:

- A. Que el Cesionario solicitó registrar ante la Oficina de Patentes de Colombia la siguiente patente:

Título del Invento	
Challenge-Based Authentication Without Requiring Knowledge of Secret Authentication Data Autenticación Desafío-Basado Sin Requerir Conocimiento De Datos De La Autenticación Confidenciales	

- B. Que los Cedentes son los autores del invento objeto de la solicitud de patente arriba mencionada.
- 6

75

C. Que el Cesionario se encuentra interesado en obtener el traspaso del invento
arriba mencionado, y los Cedentes están interesados en traspasarlo al
Cesionario.

Se ha celebrado el siguiente acuerdo:

Primero: Los Cedentes asignan y traspasan al Cesionario todos los derechos
que ellos poseen relacionados con el invento objeto de la solicitud de patente
mencionada en el literal A de este documento.

Segundo: El Cesionario acepta el traspaso arriba mencionado.

Tercero: Este traspaso debe ser vinculante y beneficiar a las partes, a sus
subsidiarios, afiliados, sucesores, cesionarios y concesionarios o personas
autorizadas, si los hay.

Firmado el 30 de Septiembre de 2004 por

Christopher G. Kaler
(Cedente)

Documento firmado y jurado ante mí, Laurie A. Heneghan, Notario Público,
hoy 30 de Septiembre de 2004.



76

Firmado el 28 de Septiembre de 2004, por

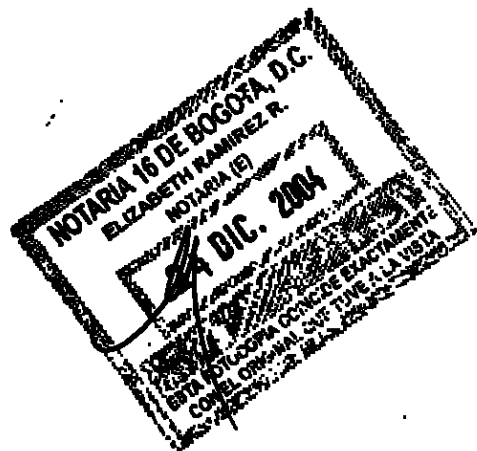
Max G. Morris
(Cesionario)

Documento firmado y jurado ante mí, Laurie A. Heneghan, Notario Público,
hoy 28 de Septiembre de 2004.

(Firmado)
Laurie A. Heneghan
Notario Público

[Sello Notarial]
LAURIE A. HENEGHAN
NOTARIO PÚBLICO
Mi comisión finaliza el
11- 6 - 08
ESTADO DE WASHINGTON

(Este documento se debe legalizar con Apostilla)



Martha S. Sarmiento S.

Martha S. Sarmiento S.
Traductora Oficial Juramentada
Resolución No. 835 Minjusticia

84
77

CONSTANCIA DE TRADUCCIÓN OFICIAL

Yo, Martha Sofía Sarmiento Solano, identificada con Cédula de Ciudadanía No. 41.686.291, de Bogotá, HAGO CONSTAR que el presente documento es la versión en idioma Español del Assignment / Traspaso de Patente firmado por Christopher G. Kaller, Cedente y Max G. Morris, Cesionario.

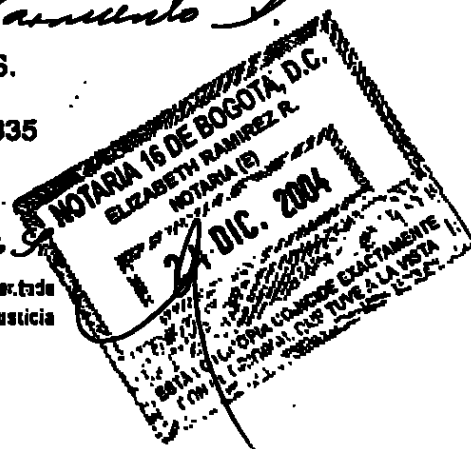
Dicho traspaso fue presentado y firmado ante el Notario Público del Estado de Washington, LAURIE A. HENEGHAN los días 28 y 30 de Septiembre de 2004. También hace parte del documento la Apostilla Número 200424324, con fecha 8 de Octubre de 2004 y firmada por Sam Reed, Secretario de Estado del Estado de Washington.

Martha S. Sarmiento S.

Martha S. Sarmiento S.
Traductora Oficial
Resolución Minjusticia 835

Martha S. Sarmiento S.

Traductora Oficial Juramentada
Resolución No. 835 Minjusticia



78

83
②
78

PA 1227623

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

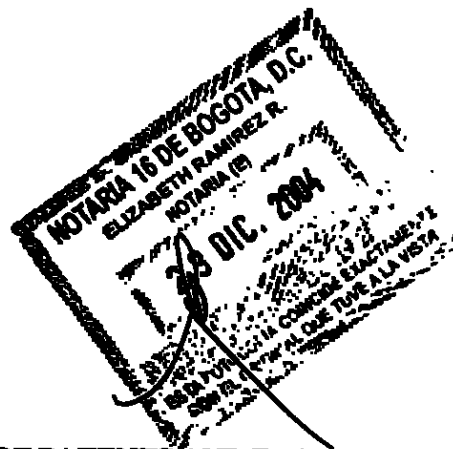
United States Patent and Trademark Office

October 20, 2004

**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: 10/917,786

FILING DATE: August 13, 2004



**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**



P. R. Grant
P. R. GRANT
Certifying Officer

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
13768.485.1Total Pages in this Submission
4**COMMISSIONER FOR PATENTS**P.O. Box 1480
Alexandria, VA 22313-1480

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

CHALLENGE-BASED AUTHENTICATION WITHOUT REQUIRING KNOWLEDGE OF SECRET AUTHENTICATION DATA

and invented by:

Max G. Morris
Christopher G. Kaler

If a CONTINUATION APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-In-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-In-part (CIP) of prior application No.: _____

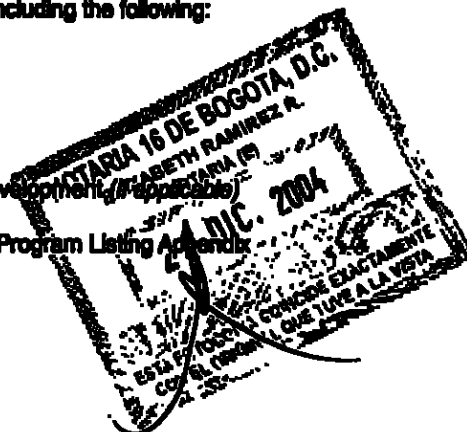
Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-In-part (CIP) of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 35 pages and including the following:
 - a. ☒ Descriptive Title of the Invention
 - b. ☒ Cross References to Related Applications (if applicable)
 - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
 - d. ☐ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix
 - e. ☒ Background of the Invention
 - f. ☒ Brief Summary of the Invention
 - g. ☒ Brief Description of the Drawings (if filed)
 - h. ☒ Detailed Description
 - i. ☒ Claim(s) as Classified Below
 - j. ☒ Abstract of the Disclosure



UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
1376L485.1

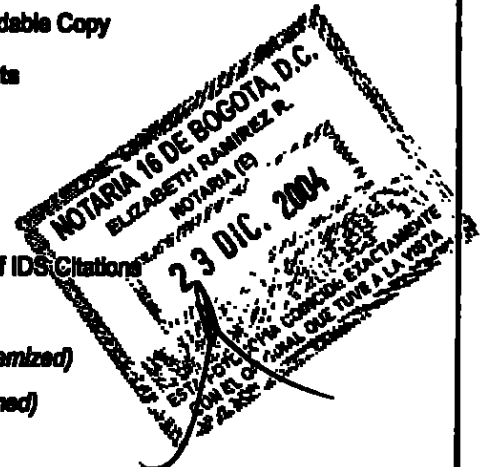
Total Pages in this Submission
4

Application Elements (Continued)

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
- a. ☒ Formal Number of Sheets 4
- b. ☐ Informal Number of Sheets _____
4. ☐ Oath or Declaration
- a. ☐ Newly executed (original or copy) ☐ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)
- c. ☐ With Power of Attorney ☐ Without Power of Attorney
- d. ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. ☐ Application Data Sheet (See 37 CFR 1.76)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)
- a. ☐ Computer Readable Form (CRF)
- b. ☐ Specification Sequence Listing on:
- I. ☐ CD-ROM or CD-R (2 copies); or
- II. ☐ Paper
- c. ☐ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(B) Statement (when there is an assignee)
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☒ Certificate of Mailing
- ☐ First Class ☒ Express Mail (Specify Label No.): EV 510294625 US



UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
13768485.1

Total Pages in this Submission
4

Accompanying Application Parts (Continued)

17. ☒ **Additional Enclosures (please identify below):**

PTO 2038 Credit Card form for \$1,130.00

The present application claims priority to the United States provisional patent application serial number 60/515,461 filed October 29, 2003, which provisional application is incorporated herein by reference in its entirety.

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. ☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.



82

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity) <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>						Docket No. 13768485.1
						Total Pages in this Submission 4

Fee Calculation and Transmittal

CLAIMS AS FILED						
For	#Filed	#Allowed	#Extra	Rate		Fee
Total Claims	40	- 20 =	20	x	\$18.00	\$360.00
Indep. Claims	3	- 3 =	0	x	\$88.00	\$0.00
Multiple Dependent Claims (check if applicable) ☐						\$0.00
BASIC FEE						\$770.00
OTHER FEE (specify purpose)						\$0.00
TOTAL FILING FEE						\$1,130.00

☐ A check in the amount of _____ to cover the filing fee is enclosed.

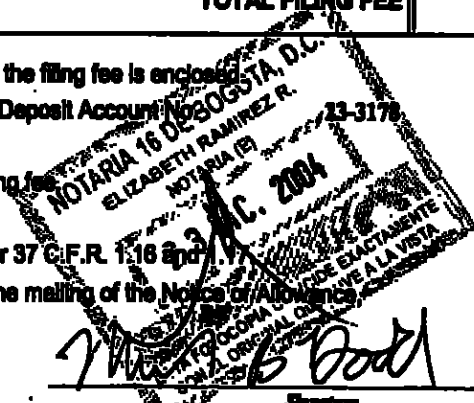
☒ The Director is hereby authorized to charge and credit Deposit Account No. 8060551A, D.C. as described below.

☐ Charge the amount of _____ as filing fee.

☒ Credit any overpayment.

☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.

☒ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance pursuant to 37 C.F.R. 1.311(b).

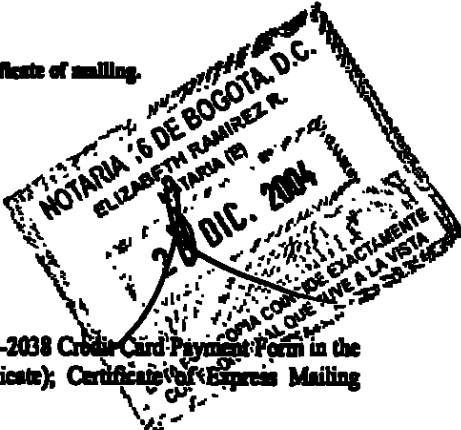


Signature

Dated: August 13, 2004
Customer Number: 022913

Michael B. Dedd
Reg. No.: 46,437
Attorney for Applicant
Customer No.: 022913

cc:

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): Max G. Morris et al.			Docket No. 13768.485.1	
Application No. Unknown	Filing Date August 13, 2004	Examiner Unknown	Customer No. 022913	Group Art Unit Unknown
Invention: CHALLENGE-BASED AUTHENTICATION WITHOUT REQUIRING KNOWLEDGE OF SECRET AUTHENTICATION DATA				
I hereby certify that the following correspondence: (see below) (Identify type of correspondence) is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on <u>August 13, 2004</u> (Date) _____ (Typed or Printed Name of Person Mailing Correspondence) _____ (Signature of Person Mailing Correspondence) _____ EV 510294625 US ("Express Mail" Mailing Label Number) Note: Each paper must have its own certificate of mailing.  Patent application (35 pgs.); 4 sheets of formal drawings; PTO-2038 Credit Card Payment Form in the amount of \$1,130.00; Transmittal letter (4 pgs. in duplicate); Certificate of Express Mailing (EV510294625US), Postcard				

POB/REV03

84

UNITED STATES PATENT APPLICATION

of

Max G. Morris

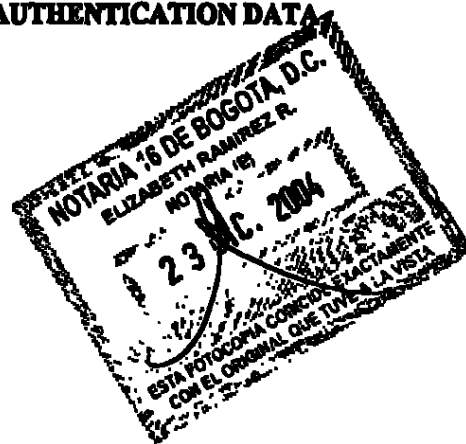
and

Christopher G. Kaler

for

**CHALLENGE-BASED AUTHENTICATION WITHOUT REQUIRING
KNOWLEDGE OF SECRET AUTHENTICATION DATA**

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1800 MAGNOLIA TOWER
80 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



86

85

**CHALLENGE-BASED AUTHENTICATION WITHOUT REQUIRING
KNOWLEDGE OF SECRET AUTHENTICATION DATA**

BACKGROUND OF THE INVENTION

1. Cross-Reference to Related Applications

[0001] The present application claims priority to United States provisional patent application serial number 60/515,461 filed October 29, 2003, which provisional application is incorporated herein by reference in its entirety.

2. The Field of the Invention

[0002] The present invention relates generally to authentication. More specifically, the present invention relates to challenge-based authentication mechanisms that do not require knowledge of secret authentication data.

3. Background and Relevant Art

[0003] Computing technology has transformed the way we work and play. Computing systems and devices (hereinafter also referred to simply as "computing entities") now take a wide variety of forms including desktop computers, laptop computers, tablet PCs, Personal Digital Assistants (PDAs), household devices and the like. In its most basic form, a computing system includes system memory and one or more processors. Software in the system memory may be executed by the processor to direct the other hardware of the computing system to perform desired functions. In other computing entities, logic is implemented using hardware, or a combination of software and hardware.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1800 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

86

[0004] Networking technologies enable computing entities to communicate even over vast distances, thereby expanding on computer functionality. For example, networking technologies enable such applications as e-mail, web browsing, file transfer, instant messaging, electronic whiteboarding, network collaboration, and the like. Accordingly, computer networks enable widespread communication and information access.

[0005] Unfortunately, computer networks also can potentially open up connected computing entities to security breaches. One type of security breach is for one computing system or user to make false claims about who they are to thereby access resources they should not have access to. In order to guard against this, an authenticatee computing entity (i.e., a computing entity that requires authentication) will often require an authenticator computing entity (i.e., a computing entity that must authenticate) to authenticate itself. The authenticatee computing entity may then make a more informed decision regarding how to interact with the authenticator computing entity.

[0006] One particularly useful form of authentication is often referred to as challenge/response authentication. In this form of authentication, when an authenticator computing entity (hereinafter also referred to as the "authenticator") is to authenticate to an authenticatee computing entity (hereinafter also referred to as the "authenticatee"), the authenticatee sends a challenge to the authenticator. The authenticator then generates a response (also referred to herein as an "answer") to the challenge typically by applying a one-way hash algorithm to the challenge using secret data available to the authenticatee and authenticator. This secret data may be, for example, a password corresponding to the authenticator. The authenticator likewise also generates the same answer using the same hashing algorithm and using the same secret data. The authenticator then provides its answer to the authenticatee. The authenticatee then compares the answer that the

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1600 EAGLE OAK TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

87

authenticator generated with the answer that the authenticatee generated. If the answers match, then the authentication is successful. The challenge/response authentication is advantageous in that the secret data itself is not transmitted, and thus may not be intercepted.

[0007] However, this challenge/response authentication requires that the authenticator and authenticatee computing entities have access to the secret data used for authentication, and that the authenticator and authenticatee computing entities generate the answer. In some environments this may not be desirable. For example, many computing entities have limited processing power. The generation of an answer may degrade the performance of the computing entity by diverting processing power from other processes. Furthermore, the computing entities may not be themselves secure. Accordingly, an unauthorized entity might conceivably access the secret data and use that data to falsely authenticate.

[0008] Accordingly, what would be advantageous is a challenge/response authentication mechanism that does not require the authenticator and authenticatee computing entities to generate an answer or contain the secret data itself.

WOLKMAN, N.Y. BROOKLYN
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



23
88

BRIEF SUMMARY OF THE INVENTION

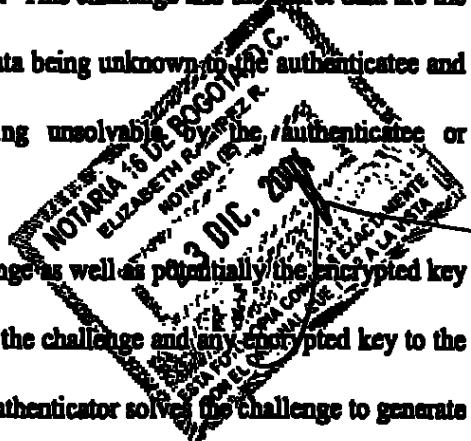
[0009] The foregoing problems with the prior state of the art are overcome by the principles of the present invention, which relate to a challenge based authentication mechanism that does not require that the authenticating computing entities be aware of the secret data used for the initial authentication.

[0010] The environment includes four computing entities, an authenticatee computing entity, a supplemental authenticatee computing entity, an authenticator computing entity, and a supplemental authenticator computing entity. The authenticator computing entity is to authenticate to the authenticatee computing entity, but does not have direct access to the secret data needed to authenticate.

[0011] First, the authenticatee acquires a challenge from the supplemental authenticatee. This challenge may be solved by the supplemental authenticator, but not by the authenticatee and authenticator. The authenticatee may also pass a secret key to the supplemental authenticatee. The supplemental authenticatee encrypts the secret key using secret data known to the supplemental authenticatee and supplemental authenticator, but not to the authenticatee and authenticator themselves. This challenge and the secret data are the basis for the authentication, despite the secret data being unknown to the authenticatee and authenticator, and despite the challenge being unsolvable by the authenticatee or authenticator directly.

[0012] The authenticatee provides the challenge as well as potentially the encrypted key to the authenticator. The authenticator provides the challenge and any encrypted key to the supplemental authenticator. The supplemental authenticator solves the challenge to generate an answer, and also decrypts the encrypted key. The supplemental authenticator provides the answer and the decrypted key to the authenticator. At this stage, the decrypted key is

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



23

89

known to the authenticator and authenticator and may be used to secure future communications between the authenticator and authenticator.

[0013] The authenticator then sends the answer to the authenticator. The authenticator then uses this answer to authenticate the authenticator either by validating the answer directly, or by causing the supplemental authenticator to validate the answer.

[0014] Additional features and advantages of the invention will be set forth in the description that follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

WONGSUNNYBROKER
A PROFESSIONAL CORPORATION
ATTORNEY AT LAW
1000 EAGLE GATE TOWER
80 EAST SOUTH TEMPL
SALT LAKE CITY, UTAH 84111



25
90

BRIEF DESCRIPTION OF THE DRAWINGS

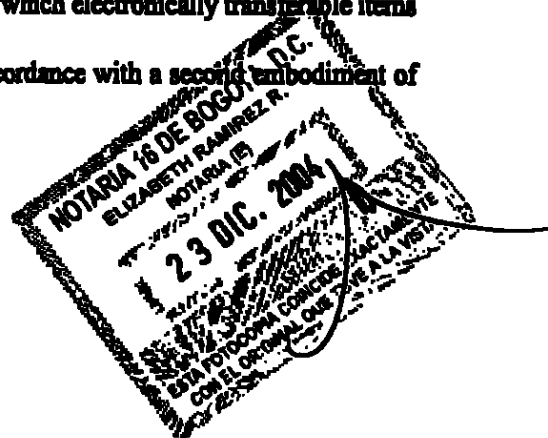
[0015] In order to describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0016] Figure 1 is a diagram of a message exchange between an authenticator, supplemental authenticator, authenticator, and supplemental authenticator computing entities in accordance with the principles of the present invention;

[0017] Figure 2 schematically illustrates a data structure in the form of a Simple Object Access Protocol (SOAP) envelope that includes SOAP headers in the form of billing and signing headers;

[0018] Figure 3 illustrates a message exchange in which electronically transferable items are transferred between two computing entities in accordance with a first embodiment of the present invention; and

[0019] Figure 4 illustrates a message exchange in which electronically transferable items are transferred between two computing entities in accordance with a second embodiment of the present invention.



WORKMAN NYDEGGER
ATTORNEYS AT LAW
1600 EAGLE CLAY TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

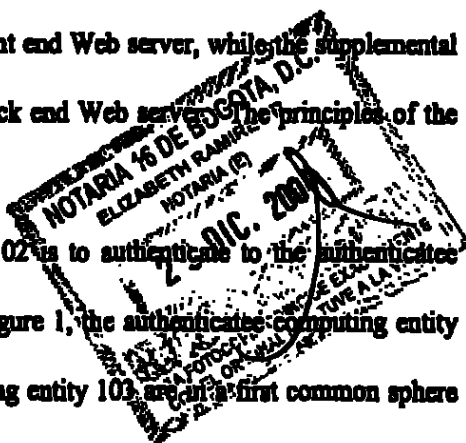
DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] The principles of the present invention provide a challenge based authentication mechanism that does not require that the authenticating computing entities be aware of the secret data used for the initial authentication, and do not require the authenticating computing entities themselves generate an answer to a challenge.

[0021] Figure 1 illustrates an environment 100 that includes four computing entities 101 through 104. Specifically, the four computing entities include what will be referred to as an authenticatee computing entity 101, an authenticator computing entity 102, a supplemental authenticatee computing entity 103, and a supplemental authenticator computing entity 104. In this description and in the claims, a "computing entity" is any device or system that may retain data in memory and/or storage, and is capable of electronic communication.

[0022] For example, each of the computing entities 101 through 104 may have access to its own internal data, and may communicate with one or more of the other computing entities. Such communication need not be across a network. For example, any two or more of the computing entities 101 through 104 may be within the same electronic device or computing system. As an example, the supplemental authenticator computing entity 104 may be a SIM card, while the authenticator computing entity 102 is a mobile telephone. The authenticatee computing entity 101 may be a front end Web server, while the supplemental authenticatee computing entity 103 may be a back end Web server. The principles of the present invention are not limited to this, however.

[0023] The authenticator computing entity 102 is to authenticate to the authenticatee computing entity 101. In the embodiment of Figure 1, the authenticatee computing entity 101 and the supplemental authenticatee computing entity 103 are in a first common sphere of trust. The authenticator computing entity 102 and the supplemental authenticator



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

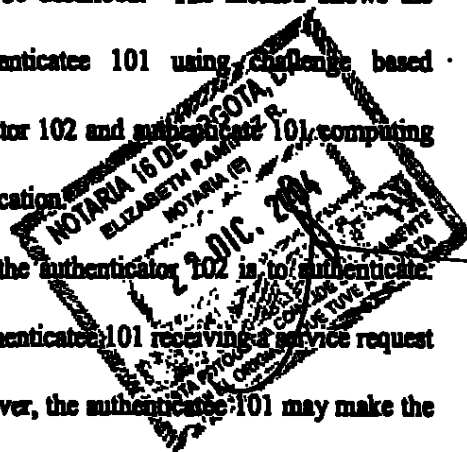
92

computing entity 104 are also in a second common sphere of trust. The supplemental authenticator computing entity 103 and the supplemental authenticator computing entity 104 are in a third common sphere of trust. A "sphere of trust" as used in this description and in the claims is defined as a collection of two or more computing entities in which each computing entity in the sphere of trust has received some assurance that the other computing entities are who they purport to be, and that information from the other computing entities is at least somewhat reliable.

[0024] In this description and in the claims, the authenticator computing entity 101, the authenticator computing entity 102, the supplemental authenticator computing entity 103, and the supplemental authenticator computing entity 104, may also be referred to as simply the "authenticator 101", the "authenticator 102", the "supplemental authenticator 103", and the "supplemental authenticator 104", respectively.

[0025] Figure 1 also shows an example message flow that results in authentication consistent with the principles of the present invention. The sequential order of a message transfer is represented sequentially by the number in the head of the arrow that represents the message transfer. Using this message flow, an authentication method in accordance with the principles of the present invention will now be described. The method allows the authenticator 102 to authenticate to the authenticator 101 using challenge based authentication and without requiring the authenticator 102 and authenticator 101 computing entities be aware of secret data used for the authentication.

[0026] The authenticator 101 determines that the authenticator 102 is to be authenticated. This may be accomplished by, for example, the authenticator 101 receiving a service request (see arrow 111) from the authenticator 102. However, the authenticator 101 may make the determination that the authenticator 102 is to be authenticated in some other manner that



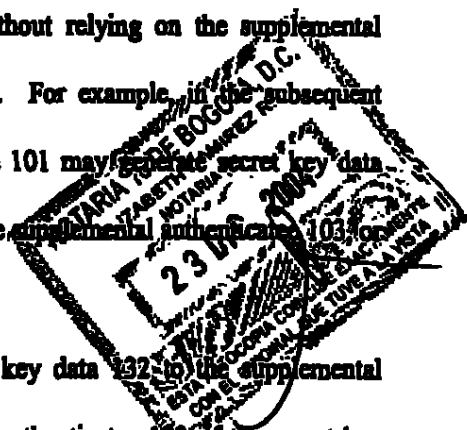
does not rely on any service request from the authenticator 102. Accordingly, the service request represented by arrow 111 is not essential.

[0027] The authenticatee 101 then acquires a challenge 131 from the supplemental authenticatee 103. This may be accomplished in any manner. However, in Figure 1, this is illustrated as being accomplished with two message transfers represented by arrows 112 and 113. Specifically, the authenticatee 101 provides a challenge request represented by arrow 112 to the supplemental authenticatee 103. The supplemental authenticatee 103 may then generate a challenge 131 in response to the challenge request, and then provides the challenge 131 to the authenticatee 101 in response to the request as represented by arrow 113. However, there are a number of alternative ways that the authenticatee 101 may acquire the challenge 131. The challenge 131 may have been provided by the supplemental authenticatee 103 without a challenge request such as, for example, when the authenticatee 101 registers with the supplemental authenticatee 103, or perhaps at predetermined times or time intervals.

[0028] In one embodiment called herein the "subsequent private communications embodiment", additional acts may be undertaken such that the authenticatee 101 and authenticator 102 may subsequently communicate without relying on the supplemental authenticatee 103 and supplemental authenticator 104. For example, in the subsequent private communications embodiment, the authenticatee 101 may generate secret key data 132 that is likely not known to the authenticator 102, the supplemental authenticatee 103, or the supplemental authenticator 104.

[0029] The authenticatee 101 provides the secret key data 132 to the supplemental authenticatee 103 thereby informing the supplemental authenticatee 103 of the secret key

WORMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



22

99

94

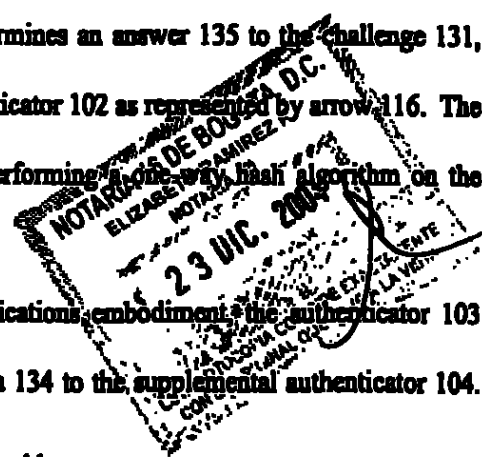
data 132. The secret key data 132 may, for example, have been provided in the same message as the challenge request represented by arrow 112.

[0030] The supplemental authenticator 103 then may encrypt the secret key data 132 using secret data 133 known to the supplemental authenticator 103 and the supplemental authenticator 104 computing entities, but not known to the authenticator 101 and the authenticator 102. The supplemental authenticator 103 then may provide the encrypted secret key data 134 to the authenticator 101. This encrypted secret key data 134 may be provided at the same time and/or in the same message that the supplemental authenticator 103 used to transfer the challenge 131 as represented by arrow 113.

[0031] The authenticator 101 then provides the challenge 131 to the authenticator 102 as represented by arrow 114. At the same time and/or in the same message, the authenticator 101 may also provide the encrypted secret key data 134 to the authenticator 102 as represented by arrow 114.

[0032] The authenticator 102 then acquires an answer to the challenge 131 from the supplemental authenticator computing entity. This may be accomplished in any manner. However, in Figure 1, this is illustrated as being accomplished with two message transfers represented by arrows 115 and 116. Specifically, the authenticator 102 provides the challenge 131 to the supplemental authenticator 104 as represented by arrow 115. The supplemental authenticator 103 may then determine an answer 135 to the challenge 131, and then provides the answer 135 to the authenticator 102 as represented by arrow 116. The answer may be generated by, for example, performing a one-way hash algorithm on the challenge 131 using the secret data 133.

[0033] In the subsequent private communications embodiment, the authenticator 103 may also provide the encrypted secret key data 134 to the supplemental authenticator 104.



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1885 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[Handwritten signature]

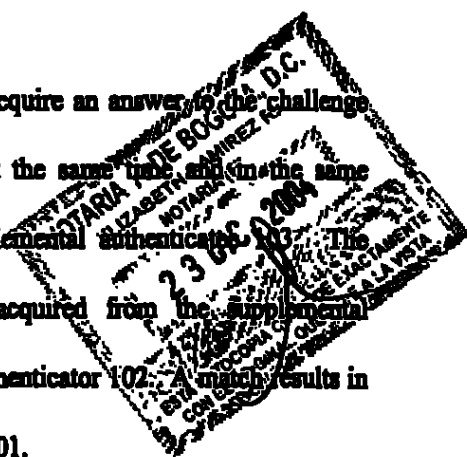
95

This may be accomplished by including the encrypted secret key data 134 in the same message as was used to transmit the challenge to the supplemental authenticator 134 as represented by arrow 115.

[0034] The supplemental authenticator 104 may then decrypt the secret key data 134 using the secret data 133 known to the supplemental authenticator 103 and the supplemental authenticator 104, thereby informing the supplemental authenticator 104 of the secret key data 132. The supplemental authenticator 104 then provides the secret key data 132 to the authenticator 102 thereby informing the authenticator 102 the secret key data 132. The supplemental authenticator 104 may provide the secret key data 132 back to the authenticator 102 potentially in the same message that was used to transfer the answer 135 to the authenticator 102. At this stage, both the authenticator 101 and authenticator 102 have access to secret key data 132. This secret key data 132 may thus be used to authenticate each other in subsequent communications independent of the supplemental authenticator 103 and supplemental authenticator 104.

[0035] The authenticator 102 provides the answer 135 to the authenticator 101 as represented by the arrow 117. The authenticator 101 may then use the answer 135 to authenticate the authenticator 102. There are a number of different ways that the authenticator 101 may do this.

[0036] In one example, the authenticator 101 may acquire an answer to the challenge from the supplemental authenticator 103, potentially at the same time and in the same manner as the challenge was acquired from the supplemental authenticator 103. The authenticator 101 may then match the answer as acquired from the supplemental authenticator 103 with the answer as provided by the authenticator 102. A match results in the authenticator 102 authenticating to the authenticator 101.



WORKMAN NYDEBOER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

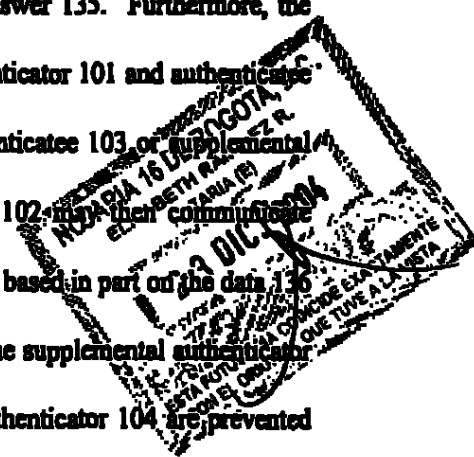
Handwritten mark resembling a stylized '2' or '7'.

126
96

[0037] Alternatively, the authenticatee 101 could delegate this comparison to the supplemental authenticatee 103 by providing the answer 135 as provided by the authenticator 102 to the supplemental authenticatee 103. The supplemental authenticatee 103 may then match the answer as provided by the authenticatee 101 with the answer that it internally generated. If a match is found, the supplemental authenticatee 103 may indicate to the authenticatee 101 that authentication is successful.

[0038] Accordingly, at this stage, the authenticator 102 has authenticated to the authenticatee 101, and the service request may be honored if appropriate. The authentication is challenge-based, and does not require the authenticatee 101 or authenticator 102 have access to the secret data 133 used to generate an answer to the challenge. Furthermore, in the subsequent private communications embodiment, the authenticator 102 and authenticatee 101 may authenticate in subsequent communications using the secret key data 132, rather than repeating the process described above.

[0039] Rather than simply securing subsequent communication based on the secret key data 132 alone, the subsequent communications may be secured using a digest of the secret key data 132 amongst one or more other items. The digest may then be used to secure subsequent communications between the authenticatee 101 and authenticator 102. The digest may also be based on the challenge 131 and/or the answer 135. Furthermore, the digest may include data 136 communicated between the authenticator 101 and authenticatee 102 that is not also communicated to the supplemental authenticatee 103 or supplemental authenticator 104. The authenticatee 101 and authenticator 102 may then communicate using the digest to secure communications. When the digest is based in part on the data 136 that is not known to the supplemental authenticatee 103 and the supplemental authenticator 104, the supplemental authenticatee 103 and supplemental authenticator 104 are prevented



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

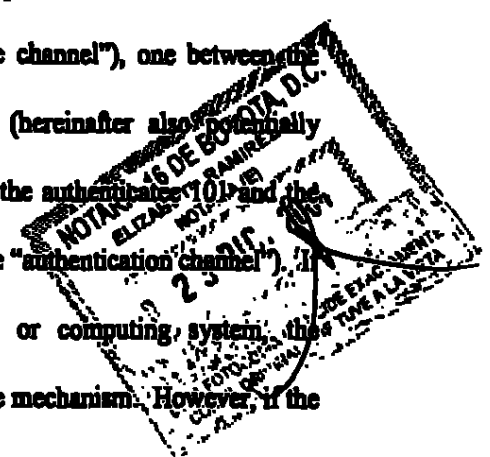
126

from easily eavesdropping or spoofing on subsequent communications between the authenticator 101 and authenticatee 102.

[0040] In one embodiment, the authenticator 102 also generates secret key data 137, which is provided to the supplemental authenticator 104. The supplemental authenticator 104 encrypts the secret key data 137, and passes the encrypted secret key data to the authenticator 102. The authenticator 102 then passes the encrypted secret key data to the authenticatee 101, which uses the supplemental authenticatee 103 to decrypt the secret key 137 using the secret data 131. The digest may then also be based upon this secret key 137.

[0041] Accordingly, a challenge-based authentication mechanism has been described in which the direct parties to the authentication (i.e., the authenticator and authenticatee computing entities) need not calculate an answer to a challenge, nor have knowledge of secret data used in the initial authentication. Furthermore, the authenticator and authenticatee computing entity may subsequently authenticate and communicate independent of the supplemental authenticator and supplemental authenticatee computing entities.

[0042] In the embodiment illustrated in Figure 1, there are several communication channels, one between the authenticatee 101 and the supplemental authenticatee 103 (hereinafter also potentially referred to as "the authenticatee channel"), one between the authenticator 102 and the supplemental authenticator 104 (hereinafter also potentially referred to as the "authenticator channel"), and one between the authenticator 102 and the authenticatee 101 (hereinafter also potentially referred to as the "authentication channel"). If the two computing entities are within the same device or computing system, then the corresponding channel may be a function call or local message mechanism. However, if the



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[Handwritten signature]

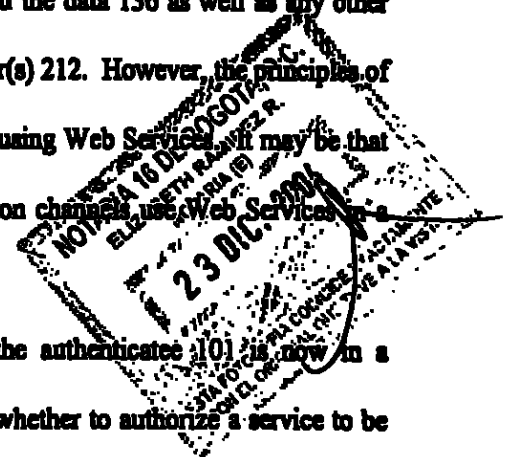
two computing entities are remotely located, the corresponding channel may use a networking protocol.

[0043] For example, if the two computing entities are located across different transport-level domains, a transport-independent network protocol may be used to communicate. One such transport-independent network protocol is known in the art as "Web Services" which uses Simple Object Access Protocol (SOAP) envelopes to convey information in a transport-independent manner. Web Services may also employ SOAP tunneling to transport across networks that do not directly support SOAP.

[0044] According to one aspect of the invention, a modification to conventional Web Services may be employed to convey information important to authentication. For example, a SOAP header may include a signing SOAP header as described in the United States provisional application 60/515,461 incorporated by reference above. Figure 2 schematically illustrates a structure of such a SOAP envelope suitable for performing billing and signing in the context of Web Services. The SOAP envelope 200 includes SOAP headers 201 and a SOAP body 202. The SOAP headers include billing header(s) 211, signing header(s) 212, amongst potentially other headers 213. The signing headers 212 may include the information for authentication. For example, the challenge 131, the secret key 132, the encrypted secret keys 134 and 137, the answer 135, and the data 136 as well as any other useful information may be included in the signing header(s) 212. However, the principles of the present invention are not limited to communication using Web Services. It may be that none of the authenticator, authenticator, or authentication channels use Web Services as a particular embodiment.

[0045] Once authentication has been completed, the authenticator 101 is now in a position to make a more intelligent decision regarding whether to authorize a service to be

WORKMAN NYDEGGER
ATTORNEYS AT LAW
1000 EAST GATE TOWER
60 EAST SOUTH TEMPLER
SALT LAKE CITY, UTAH 84111



99

provided to the authenticator 102. Since the process has at this stage progressed beyond authentication to authorization, computing entities 101 through 104 will each in the subsequent description of the subsequent drawings be referred to simply as a "computing entity".

[0046] In order to authorize a requested service, the computing entity 101 may as a condition for such authorization require the payment or transfer of electronically transferable items from the computing entity 102. In this description and in the claims, an "electronically transferable item" is any item, whether physical or electronic, whose ownership may be transferred from one entity to another by sending an electronic message. The electronic message need not be purely electronic during the transfer, but may undertake other forms such as optical forms during the transfer. Such transferable items may include money. However, the transferable items may also include any other item that is electronically transferable. For example, the items may be frequent flier miles, movie or opera ticket credits, train tickets, class registration authority, and so forth. Likewise, in order to perform the requested service, the computing entity 101 may transfer electronically transferable items to the computing entity 102.

[0047] Figure 3 illustrates the environment of Figure 1 in which there are four computing entities 301 through 304. The computing entities 301 through 304 may be the same as described above for computing entities 101 through 104, although this is not required. Computing entities 301 and 303 are in one sphere of trust represented by the area within the dashed lines. Computing entities 302 and 304 are in another sphere of trust represented by the area within the dotted lines. Computing entities 303 and 304 are within yet another sphere of trust as represented the area within the intermittent dotted/dashed lines.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

NOTARIO PUBLICO
NOTARIA DE BUENOS AIRES
23/11/2004

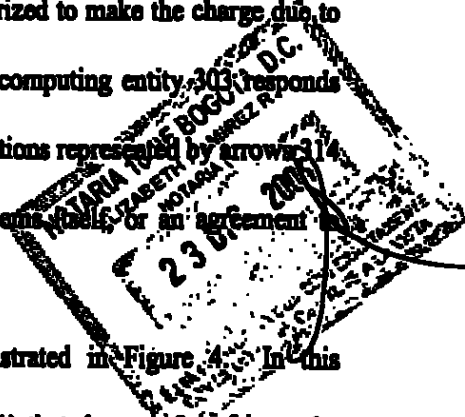
31

[0048] Figure 3 also shows a message flow showing a way of transferring electronically transferable items between computing entities 301 and 302. Computing entity 304 has authorization information 321 relevant to whether or not computing entity 302 may transfer particular items to computing entity 301. For example, if the computing entity 302 were a SIM card, the items to be transferred may be, for example, money.

[0049] The message flow shows how items could be authorized to be transferred and then actually transferred from computing entity 302 to computing entity 301. In order to authorize transfer, the computing entity 301 may inquire (see arrow 311) of computing entity 303 as to whether or not computing entity 302 has authorization to transfer the items. If the computing entity 303 does not already know, the computing entity 303 will make the inquiry (see arrow 312) to computing entity 304 as to whether or not computing entity 302 is authorized to make the transfer. If the computing entity 304 does not already know, the computing entity 304 will make inquiry (see arrow 313) to computing entity 302 about whether to make the transfer. The computing entity 302 may respond (see arrow 314) in the affirmative. Upon receiving this message, or if the computing entity 304 had been pre-authorized to make the charge due to prior communication with computing entity 302, then the computing entity 304 responds (see arrow 315) in the affirmative. Upon receiving this message, or if the computing entity 303 had been pre-authorized to make the charge due to prior communication with computing entity 304, then the computing entity 303 responds (see arrow 316) in the affirmative. The affirmative confirmations represented by arrows 314 through 316 may also include electronic transfer of the items itself, or an agreement to enforce transfer at a later time.

[0050] An alternative embodiment of transfer is illustrated in Figure 4. In this embodiment, computing entity 402 requests (see arrow 411) that the transfer of items be

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



21

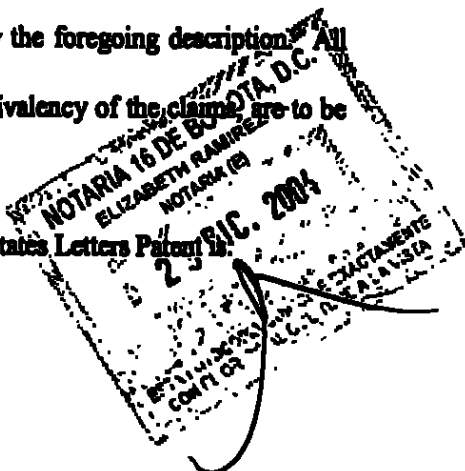
726
101

made. Computing entity 404 responds (see arrow 412) with an approval to transfer the items (see arrow 412) and then debits an account by the items to be transferred. The approval to transfer may be encrypted using secret data 433 known to the computing entities 403 and 404, but not to the computing entities 401 and 402. Computing entity 402 then provides the encrypted approval (see arrow 413) to computing entity 401, which then provides the encrypted approval (see arrow 414) to computing entity 403. The computing entity decrypts the approval using secret data 433 and then credits the account of computing entity 401 or the user of computing entity 401 in the amount of the items being transferred. Upon a subsequent reconciliation or in real-time, computing entity 403 may acquire a credit for the items transferred from computing entity 404.

[0051] . Thus, transfer of the electronically transferable items is made from the computing entity 402 (or its user) to the computing entity 401 (or its user). Transfer in the other direction from computing entity 401 to computing entity 402 may be accomplished in the same manner as described above only in the symmetrically opposite direction.

[0052] The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

[0053] What is claimed and desired secured by United States Letters Patent is,



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1600 MADISON GATE TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

28

1. In an environment that includes an authenticatee computing entity, a supplemental authenticatee computing entity, an authenticator computing entity, and a supplemental authenticator computing entity, a method for the authenticator computing entity to authenticate to the authenticatee computing entity using challenge based authentication and without requiring the authenticatee and authenticator computing entities be aware of secret data used for the authentication, the method comprising the following:

an act of the authenticatee computing entity acquiring a challenge from the supplemental authenticatee computing entity;

an act of the authenticatee computing entity providing the challenge to the authenticator computing entity;

an act of the authenticator computing entity acquiring an answer to the challenge from the supplemental authenticator computing entity;

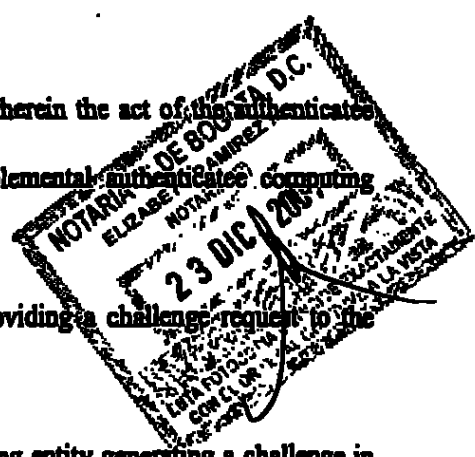
an act of the authenticator computing entity providing the answer to the authenticatee computing entity; and

an act of the authenticatee computing entity using the answer to authenticate the authenticator computing entity.

2. A method in accordance with Claim 1, wherein the act of the authenticatee computing entity acquiring a challenge from the supplemental authenticatee computing entity comprises the following:

an act of the authenticatee computing entity providing a challenge request to the supplemental authenticatee computing entity;

an act of the supplemental authenticatee computing entity generating a challenge in response to the challenge request; and



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1800 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

792
103

an act of the supplemental authenticator computing entity providing the challenge to the authenticator computing entity in response to the request.

3. A method in accordance with Claim 2, wherein the act of the authenticator computing entity acquiring an answer to the challenge from the supplemental authenticator computing entity comprises the following:

an act of the authenticator computing entity providing the challenge to the supplemental authenticator computing entity; and

an act of the supplemental authenticator computing entity determining an answer to the challenge; and

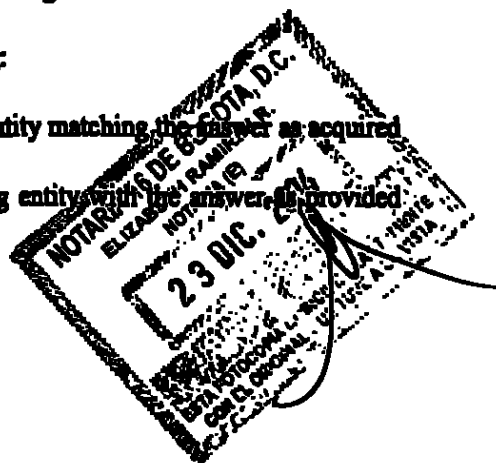
an act of the supplemental authenticator computing entity providing the answer to the authenticator computing entity.

4. A method in accordance with Claim 1, further comprising the following:

an act of the authenticator computing entity acquiring an answer to the challenge from the supplemental authenticator computing entity, wherein

the act of the authenticator computing entity using the answer to authenticate the authenticator computing entity comprises the following:

an act of the authenticator computing entity matching the answer as acquired from the supplemental authenticator computing entity with the answer as provided by the authenticator computing entity.



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPL
SALT LAKE CITY, UTAH 84111

25

700
104

5. A method in accordance with Claim 1, wherein the act of the authenticatee computing entity using the answer to authenticate the authenticator computing entity comprises the following:

an act of the authenticatee computing entity providing the answer to the supplemental authenticatee computing entity; and

an act of the supplemental authenticatee computing entity providing to the authenticatee computing entity an indication that the answer provided by the authenticator computing entity is a proper answer for the challenge acquired from the supplemental authenticatee computing entity.

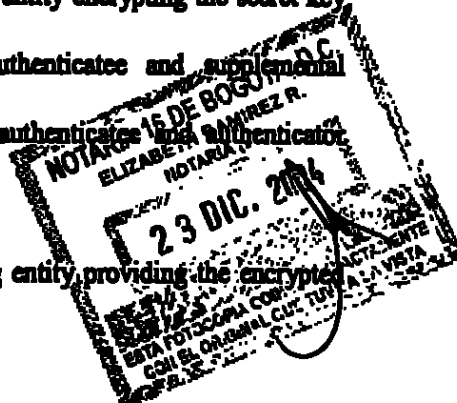
6. A method in accordance with Claim 1, further comprising:

an act of the authenticatee computing entity generating secret key data that is not known to the supplemental authenticatee, authenticator or supplemental authenticator computing entities;

an act of the authenticatee computing entity providing the secret key data to the supplemental authenticatee computing entity thereby informing the supplemental authenticatee computing entity of the secret key data;

an act of the supplemental authenticatee computing entity encrypting the secret key data using secret data known to the supplemental authenticatee and supplemental authenticator computing entities, but not known to the authenticatee and authenticator computing entities;

an act of the supplemental authenticatee computing entity providing the encrypted secret key data to the authenticatee computing entity;



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1600 EAST GATE TOWER
SUITE 1000
SALT LAKE CITY, UTAH 84111

105

an act of the authenticatee computing entity providing the encrypted secret key data to the authenticator computing entity;

an act of the authenticator computing entity providing the encrypted secret key data to the supplemental authenticator computing entity;

an act of the supplemental authenticator computing entity decrypting the secret key data using the secret data known to the supplemental authenticatee and supplemental authenticator computing entities thereby informing the supplemental authenticator computing entity of the secret key data;

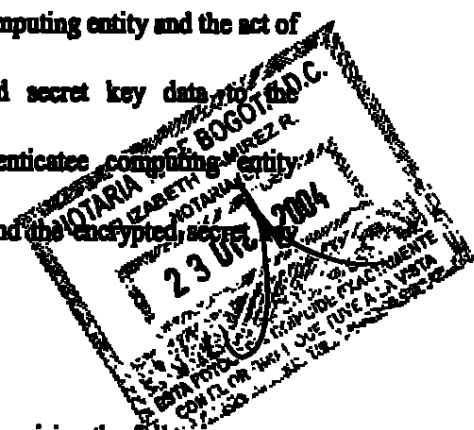
an act of the supplemental authenticator computing entity providing the secret key data to the authenticator computing entity thereby informing the authenticator computing entity of the secret key data.

7. A method in accordance with Claim 6, further comprising the following:

an act of the authenticatee and authenticator computing entities communicating using messages that are at least partially secured using the secret key data.

8. A method in accordance with Claim 6, wherein the act of the authenticatee

computing entity providing the challenge to the authenticator computing entity and the act of the authenticatee computing entity providing the encrypted secret key data to the authenticator computing entity are performed by the authenticatee computing entity providing a single message that includes both the challenge and the encrypted secret key data to the authenticator computing entity.



9. A method in accordance with Claim 6, further comprising the following:

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
80 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

37

106

an act of the authenticatee computing entity generating a digest of the secret key data combined with one or more other data items;

an act of the authenticator computing entity also generating the digest of the secret key data combined with the one or more other data items; and

an act of the authenticatee and authenticator computing entities communicating using messages that are at least partially secured using the digest.

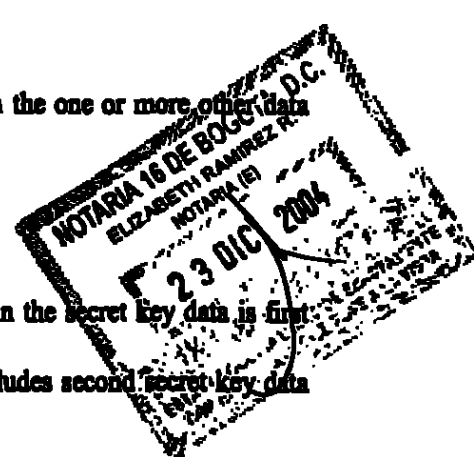
10. A method in accordance with Claim 9, wherein the one or more other data items includes the challenge.

11. A method in accordance with Claim 10, wherein the one or more other data items includes the answer.

12. A method in accordance with Claim 11, wherein the secret key data is first secret key data, wherein the one or more other data items includes second secret key data known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.

13. A method in accordance with Claim 9, wherein the one or more other data items includes the answer.

14. A method in accordance with Claim 13, wherein the secret key data is first secret key data, wherein the one or more other data items includes second secret key data



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAST GATE TOWER
SALT LAKE CITY, UTAH 84111

48

107

known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.

15. A method in accordance with Claim 9, wherein the secret key data is first secret key data, wherein the one or more other data items includes second secret key data known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.

16. A method in accordance with Claim 6, wherein the secret key data is first secret key data, the method further comprising:

an act of the authenticator computing entity generating second secret key data;

an act of the authenticator computing entity providing the second secret key data to the supplemental authenticator computing entity;

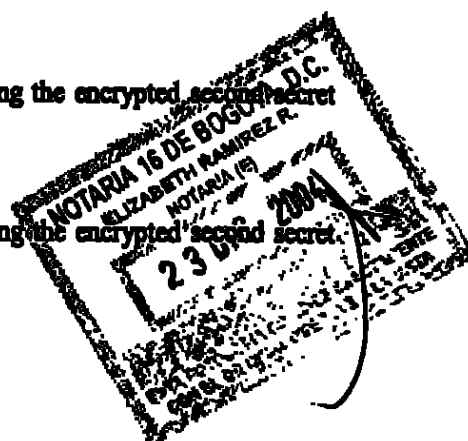
an act of the supplemental authenticator computing entity encrypting the second secret key data using the secret data known to the supplemental authenticatee and supplemental authenticator computing entities;

an act of the supplemental authenticator computing entity providing the encrypted second secret key data to the authenticator computing entity;

an act of the authenticator computing entity providing the encrypted second secret key data to the authenticatee computing entity;

an act of the authenticatee computing entity providing the encrypted second secret key data to the supplemental authenticatee computing entity;

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 BOWLE GATE TOWER
80 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



107

775
108

an act of the supplemental authenticatee computing entity decrypting the encrypted second secret key data using the secret data known to the supplemental authenticatee and supplemental authenticator computing entities; and

an act of the supplemental authenticatee computing entity providing the second secret key data to the authenticatee computing entity.

17. A method in accordance with Claim 16, further comprising the following:

an act of the authenticatee computing entity generating a digest of the first and second secret key data combined with one or more other data items;

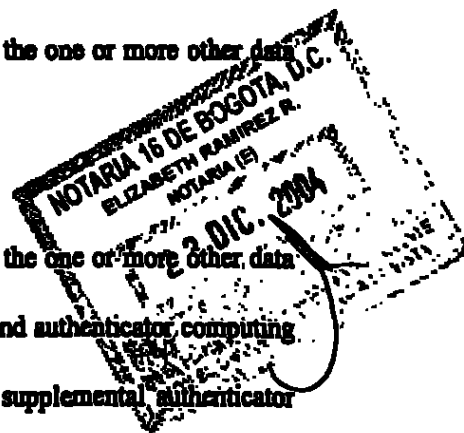
an act of the authenticator computing entity also generating the digest of the first and second secret key data combined with the one or more other data items; and

an act of the authenticatee and authenticator computing entities communicating using messages that are at least partially secured using the digest.

18. A method in accordance with Claim 17, wherein the one or more other data items includes the challenge.

19. A method in accordance with Claim 18, wherein the one or more other data items includes the answer.

20. A method in accordance with Claim 19, wherein the one or more other data items includes third secret key data known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1600 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

[Handwritten mark]

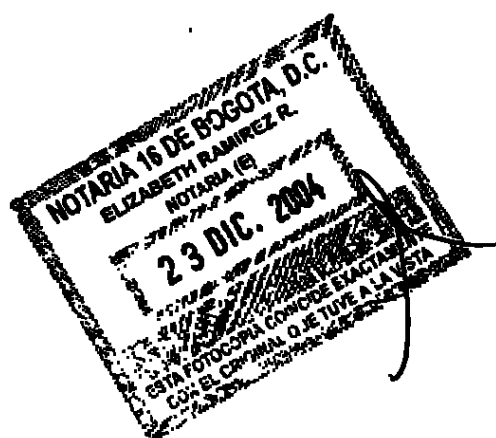
109

21. A method in accordance with Claim 17, wherein the one or more other data items includes the answer.

22. A method in accordance with Claim 21, wherein the one or more other data items includes third secret key data known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.

23. A method in accordance with Claim 17, wherein the one or more other data items includes third secret key data known to the authenticatee and authenticator computing entities, but not known to the supplemental authenticatee and supplemental authenticator computing entities.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



201

24. In an environment that includes an authenticatee computing entity, a supplemental authenticatee computing entity, an authenticator computing entity, and a supplemental authenticator computing entity, a method for the authenticatee computing entity to authenticate the authenticator computing entity using challenge based authentication and without requiring the authenticatee and authenticator computing entities be aware of secret data used for the authentication, the method comprising the following:

an act of the acquiring a challenge from the supplemental authenticatee computing entity;

an act of providing the challenge to the authenticator computing entity, wherein the authenticator computing entity acquires an answer to the challenge from the supplemental authenticator computing entity;

an act of the acquiring the answer from the authenticator computing entity; and

an act of the using the answer to authenticate the authenticator computing entity.

25. A method in accordance with Claim 24, wherein the act of acquiring a challenge from the supplemental authenticatee computing entity comprises the following:

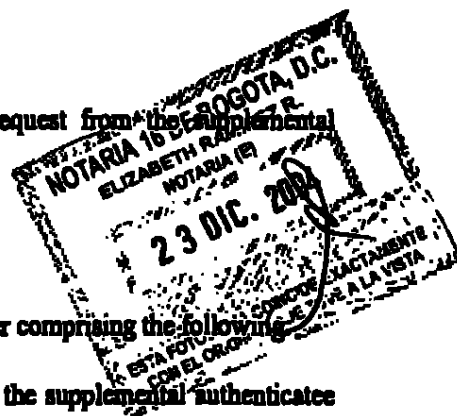
an act of providing a challenge request to the supplemental authenticatee computing entity; and

an act of acquiring an answer to the challenge request from the supplemental authenticatee computing entity.

26. A method in accordance with Claim 24, further comprising the following:

an act of acquiring an answer to the challenge from the supplemental authenticatee computing entity, wherein

WORKMAN NYDEROGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 BAYVIEW TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



X

776
111

the act of using the answer to authenticate the authenticator computing entity comprises the following:

an act of matching the answer as acquired from the supplemental authenticatee computing entity with the answer as provided by the authenticator computing entity.

27. A method in accordance with Claim 24, wherein the act of using the answer to authenticate the authenticator computing entity comprises the following:

an act of providing the answer to the supplemental authenticatee computing entity;
and

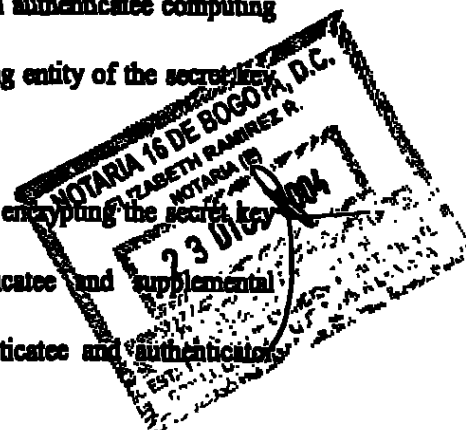
an act of receiving from the supplemental authenticatee computing entity an indication that the answer provided by the authenticator computing entity is a proper answer for the challenge acquired from the supplemental authenticatee computing entity.

28. A method in accordance with Claim 24, further comprising:

an act of the generating secret key data that is not known to the supplemental authenticatee, authenticator or supplemental authenticator computing entities;

an act of providing the secret key data to the supplemental authenticatee computing entity thereby informing the supplemental authenticatee computing entity of the secret key data;

an act of the supplemental authenticatee computing entity encrypting the secret key data using secret data known to the supplemental authenticatee and supplemental authenticator computing entities, but not known to the authenticatee and authenticator computing entities;



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAST GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

112

an act of the acquiring an encrypted secret key data from the supplemental authenticator computing entity, the encrypted secret key data being the secret key data encrypted using secret data known to the supplemental authenticator and supplemental authenticator computing entities, but not known by the authenticator and authenticator computing entities; and

an act of providing the encrypted secret key data to the authenticator computing entity, wherein the authenticator computing entity provides the encrypted secret key data to the supplemental authenticator computing entity for decryption by the supplemental authenticator computing entity, and receives the secret key data.

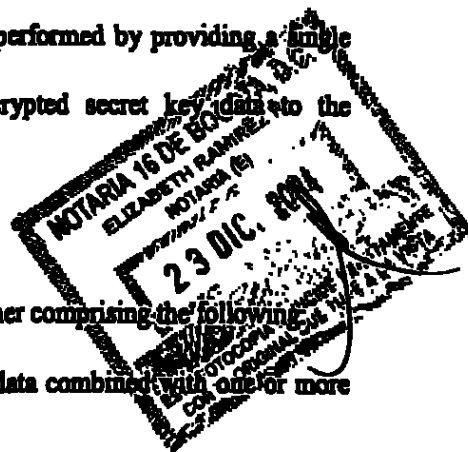
29. A method in accordance with Claim 28, further comprising the following:

an act of communicating with the authenticator computing entity using messages that are at least partially secured using the secret key data.

30. A method in accordance with Claim 28, wherein the act of providing the challenge to the authenticator computing entity and the act of the providing the encrypted secret key data to the authenticator computing entity are performed by providing a single message that includes both the challenge and the encrypted secret key data to the authenticator computing entity.

31. A method in accordance with Claim 28, further comprising the following:

an act of the generating a digest of the secret key data combined with one or more other data items;

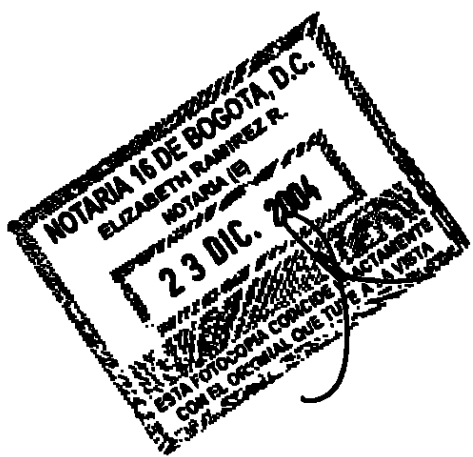


WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1850 MAGNOLIA TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

113

an act of the communicating with the authenticator computing entity using messages
that are at least partially secured using the digest.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



32. A computer program product for use in an environment that includes an authenticatee computing entity, a supplemental computing entity, an authenticator computing entity, and a supplemental authenticator computing entity, the computer program product for implementing a method for the authenticatee computing entity to authenticate the authenticator computing entity using challenge based authentication and without requiring the authenticatee and authenticator computing entities be aware of secret data used for the authentication, the computer program product comprising one or more computer-readable media having thereon computer-executable instructions, that when executed by the authenticatee computing entity, causes the computing entity to perform the method, the method comprising the following:

an act of the acquiring a challenge from the supplemental authenticatee computing entity;

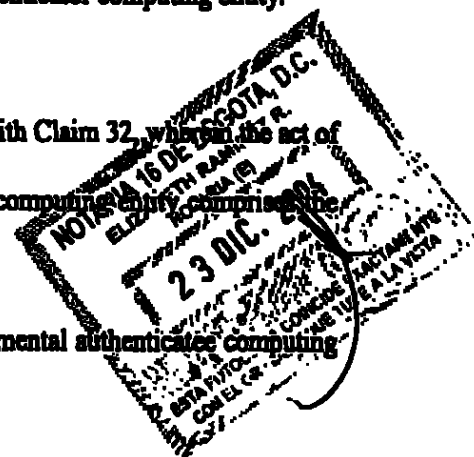
an act of providing the challenge to the authenticator computing entity, wherein the authenticator computing entity acquires an answer to the challenge from the supplemental authenticator computing entity,

an act of the acquiring the answer from the authenticator computing entity; and

an act of the using the answer to authenticate the authenticator computing entity.

33. A computer program product in accordance with Claim 32, wherein the act of acquiring a challenge from the supplemental authenticatee computing entity comprises the following:

an act of providing a challenge request to the supplemental authenticatee computing entity; and



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1800 EAGLE GATE TOWER
80 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

56

115

an act of acquiring an answer to the challenge request from the supplemental authenticatee computing entity.

34. A computer program product in accordance with Claim 33, wherein the method further comprises the following:

an act of acquiring an answer to the challenge from the supplemental authenticatee computing entity, wherein

the act of using the answer to authenticate the authenticator computing entity comprises the following:

an act of matching the answer as acquired from the supplemental authenticatee computing entity with the answer as provided by the authenticator computing entity.

35. A computer program product in accordance with Claim 32, wherein the act of using the answer to authenticate the authenticator computing entity comprises the following:

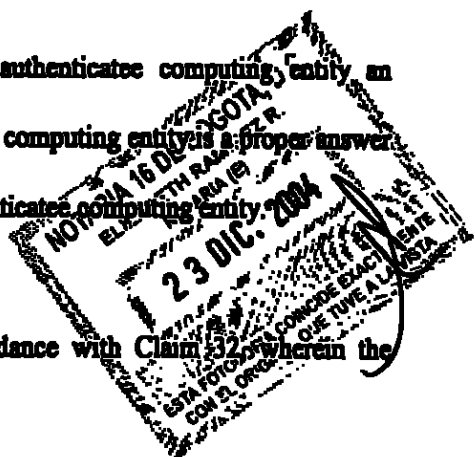
an act of providing the answer to the supplemental authenticatee computing entity;

and

an act of receiving from the supplemental authenticatee computing entity an indication that the answer provided by the authenticator computing entity is a proper answer for the challenge acquired from the supplemental authenticatee computing entity.

36. A computer program product in accordance with Claim 32, wherein the method further comprises:

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



48

121
116

an act of the generating secret key data that is not known to the supplemental authenticatee, authenticator or supplemental authenticator computing entities;

an act of providing the secret key data to the supplemental authenticatee computing entity thereby informing the supplemental authenticatee computing entity of the secret key data;

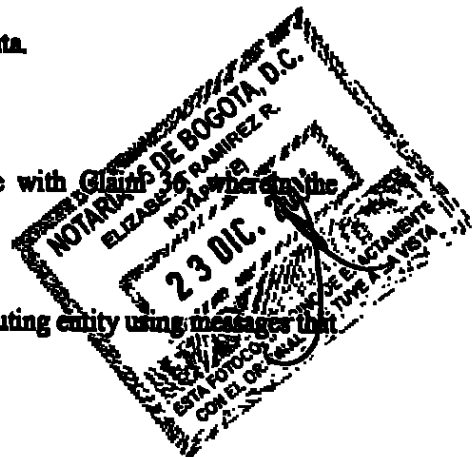
an act of the supplemental authenticatee computing entity encrypting the secret key data using secret data known to the supplemental authenticatee and supplemental authenticator computing entities, but not known to the authenticatee and authenticator computing entities;

an act of the acquiring an encrypted secret key data from the supplemental authenticatee computing entity, the encrypted secret key data being the secret key data encrypted using secret data known to the supplemental authenticatee and supplemental authenticator computing entities, but not known by the authenticatee and authenticator computing entities; and

an act of providing the encrypted secret key data to the authenticator computing entity, wherein the authenticator computing entity provides the encrypted secret key data to the supplemental authenticator computing entity for decryption by the supplemental authenticator computing entity, and receives the secret key data.

37. A computer program product in accordance with Claim 1, wherein the method further comprises the following:

an act of communicating with the authenticator computing entity using messages that are at least partially secured using the secret key data.



WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

49

122
117

38. A computer program product in accordance with Claim 36, wherein the act of providing the challenge to the authenticator computing entity and the act of the providing the encrypted secret key data to the authenticator computing entity are performed by providing a single message that includes both the challenge and the encrypted secret key data to the authenticator computing entity.

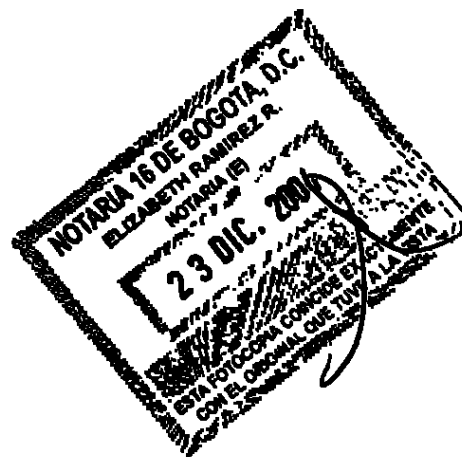
39. A computer program product in accordance with Claim 36, wherein the method further comprises the following:

an act of the generating a digest of the secret key data combined with one or more other data items;

an act of the communicating with the authenticator computing entity using messages that are at least partially secured using the digest.

40. A computer program product in accordance with Claim 36, wherein the one or more computer-readable media are physical media.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



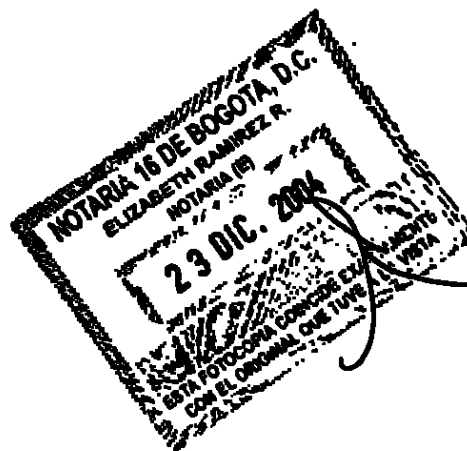
125
118

ABSTRACT OF THE DISCLOSURE

A challenge based authentication mechanism that does not require that the authenticating computing entities be aware of the secret data used for the initial authentication. An authenticator computing entity is to authenticate to the authenticatee computing entity. First, the authenticatee computing entity acquires a challenge from a supplemental authenticatee computing entity. The authenticatee computing entity provides the challenge to the authenticator computing entity, which has a supplemental authenticator computing entity solve the challenge. The authenticator computing entity sends the answer to the authenticatee computing entity, which uses the answer to authenticate the authenticator computing entity.

W:\13768\485.1\A\1.0000000492V001.doc

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



[Handwritten signature]

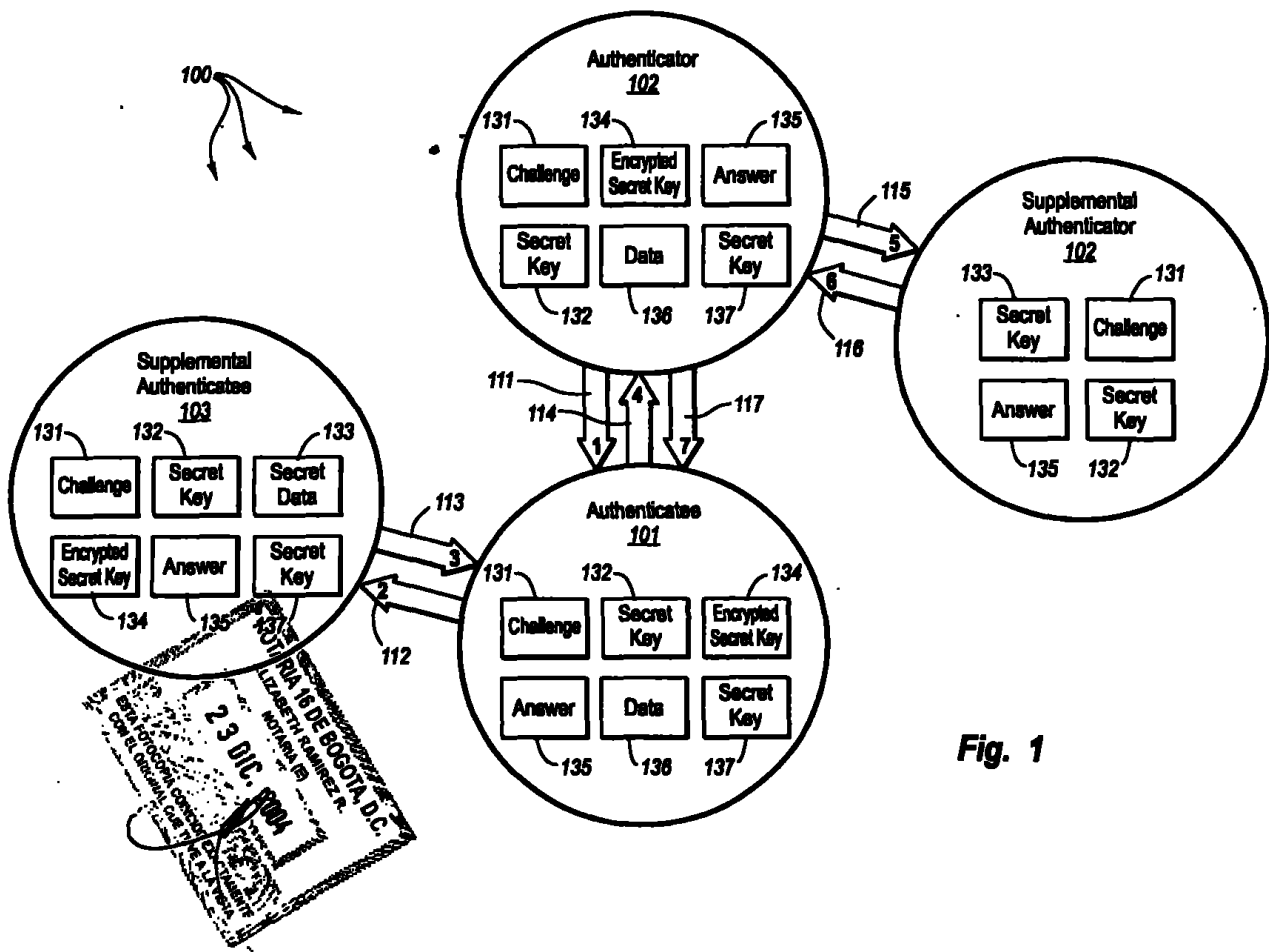


Fig. 1

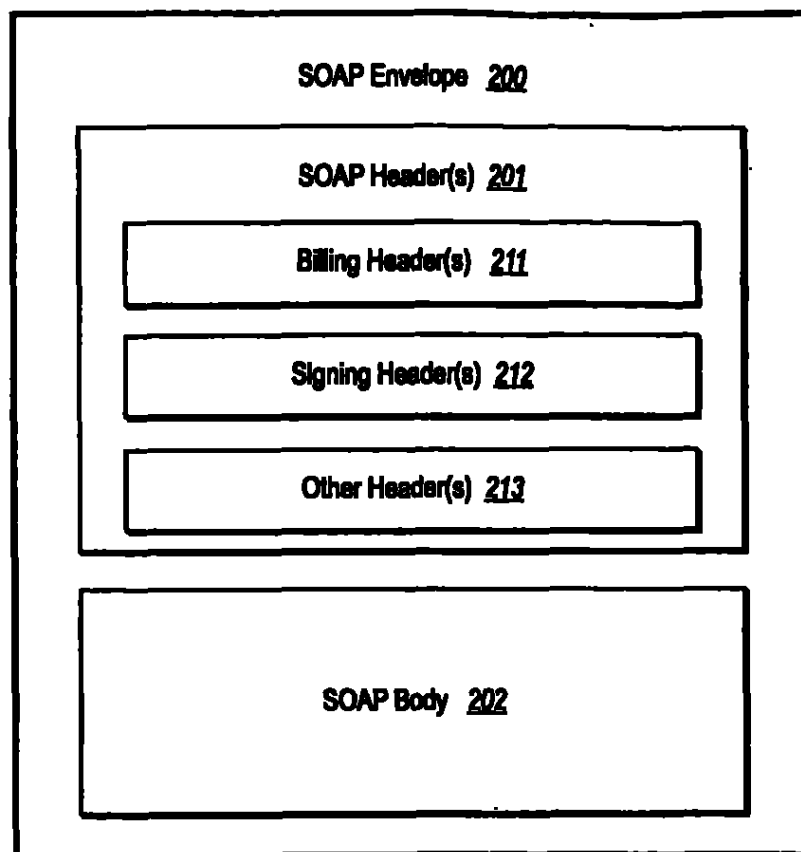


Fig. 2



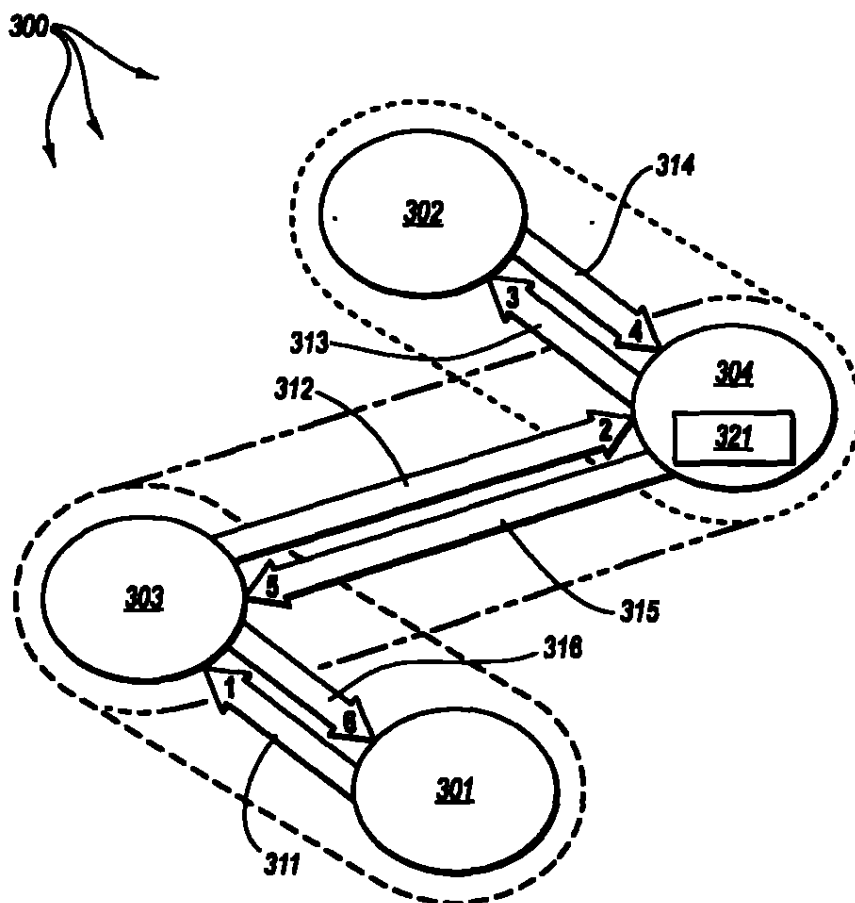


Fig. 3



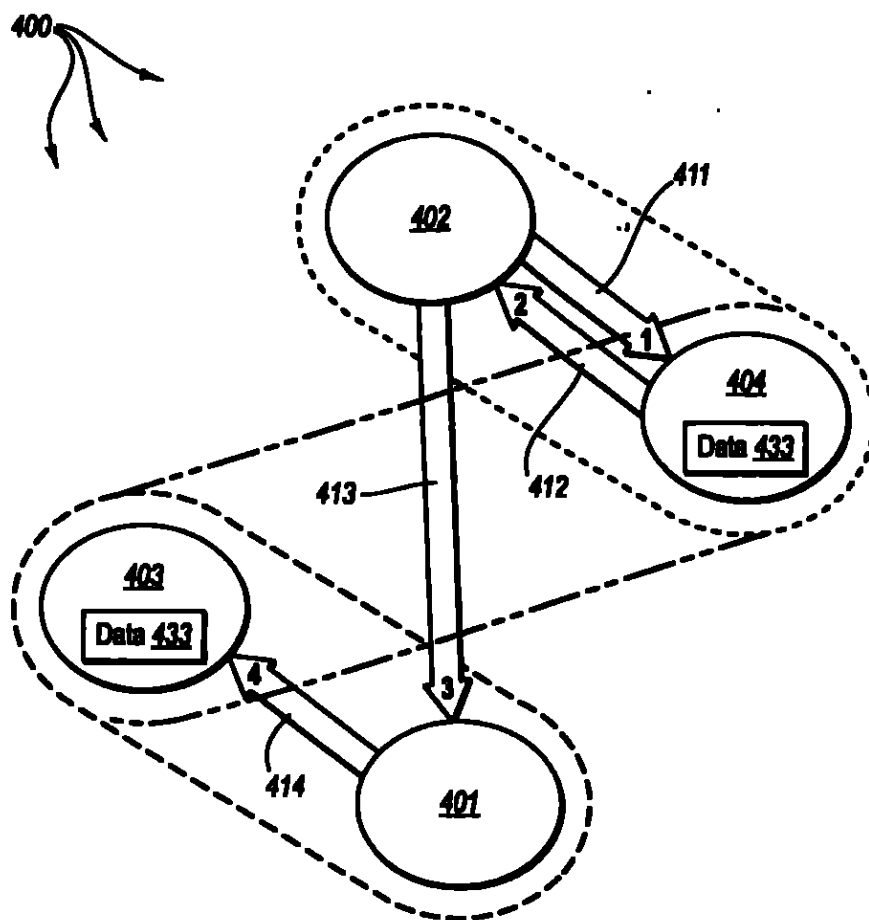


Fig. 4



LOS ESTADOS UNIDOS DE AMERICA.
A todos aquellos a los que se presente este documento:

EL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS

La Oficina de Patentes y Marcas de los Estados Unidos

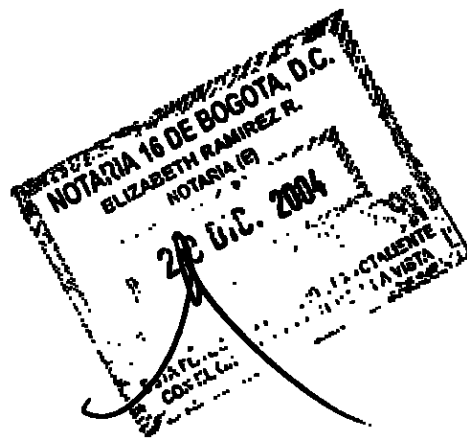
Octubre 20, 2004.

ESTO CERTIFICA QUE EL ANEXO A LA PRESENTE ES UNA COPIA AUTENTICA DE LOS REGISTROS DE LA OFICINA DE PATENTES Y MARCAS DE LOS ESTADOS UNIDOS DE AMERICA CORRESPONDIENTES A LOS DOCUMENTOS DE LA SOLICITUD DE PATENTE IDENTIFICADA A CONTINUACIÓN LOS CUALES CUMPLIERON CON LOS REQUERIMIENTOS PARA OTORGARLE UNA FECHA DE PRESENTACIÓN BAJO EL 35 USC 111.

NUMERO DE SOLICITUD: 10/917.786
FECHA DE SOLICITUD: Agosto 13, 2004.

(SELLO DE LA OFICINA DE PATENTES Y MARCAS DE LOS ESTADOS UNIDOS,
DEPARTAMENTO DE COMERCIO) Por la autoridad del
Comisionado de Patentes y Marcas

Firmado (Ilegible)
P.R. GRANT
Oficial de Certificación



(Sello con código de barras)
18351 U.S. PTO
Código No. 081304

(Sello con código de barras)
19270 U.S. PTO
10/917786
Código No. 081304

Sello de Correo Expreso No. EV510294625 US

**TRANSMISIÓN DE SOLICITUD DE PATENTE DE UTILIDAD
(COMO GRAN ENTIDAD)**
(Solamente para solicitudes nuevas no provisionales bajo 37 CFR 1.53 (b))

Archivo No.
13768.485.1
Total de páginas en esta
presentación
4

COMISIONADO PARA PATENTES
P.O. Box 1450
Alexandria VA, 22313-1450

Se transmite por este medio para solicitud bajo el 35 U.S.C. 111 (a) y 37 C.F.R. 1.53. (b), una solicitud de patente para la invención titulada:

**LA AUTENTICACIÓN DESAFÍO-BASADO SIN REQUERIR CONOCIMIENTO DE DATOS DE
LA AUTENTICACIÓN CONFIDENCIALES**

E Inventada por:

Max G. Morris
Christopher G. Kaler

Si es continuación de una solicitud, marque la casilla apropiada y suministre la siguiente información requerida:

- ☐ Continuación ☐ Divisional ☐ Continuación-en-parte (CIP) de la Solicitud anterior No. _____
Que es una:
- ☐ Continuación ☐ Divisional ☐ Continuación-en-parte (CIP) de la Solicitud anterior No. _____
Que es una:
- ☐ Continuación ☐ Divisional ☐ Continuación-en-parte (CIP) de la Solicitud anterior No. _____

Se encuentran adjuntos:

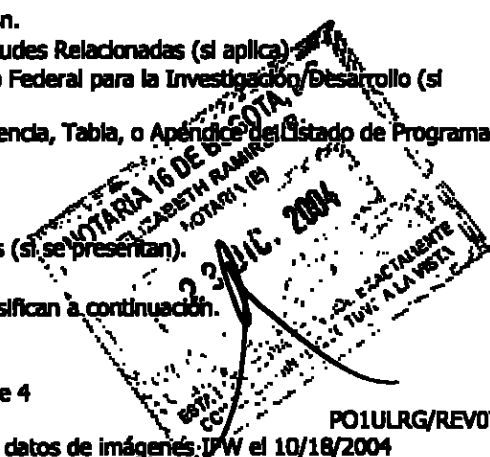
Elementos de la Solicitud

1. ☒ Cargo de presentación como fue calculado y transmitido como se describe abajo.
2. ☒ La especificación tiene 35 páginas e incluye lo siguiente:
 - a. ☒ Título Descriptivo de la Invención.
 - b. ☒ Referencias cruzadas con Solicitudes Relacionadas (si aplica).
 - c. ☐ Declaración relativa a patrocinio Federal para la Investigación/Desarrollo (si aplica).
 - d. ☐ Referencia a un Listado de Secuencia, Tabla, o Apéndice del Estado de Programa de Cómputo.
 - e. ☒ Antecedentes de la Invención.
 - f. ☒ Resumen de la Invención.
 - g. ☒ Breve descripción de los Dibuños (si se presentan).
 - h. ☒ Descripción Detallada.
 - i. ☒ Reivindicación (es) como se Clasifican a continuación.
 - j. ☒ Abstracto de lo revelado.

Página 1 de 4

Copia proporcionada por USPTO de la base de datos de imágenes: TFW el 10/18/2004

PO1ULRG/REV07



**TRANSMISIÓN DE SOLICITUD DE PATENTE DE UTILIDAD
(COMO GRAN ENTIDAD)***(Solamente para solicitudes nuevas no provisionales bajo 37 CFR 1.53 (b))*Archivo No.
13768.485.1Total de páginas en esta
presentación
4**Elementos de la Solicitud (Continuación)**

3. ☒ Dibujo (s) (cuando sea necesario como lo prescribe el 35 USC 113)
- a. ☒ Formal Numero de Hojas 4
- b. ☐ Informal Numero de Hojas _____
4. ☐ Juramento o Declaración
- a. ☐ Nuevamente ejecutada (original o copia) ☐ Inejecutada
- b. ☐ Copia de una anterior aplicación (37 CFR 1.63(d)) (para continuación/divisional únicamente)
- c. ☐ Con poder de abogado ☐ Sin poder de abogado
- d. ☐ **REMOCIÓN DE INVENTORE(S)**
Declaración firmada aneja removiendo inventor(es) mencionados en solicitud anterior, ver 37 C.F.R. 1.63 (d)(2) y 1.33 (b).
5. ☐ Incorporación por referencia (utilizable si la casilla 4b está marcada).
La revelación integral de la solicitud anterior, de la cual una copia de el juramento o declaración es proporcionada bajo la Casilla 4b, se considera como parte de la divulgación de la solicitud adjunta y es por este medio incorporada por referencia a la misma.
6. ☐ CD ROM o CD-R en duplicado, tabla grande o Programa de Cómputo (Apéndice)
7. ☐ Hoja de Datos de la Solicitud. (Ver 37 CFR 1.76).
8. ☐ Presentación de secuencias de Nucleótidos y/o Amino-ácidos (si es aplicable, todos deben ser incluidos).
- a. ☐ Legible en Formato de Cómputo (CFR)
- b. ☐ Especificación de Secuencia Listada en:
- i. ☐ CD-ROM o CD-R (2 Copias); o
- ii. ☐ Papel
- c. Declaración(es) Verificando la Identidad del Papel y la Copia legible en formato de Cómputo

Partes que acompañan la solicitud

9. ☐ Documentos de Traspaso (carátula y documento (s)).
10. ☐ 37 CFR 3.73 (B) Declaración (cuando hay un cesionario)
11. ☐ Documento de Traducción al Inglés (Si aplica)
12. ☐ Declaración de divulgación de la Información/PTO-1449 Copias de Citaciones de IDS
13. ☐ Corrección preliminar
14. ☒ Recibo de retorno postal (MPEP 503) (Debe ser respaldadamente firmado)
15. ☐ Copia Certificada de los Documentos de Prioridad (si una Prioridad extranjera es reivindicada).
16. ☒ Certificado de Correo
- ☐ Primera Clase ☒ Correo Expreso (Especificar Sello No. EV510294625US)

Página 2 de 4

Copia proporcionada por USPTO de la base de datos de imágenes IFW el 10/18/2004

PO1ULRG/REV07

125

SA

**TRANSMISIÓN DE SOLICITUD DE PATENTE DE UTILIDAD
(COMO GRAN ENTIDAD)**
(Solamente para solicitudes nuevas no provisionales bajo 37 CFR 1.53 (b))Archivo No.
13768.485.1
Total de páginas en esta
presentación
4**Elementos de la Solicitud (Continuación)**

- 17.
- ☒
- Anexos adicionales (por favor identificar abajo):

- PTO 2038 Forma de Tarjeta de Crédito por \$1.130
- La presente Solicitud reivindica prioridad de la Solicitud de Patente Provisional de los Estados Unidos con número serial 60/515,461 presentada el 29 de Octubre de 2003, cuya solicitud provisional está incorporada a esta en su integridad por referencia.

Solicitud de No Publicación de Acuerdo con 35 U.S.C. 122 (b)(2)

18. De acuerdo con 35 U.S.C. 122 (b)(2). El Solicitante requiere que la presente solicitud de patente no sea publicada de acuerdo con 35 U.S.C. 122 (b)(1). El solicitante por medio de la presente certifica que la invención divulgada en esta solicitud no ha sido ni será objeto de una solicitud presentada en otro país, o bajo tratados internacionales multilaterales, que requieran la publicación de solicitudes 18 meses después de la presentación de la solicitud.

Advertencia

El solicitante que formule una solicitud de no publicación, pero que subsecuentemente presente en un país extranjero o bajo un tratado internacional especificado en 35 U.S.C. 122 (b)(2)(B)(i), debe notificar al Director de tal presentación, no mas tarde de 45 días después de la fecha de presentación de tal solicitud extranjera o internacional. El proporcionar esta noticia por el solicitante dentro del período aquí prescrito, resultará en el abandono de la solicitud, salvo que se demuestra a satisfacción del Director que el retraso en presentar la noticia no fue intencional.



Página 3 de 4

PO1ULRG/REV07

Copia proporcionada por USPTO de la base de datos de Imágenes IFW el 10/18/2004

**TRANSMISIÓN DE SOLICITUD DE PATENTE DE UTILIDAD
(COMO GRAN ENTIDAD)**
(Solamente para solicitudes nuevas no provisionales bajo 37 CFR 1.53 (b))Archivo No.
13768.485.1
Total de páginas en esta
presentación
4**Cálculo de Cargos y Transmisión.****REIVINDICACIONES COMO FUERON PRESENTADAS**

Para	#Presentado	#Permitido	#Extra	Cargo	Tasa
Total Reivindicaciones	40	-20=	20	X 18.00	\$360.00
Reivindicaciones Indep.	3	-3=	0	X 86.00	\$0.00
Reivindicaciones múltiples dependientes (marcar si es aplicable) ☐					\$0.00
Tasa Básica					\$770.00
Otras Tasas (especificar propósito)					\$0.00
Total Tasa de Presentación					\$1,130.00

☐ Un cheque por el monto de para cubrir la tasa de presentación adjunta.☒ El Director está autorizado por medio de la presente a cobrar la Cuenta de Depósito No. 23-3178 como se describe a continuación.Cargo en el monto de como tasa de presentación.
Crédito y sobrepago.Cargo de cualquier tasa de presentación requerida bajo 327 C.F.R. 1.16 y 1.17.
Cargo de la tasa de emisión fijada en 37 C.F.R. 1.18 con el envío por correo de la Noticia de Concesión, de acuerdo con 37 C.F.R. 1.311 (b).Fecha: Agosto 13, 2004.
Cliente No. 022913Firma
Michael B. Dodd
Reg. No.:46,437
Abogado del Solicitante
Cliente No.:022913

Página 3 de 4

PO1ULRG/REV07

Copia proporcionada por USPTO de la base de datos de Imágenes IFW el 10/18/2004

128

CERTIFICADO DE ENVIO POR "CORREO EXPRESO" (37 CFR1.10)				Archivo No. 13768.485.1	
<i>Solicitante(s): Max G. Morris et al</i>					
Solicitud No. Desconocida	Fecha de solicitud Agosto 13, 2004	Examinador Desconocido	Cliente No. 022913	Unidad de Grupo de Arte Desconocida	
Invento: LA AUTENTICACIÓN DESAFIO-BASADO SIN REQUERIR CONOCIMIENTO DE DATOS DE LA AUTENTICACIÓN CONFIDENCIALES					

Por medio de la presente certifico que la presente correspondencia:

(ver abajo)

(Identificar el tipo de correspondencia)

Está siendo depositada ante el Servicio Postal de los Estados Unidos "Oficina Correo Expreso al Remitido" servicio bajo 37 CFR 1.10 un sobre dirigido a: Comisionado de Patentes, P.O. BOX 1450, Alexandria VA 22313-1450 en

Agosto 13, 2004

(fecha)

Dea So

(Nombre de la persona enviando la correspondencia digitado o impreso)

FIRMA ILEGIBLE

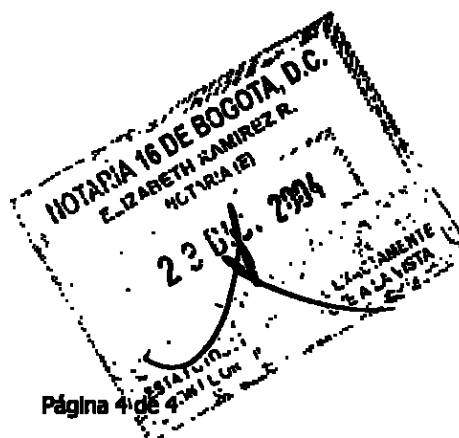
(Firma de la persona enviando la correspondencia)

EV510294625 US

(Sello de Envío de Correo "Express Mail")

Nota: Cada papel debe tener su certificado de correo

Solicitud de patente (35 pag.); 4 páginas de dibujos formales; formato de pago tarjeta de crédito PTO-2038 por valor de \$1.130.00; Carta de transmisión (4 pag. En duplicado); Certificado de "Express Mailing" (EV510294625US), Tarjeta Postal.



Página 4 de 4

P06A/REV03

Copia proporcionada por USPTO de la base de datos de Imágenes IFW el 10/18/2004

10

SOLICITUD DE PATENTE DE LOS ESTADOS UNIDOS

De

Max G. Morris

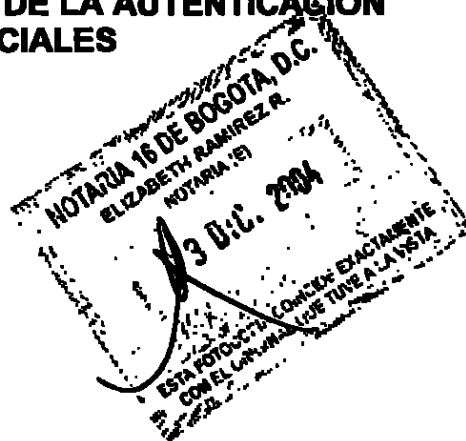
y

Christopher G. Kaler

para

**LA AUTENTICACIÓN DESAFÍO-BASADO SIN REQUERIR
CONOCIMIENTO DE DATOS DE LA AUTENTICACIÓN
CONFIDENCIALES**

(Sello)
Workman Nydegger
Sociedad Profesional
Abogados
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City Utah 84111



Copia proporcionada por USPTO de la base de datos de Imágenes IFW el 10/18/2004

APLICACIÓN DE PATENTES DE LOS ESTADOS UNIDOS

de

Max G. Morris

Y

Christopher G. Kaler

Para

**LA AUTENTICACIÓN DESAFÍO-BASADO SIN REQUERIR CONOCIMIENTO DE
DATOS DE LA AUTENTICACIÓN CONFIDENCIALES**

131

LA AUTENTICACIÓN DESAFÍO-BASADA SIN REQUERIR CONOCIMIENTO DE DATOS DE LA AUTENTICACIÓN CONFIDENCIALES

EL FONDO DE LA INVENCION

1. Referencia de Cruce de las Aplicaciones Relacionadas

[0001] La aplicación presente exige la prioridad a Estados Unidos el número de serie de la aplicación patente provisional 60/515,461 archivado el 29 de octubre de 2003, cuya aplicación provisional está aquí dentro incorporada por referencia en su integridad.

2. El Campo de la Invención

[0002] La invención presente generalmente se refiere a la autenticación. Más específicamente, la invención presente se refiere a mecanismos de autenticación desafío-basado (challenge-based) que no requieren conocimiento de datos de autenticación confidenciales.

3. El Fondo y El Arte Pertinente

[0003] La tecnología de cómputo ha transformado la manera como nosotros trabajamos y jugamos. Los sistemas de cómputo y los dispositivos (aquí después también referidos simplemente como "entidades de cómputo") ahora toman una variedad amplia de formas incluso las computadoras de escritorio, las computadoras portátiles, los "tablet" PCs, los Asistentes Digitales Personales (PDAs), dispositivos de casa y similares. En su más básica forma, un sistema de informática incluye memoria del sistema y uno o más procesadores. El software en el sistema de memoria puede ejecutarse por el procesador para dirigir el otro hardware del sistema de informática para realizar las funciones deseadas. En otras entidades de cómputo, la lógica se lleva a cabo usando el hardware, o una combinación de software y hardware.

[0004] Las tecnologías de RED permiten a las entidades de cómputo incluso comunicarse sobre inmensas distancias, extendiendo la funcionalidad de la computadora. Por ejemplo, las tecnologías de RED habilitan tales aplicaciones como el correo electrónico, navegación WEB, el traslado del archivo, la mensajería instantánea, el tablero "whiteboarding" electrónico, la colaboración de red, y similares. Por lo tanto, las redes de computadores habilitan la comunicación extendida y el acceso a la información.

[0005] Desafortunadamente, las redes de computadoras también pueden abrir potencialmente las entidades de informática conectadas a las brechas de seguridad. Un tipo de brecha de seguridad es para un sistema de cómputo o usuario para hacer demandas falsas sobre quién de ellos puede acceder los recursos por eso ellos no deben tener el acceso. Para garantizar esto, una de cómputo autenticada (es decir, una entidad de cómputo que requiere la autenticación) requerirá a menudo un autenticador de cómputo de entidad (es decir, una entidad de cómputo que debe autenticar) para autenticarse. Las entidades de cómputo que autentican pueden tomar una decisión más informada que se considera cómo actuar recíprocamente con el autenticador de la entidad de cómputo.

[0006] Un formulario particularmente útil de autenticación está a menudo llamado como la autenticación del desafío-respuesta (challenge/response). En este formulario de autenticación, cuando un autenticador de entidad (después también llamado el "autenticador") para autenticar a una entidad de cómputo autenticada (después también llamado el "autenticado"), el autenticado envía un desafío al autenticador. El autenticado genera una contestación (también se refirió aquí

8

127
132

dentro como una respuesta) al desafío típicamente aplicando un algoritmo de detalle en un sentido único al desafío que usa los datos confidenciales disponibles al autenticado y al autenticador. Por ejemplo, estos datos confidenciales pueden ser una contraseña que corresponde al autenticador. El autenticador igualmente también genera la misma respuesta usando el mismo algoritmo detallando y usando los mismos datos confidenciales. El autenticador proporciona su respuesta entonces al autenticado. El autenticado compara la respuesta que los autenticadores generaron con la respuesta que los autenticados generaron. Si las respuestas emparejan, entonces la autenticación tiene éxito. La autenticación del desafío-respuesta (challenge/response) es ventajosa en que los propios datos confidenciales no se transmiten, y así no pueden interceptarse.

[0007] Sin embargo, esta autenticación del desafío-respuesta (challenge/response) requiere que el autenticador y el autenticado que computan las entidades tienen acceso a los datos confidenciales usados para la autenticación, y el autenticador y el autenticado de las entidades de cómputo generan la respuesta. En algunos ambientes esto no puede ser deseable. Por ejemplo, muchas entidades de la informática han limitado el poder del proceso. La generación de una respuesta puede degradar la actuación de la entidad de cómputo desviando el poder del proceso de otros procesos. Además, las entidades de cómputo no pueden ser afianzadas. En concordancia, una entidad desautorizada podría acceder los datos confidenciales plausiblemente y podría usar los datos para autenticar falsamente.

[0008] En concordancia, lo que sería ventajoso es un mecanismo de autenticación de desafío-respuesta (challenge/response) que no requiere las entidades de cómputo autenticador y autenticado para generar una respuesta o contener los datos confidenciales el mismo.

EL RESUMEN BREVE DE LA INVENCION

[0009] Los problemas anteriores con el estado anterior del arte son superados por los principios de la invención presente que relaciona un desafío basado en el mecanismo de autenticación que no requiere que las entidades de cómputo autenticadas sean conscientes de los datos confidenciales usados para la autenticación inicial.

[0010] El ambiente incluye cuatro entidades de cómputo, una entidad de cómputo autenticado, una entidad de cómputo autenticador, una entidad de cómputo del autenticador, y un autenticador suplitorio de la entidad de cómputo. El autenticador de la entidad de cómputo es para autenticar a la entidad de cómputo del autenticado, pero no tiene acceso directo a los datos confidenciales necesarios para autenticar.

[0011] Primero, el autenticado adquiere un desafío del autenticado suplitorio. Este desafío puede resolverse por el autenticador suplitorio, pero no por el autenticado y autenticador. Los autenticados también pueden pasar una clave confidencial al autenticado suplitorio. El autenticado suplitorio encripta la clave confidencial que usa los datos confidenciales conocidos por el autenticado y el autenticador suplitorios, pero no para el autenticado y autenticador mismos. Este desafío y los datos confidenciales son la base para la autenticación, a pesar de los datos confidenciales que son desconocidos al autenticado y autenticador, y a pesar del desafío que es directamente insoluble por el autenticado o autenticador.

[0012] El autenticado proporciona el desafío así como potencialmente la clave encriptada al autenticador. El autenticador proporciona el desafío y cualquiera encriptación de la clave al autenticador suplitorio. El autenticador suplitorio resuelve el desafío para generar una respuesta, y también descifra la clave encriptada. El autenticador suplitorio proporciona la respuesta y la clave descifrada al autenticador. En esta fase, la clave descifrada se conoce por el autenticado y autenticador y puede usarse para afianzar las comunicaciones futuras entre el autenticado y autenticador.

133

133

[0013] El autenticador envía la respuesta entonces al autenticado. El autenticado usa esta respuesta luego para autenticar el autenticador validando la respuesta directamente, o causando el autenticado supletorio para validar la respuesta.

[0014] Se configurarán los rasgos adicionales y ventajas de la invención en la descripción que sigue, y en parte será obvio la descripción, o puede aprenderse por la práctica de la invención. Pueden comprenderse los rasgos y ventajas de la invención y pueden obtenerse por medio de los instrumentos y combinaciones particularmente apuntando fuera de las demandas añadidas. Éstos y otros rasgos de la invención presente se pondrán claros más ampliamente en la descripción siguiente y las demandas añadidas, o puede aprenderse más adelante por la práctica de la invención como el juego aquí después.

DESCRIPCIÓN BREVE DE LOS GRAFICOS

[0015] Para describir la manera de lo anterior descrito pueden obtenerse otras ventajas y rasgos de la invención, una descripción más particular de la invención brevemente descrita anteriormente se dará por referencia a las encarnaciones específicas que se ilustran en los gráficos añadidos. Entendiendo que estos gráficos muestran sólo personalizaciones típicas de la invención y no son consideradas por consiguiente limitadas de su alcance, la invención se describirá y se explicará con la especificidad adicional y se detallará a través del uso de los gráficos adjuntos en los cuales:

[0016] La figura 1 es un diagrama de un intercambio del mensaje entre un autenticado, autenticado supletorio, autenticador, y el autenticador supletorio de las entidades de cómputo de acuerdo con los principios de la invención presente;

[0017] La figura 2 ilustra una estructura de datos esquemáticamente en la forma de un Protocolo de Acceso de Objeto Simple (SOAP) que incluye encabezados de SOAP en la forma de cargar y firmar los encabezados;

[0018] La figura 3 ilustra un intercambio de mensajes en que electrónicamente se transfieren los artículos transferibles entre dos entidades de cómputo de acuerdo con una primera personalización de la invención presente; y

[0019] La figura 4 ilustra un intercambio de mensaje en que electrónicamente se transfieren los artículos transferibles entre dos entidades de cómputo de acuerdo con una segunda personalización de la invención presente.

DESCRIPCIÓN DETALLADA DE LAS PERSONALIZACIONES PREFERIDAS

[0020] Los principios de la invención presente proporcionan un desafío basado en el mecanismo de autenticación que no requiere que las entidades de cómputo autenticando sean conscientes de los datos confidenciales usados para la autenticación inicial, y no requiere la autenticación de las entidades de cómputo mismas que genere una respuesta a un desafío.

[0021] La figura 1 ilustra un ambiente 100 que incluye cuatro entidades de cómputo 101 a través de el 104. Específicamente, las cuatro entidades de cómputo incluyen lo que será llamado una entidad de cómputo autenticado 101, una entidad de cómputo autenticador 102, una entidad de cómputo autenticado supletorio 103, y una entidad de cómputo autenticador supletorio 104. En esta descripción y en las demandas, una "entidad de cómputo es cualquier dispositivo o sistema que puede retener los datos en la memoria y/o almacenamiento, y es capaz de realizar comunicación electrónica.

[0022] Por ejemplo, cada una de las entidades de cómputo 101 a través de 104 pueden tener acceso a sus propios datos interiores, y puede comunicarse con uno o más de las otras entidades de cómputo. Tal necesidad de comunicación no está por red. Por ejemplo, cualquier dos o más entidades de cómputo 101 a

134

AD
B4

través de 104 pueden estar dentro del mismo dispositivo electrónico o sistema de cómputo. Como un ejemplo, los autenticadores supletorios de la entidad de cómputo 104 pueden ser una tarjeta SIM, mientras el autenticador de la entidad de cómputo 102 es un teléfono móvil. Las entidades de cómputo autenticados 101 pueden ser la aplicación frontal del servidor Web, mientras las entidades de cómputo autenticado 103 pueden ser la parte de atrás el servidor Web. No se limitan los principios de la invención presente a esto, sin embargo.

[0023] La entidad de cómputo del autenticador 102 es para autenticar la entidad de cómputo 101. En la personalización de la Figura 1, la entidad de cómputo 101 y la entidad de cómputo autenticado supletorio 103 están en una primera esfera común de confianza. Las entidades de cómputo del autenticador 102 y el autenticador supletorio de la entidad de cómputo 104 también están en una segunda esfera común de confianza. Los autenticadores supletorios de la entidad de cómputo 103 y el autenticador supletorio de la entidad de cómputo 104 están en una tercera esfera común de confianza. Una "esfera de confianza" como la usada en esta descripción y en las demandas se define como una colección de dos o más entidades de cómputo en que cada entidad de cómputo en la esfera de confianza ha recibido un poco de convicción sobre como son las otras entidades de cómputo y que pretenden ser, y esa información de las otras entidades de cómputo es por lo menos algo fiable.

[0024] En esta descripción y en las demandas, el autenticado de la entidad de cómputo 101, el autenticador de la entidad de cómputo 102, el autenticado supletorio de la entidad de cómputo 103, y el autenticador supletorio de la entidad de cómputo 104, también pueden estar llamados simplemente el "autenticado 101", el "autenticador 102", el autenticado supletorio 103" "y el autenticador supletorio 104", respectivamente.

[0025] La figura 1 también muestra un flujo de mensaje de ejemplo que produce la autenticación consistente con los principios de la invención presente. El orden secuencial de un traslado de mensaje se representa secuencialmente por el número en la cabeza de la flecha que representa el traslado del mensaje. Usando este flujo del mensaje, un método de la autenticación de acuerdo con los principios de la invención presente se describirá ahora. El método permite el autenticador 102 para autenticar al autenticado 101 usando desafío-basado en la autenticación y sin requerir que las entidades de cómputo del autenticador 102 y el autenticado 101 sean conscientes de los datos confidenciales usados para la autenticación.

[0026] El autenticado 101 determina que el autenticador 102 es autenticado. Por ejemplo, esto puede lograrse por el autenticado 101 que recibe una demanda de servicio (vea flecha 111) del autenticador 102. Sin embargo, los autenticados 101 pueden hacer la determinación de que el autenticador 102 será autenticado de alguna otra manera que no confía en cualquier demanda de servicio del autenticador 102. En concordancia, la demanda de servicio representada por la flecha 111 no es esencial.

[0027] El autenticado 101 luego adquiere un desafío 131 del autenticado 103 supletorio. Esto puede lograrse de cualquier manera. Sin embargo, en la Figura 1, esto se ilustra como se cumple con dos transferencias de mensaje representados por las flechas 112 y 113. Específicamente, el autenticado 101 proporciona una demanda del desafío representada por la flecha 112 al autenticado 103 supletorio. Los autenticados 103 supletorios pueden luego generar un desafío 131 en la contestación a la demanda del desafío, y entonces proporciona el desafío 131 al autenticado 101 en la contestación a la demanda como se representa por la flecha 113. Sin embargo, hay varias maneras alternativas en que los autenticados 101 pueden adquirir el desafío 131. El desafío 131 se puede haber proporcionado por el autenticado 103 supletorio sin una demanda del desafío como, por ejemplo, cuando el autenticado 101 se registra con el autenticado 103 supletorio, o quizás a tiempos predeterminados o intervalos de tiempo.

%

[0028] En una personalización llamada aquí la "personalización subsiguiente de comunicaciones privadas", pueden emprenderse los actos adicionales tal que el autenticado 101 y el autenticador 102 pueden comunicarse como consecuencia sin confiar en el autenticado 103 suplitorio y el autenticador 104 suplitorio. Por ejemplo, en la personalización de comunicaciones privada subsiguiente, los autenticados 101 pueden generar datos 132 confidenciales importantes que probablemente no conocen al autenticador 102, el autenticado 103 suplitorio, o el autenticador 104 suplitorio.

[0029] El autenticado 101 proporciona los datos 132 importantes confidenciales al autenticado 103 suplitorio que informa al autenticado 103 suplitorio de los datos 132 importantes confidenciales por eso. Los datos importantes confidenciales 132 pueden, por ejemplo, haber sido proporcionados en el mismo mensaje como la demanda del desafío representada por flecha 112.

[0030] Los autenticados 103 suplitorios pueden luego encriptar los datos importantes confidenciales 132 usando datos confidenciales conocidos 133 para las entidades de cómputo autenticado 103 suplitorio y el autenticador suplitorio 104, pero no conocidos por el autenticado 101 y el autenticador 102. Los autenticados 103 suplitorios pueden luego proporcionar los datos 134 importantes confidenciales encriptados al autenticado 101. Estos datos importantes encriptados pueden proporcionar los datos 134 importantes confidenciales al mismo tiempo y/o en el mismo mensaje que los autenticados 103 suplitorios usados para transferir el desafío 131 como está representado por la flecha 113.

[0031] El autenticado 101 proporciona luego el desafío 131 al autenticador 102 como se representa por flecha 114. Al mismo tiempo y/o en el mismo mensaje, los autenticados 101 pueden proporcionar también los datos 134 importantes confidenciales encriptados al autenticador 102 como lo representado por flecha 114.

[0032] El autenticador 102 adquiere entonces una respuesta del desafío 131 del autenticador suplitorio de la entidad de cómputo. Esto puede lograrse de cualquier manera. Sin embargo, en la Figura 1, se ilustra como puede ser cumplido con dos traslados del mensaje representado por las flechas 115 y 116. Específicamente, el autenticador 102 proporciona el desafío 131 al autenticador 104 suplitorio como lo representado por flecha 115. Los autenticadores 103 suplitorios pueden determinar una respuesta 135 al desafío 131, y luego proporcionar la respuesta 135 al autenticador 102 como lo representado por flecha 116. La respuesta puede generarse por, por ejemplo, realizando un algoritmo de detalle en un sentido único en el desafío 131 usando los datos 133 confidenciales.

[0033] En la personalización de comunicaciones privada subsiguiente, los autenticadores 103 pueden proporcionar también los datos 134 importantes confidenciales encriptados al autenticador 104 suplitorio. Esto puede lograrse incluyendo los datos 134 importantes confidenciales encriptados en el mismo mensaje como fue usado para transmitir el desafío al autenticador 134 suplitorio como lo representado por la flecha 115.

[0034] Los autenticadores 104 suplitorios pueden descifrar los datos 134 importantes confidenciales que usan los datos 133 confidenciales conocidos por el autenticado 103 suplitorio y el autenticador 104 suplitorio, mientras se informa al autenticador 104 suplitorio de los datos importantes confidenciales 132. El autenticador 104 suplitorio proporciona los datos 132 importantes confidenciales al autenticador 102 que informa los datos importantes confidenciales 132 al autenticador 102. Los autenticadores 104 suplitorios pueden proporcionar en retorno potencialmente los datos 132 importantes confidenciales al autenticador 102 en el mismo mensaje que fue usado para transferir la respuesta 135 al autenticador 102. En esta fase, el autenticado 101 y el autenticador 102 tienen el acceso a los datos importantes confidenciales 132. Estos datos importantes

confidenciales 132 pueden usarse así para autenticarnos en las comunicaciones subsecuentes independientes del autenticado 103 supletorio y el autenticador 104 supletorio.

[0035] El autenticador 102 proporciona la respuesta 135 al autenticador 101 como lo representado por la flecha 117. Los autenticados 101 pueden usar la respuesta 135 entonces para autenticar el autenticador 102. Hay varias maneras diferentes en que los autenticados 101 pueden hacer esto.

[0036] En un ejemplo, los autenticados 101 pueden adquirir una respuesta al desafío del autenticado 103 supletorio, potencialmente al mismo tiempo y de la misma manera como el desafío fue adquirido del autenticado 103 supletorio. Los autenticados 101 pueden entonces coincidir la respuesta como lo adquirido del autenticado 103 supletorio con la respuesta como lo proporcionado por el autenticador 102. Una coincidencia produce en el autenticador 102 la autenticación para el autenticado 101.

[0037] Alternativamente, los autenticados 101 podrían delegar esta comparación al autenticado 103 supletorio proporcionando la respuesta 135 como lo proporcionado por el autenticador 102 al autenticado 103 supletorio. Los autenticados 103 supletorios pueden coincidir la respuesta entonces como lo proporcionado por el autenticado 101 con la respuesta que generó internamente. Si una coincidencia se encuentra, los autenticados 103 supletorios pueden indicar al autenticado 101 que esa autenticación tiene el éxito.

[0038] En concordancia, en esta fase, el autenticador 102 ha autenticado al autenticado 101, y la demanda de servicio puede honrarse si es apropiado. La autenticación es desafío-basado, y no requiere que el autenticado 101 o el autenticador 102 tengan acceso a los datos 133 confidenciales generados en una respuesta al desafío. Además, en la personalización de comunicaciones privada subsiguiente, el autenticador 102 y el autenticado 101 pueden autenticar en comunicaciones subsecuentes que usan los datos importantes confidenciales 132, en lugar de repetir el proceso descrito anteriormente.

[0039] En lugar de asegurar simplemente la comunicación subsecuente basada en los datos importantes confidenciales 132, las comunicaciones subsecuentes que usan un compendio de los datos importantes confidenciales 132 entre uno o más artículos pueden afianzarse. El compendio puede usarse para afianzar las comunicaciones subsecuentes entre el autenticado 101 y el autenticador 102. El compendio también puede ser basado en el desafío 131 y/o la respuesta 135. Además, el compendio puede incluir datos 136 comunicados entre el autenticador 101 y el autenticado 102 que tampoco se comunican al autenticado 103 supletorio o al autenticador 104 supletorio. El autenticado 101 y el autenticador 102 pueden luego comunicarse usando el compendio para afianzar las comunicaciones. Cuando el compendio es en parte basado en los datos 136 que no conoce el autenticado 103 supletorio y el autenticador 104 supletorio, el autenticado 103 supletorio y el autenticador 104 supletorio se previenen fácilmente de escuchar detrás de las puertas (eavesdropping) o de engañarse (spoofing) en las comunicaciones subsecuentes entre el autenticador 101 y el autenticado 102.

[0040] En una personalización, el autenticador 102 genera también datos importantes confidenciales 137 que se proporcionan al autenticador 104 supletorio. El autenticador 104 supletorio encripta los datos importantes confidenciales 137, y pasa los datos importantes confidenciales encriptados al autenticador 102. El autenticador 102 entonces pasa los datos importantes confidenciales encriptados al autenticado 101 que usa el autenticado 103 supletorio para descifrar la clave 137 confidencial que usa los datos 131 confidenciales. El compendio puede ser basado entonces también en esta clave 137 confidencial.

[0041] En concordancia, un mecanismo de autenticación desafío-basado se ha descrito en las partes directas a la autenticación (es decir, el autenticador y el

136

137

autenticado de las entidades de cómputo) no necesario calcular una respuesta a un desafío, ni tiene conocimiento de datos confidenciales usados en la autenticación inicial. Además, el autenticador y el autenticado de la entidad de cómputo que pueden autenticarse como consecuencia y pueden comunicarse independientemente del autenticador suplitorio y del autenticado suplitorio de las entidades de cómputo.

[0042] En la personalización ilustrada en la Figura 1, hay varios canales de comunicación, uno entre el autenticado 101 y el autenticado 103 suplitorio (después también potencialmente llamado "el canal autenticado"), uno entre el autenticador 102 y el autenticador 104 suplitorio (después también potencialmente llamado el "cauce del autenticador"), y uno entre el autenticado 101 y el autenticador 102 (después también potencialmente llamado el "canal de autenticación"). Si las dos entidades de cómputo están dentro del mismo dispositivo o sistema de cómputo, el canal correspondiente puede ser una llamada de la función o el mecanismo del mensaje local. Sin embargo, si las dos entidades de cómputo se localizan remotamente, el canal correspondiente puede usar un protocolo de gestión de redes.

[0043] Por ejemplo, si las dos entidades de cómputo se localizan por dominios de transporte-nivelados diferentes, un protocolo de red transporte-independiente puede usarse para comunicarse. Un protocolo de la red transporte-independiente es conocido en el arte como Servicios WEB "Web Services" usa el Protocolo de Acceso de Objeto Simple (SOAP) que cubre para llevar la información de una manera transporte-independiente. Los Servicios Web también pueden emplear SOAP socavando para transportar a través de redes que no soportan SOAP directamente.

[0044] De acuerdo con un aspecto de la invención, una modificación a los Servicios Web convencionales puede emplearse para llevar la información importante a la autenticación. Por ejemplo, un encabezado de SOAP puede incluir un encabezado firmado de SOAP como el descrito en la aplicación 60/515,461 provisional de los Estados Unidos incorporada anteriormente por referencia. La Figure 2 esquemáticamente ilustra una estructura de SOAP tal que cubre convenientemente para realizar la facturación y firma en el contexto de Servicios Web. La cubierta SOAP 200 incluye los encabezados SOAP 201 y el cuerpo de SOAP 202. Los encabezados de SOAP incluyen los encabezados de facturación 211, encabezados de firma 212, entre potencialmente otros encabezados 213. Los encabezados de firma 212 pueden incluir la información para la autenticación. Por ejemplo, el desafío 131, la clave confidencial 132, las claves confidenciales encriptadas 134 y 137, la respuesta 135, y los datos 136 así como cualquier otra información útil puede ser incluida en los encabezados de firma 212. Sin embargo, los principios de la invención presente no se limitan a la comunicación que usa los Servicios de Web. Puede ser que ninguno del autenticado, autenticador, o los canales de autenticación usen los Servicios Web en una personalización particular.

[0045] Una vez la autenticación se ha completado, el autenticado 101 está ahora en una posición para tomar una decisión más inteligente sin importar si la autorización del servicio ha sido proporcionada por el autenticador 102. Desde que el proceso tiene este estado de progreso más allá de la autenticación a la autorización, las entidades de cómputo 101 a través de la 104 cada una en la descripción subsiguiente de los gráficos para ser referidos simplemente como una "entidad de cómputo".

[0046] Para autorizar un servicio pedido, la entidad de cómputo 101 puede requerir como una condición para tal autorización el pago o traslado de artículos transferibles electrónicamente de la entidad de cómputo. En esta descripción y en las demandas, un "artículo electrónicamente" transferible es cualquier artículo, físico o electrónico cuya propiedad puede transferirse de una entidad a otra enviando un mensaje electrónico. La necesidad del mensaje electrónico no es

61

completamente electrónico durante el traslado, pero puede emprender otras formas como las formas ópticas durante el traslado. Tales artículos transferibles pueden incluir dinero. Sin embargo, los artículos transferibles también pueden incluir cualquier otro artículo que es electrónicamente transferible. Por ejemplo, los artículos pueden ser millas de viajero frecuentes, películas o créditos de boleto de ópera, boletos del tren, la autoridad de registro de clase, etc. Igualmente para realizar el servicio pedido, la entidad de cómputo 101 puede transferir los artículos transferibles electrónicamente a la entidad de cómputo 102.

[0047] La figura 3 ilustra el ambiente de la Figura 1 en la cual hay cuatro entidades de cómputo 301 a través de 304. Las entidades de cómputo 301 a través de 304 pueden ser igual que lo descrito anteriormente para computar entidades 101 a través de 104, aunque esto no se requiere. Las entidades de cómputo 301 y 303 están en una esfera de confianza representada por el área dentro de las líneas punteadas. Las entidades de cómputo 302 y 304 están en otra esfera de confianza representada por el área dentro de las líneas punteadas. Las entidades de cómputo 303 y 304 están todavía dentro de otra esfera de confianza como lo representado en el área dentro de las líneas punteadas.

[0048] La figura 3 también muestra un flujo del mensaje que muestra una manera de transferir los artículos transferibles electrónicamente entre las entidades de cómputo 301 y 302. La entidad de cómputo 304 tiene la autorización de información 321 pertinente independientemente de si la entidad de cómputo 302 pueden transferir los artículos particulares a la entidad de cómputo 301. Por ejemplo, si la entidad de cómputo 302 es una tarjeta SIM, los artículos a ser transferidos pueden ser, por ejemplo, dinero.

[0049] El flujo del mensaje muestra cómo los artículos pueden ser autorizados para ser transferidos y entonces realmente podrían transferirse de la entidad de cómputo 302 a la entidad de cómputo 301. Para autorizar el traslado, la entidad de cómputo 301 puede indagar (vea flecha 311) de la entidad de cómputo 303 acerca de si o no la entidad de cómputo 302 tiene la autorización para transferir los artículos. Si la entidad de cómputo 303 no sabe, la entidad de cómputo 303 hará la pregunta (vea flecha 312) a la entidad de cómputo 304 acerca de si o no la entidad de cómputo 302 esta autorizada para hacer el traslado. Si la entidad de cómputo 304 no sabe, la entidad de cómputo 304 hará la pregunta (vea flecha 313) a la entidad de cómputo 302 para hacer el traslado. La entidad de cómputo 302 puede responder (vea flecha 314) afirmativo. Al recibir este mensaje, si la entidad de cómputo 304 había sido pre-autorizada para hacer el cargo debido a la comunicación anterior con la entidad de cómputo 302, entonces la entidad de cómputo 304 responde (vea flecha 315) afirmativo. Al recibir este mensaje, si la entidad de cómputo 303 había sido pre-autorizada para hacer el cargo debido a la comunicación anterior con la entidad de cómputo 304, entonces la entidad de cómputo 303 responde (vea flecha 316) afirmativo. Las confirmaciones afirmativas representadas por flechas 314 a través de la 316 también pueden incluir traslado electrónico de los artículos, o un acuerdo para dar autorización al traslado en un momento posterior.

[0050] Una personalización alternativa de traslado se ilustra en la Figura 4. En esta personalización, la entidad de cómputo 402 demanda (vea flecha 411) que el traslado de artículos se haga. La entidad de cómputo 404 responde (vea flecha 412) con una aprobación para transferir los artículos (vea flecha 412) y entonces los débitos de una cuenta por los artículos puede ser transferido. La aprobación para transferir que usa los datos confidenciales 433 conocidos a las entidades de cómputo 403 y 404 pueden encriptarse, pero no a las entidades de cómputo 401 y 402. La entidad de cómputo 402 proporciona luego la aprobación encriptada (vea flecha 413) a la entidad de cómputo 401, que entonces proporciona la aprobación encriptada (vea flecha 414) a la entidad de cómputo 403. La entidad de cómputo descifra la aprobación que usa los datos confidenciales 433 y entonces acredita la cuenta de la entidad de cómputo 401 del usuario entidad de cómputo 401 en la cantidad de los artículos a transferir. En una conciliación subsiguiente o en

tiempo-real, la entidad de cómputo 403 puede adquirir un crédito para los artículos transferidos de la entidad de cómputo 404.

139

[0051] Así, la transferencia electrónica de los artículos transferibles son hechos desde la entidad de cómputo 402 (o su usuario) a la entidad de cómputo 401 (o su usuario). Transferir en la otra dirección de la entidad de cómputo 401 a la entidad de cómputo 402 puede lograrse de la misma manera como lo descrito anteriormente sólo en el la dirección simétricamente opuesta.

[0052] La invención presente puede ser incluida en otras formas específicas sin partir desde las características esenciales de su espíritu. Las personalizaciones descritas sólo serán consideradas en todo los aspectos como ilustrativo y no restrictivo. El alcance de la invención, por consiguiente, se indica por las demandas añadidas en lugar de por la descripción anterior. Todos los cambios, que vienen dentro del significado y rango de equivalencia de las demandas, será cubierto dentro de su alcance.

[0053] Lo que se exige y se desea con seguridad por las Cartas Patentes de los Estados Unidos es:

1. En un ambiente que incluye una entidad de cómputo autenticada, una entidad de cómputo suplente, un autenticador de la entidad de cómputo, y un autenticador supletorio de entidad de cómputo, un método para el autenticador de la entidad de cómputo para autenticar al autenticado de la entidad de cómputo que usa el desafío-basado en la autenticación y sin requerir que el autenticado y autenticador de las entidades de cómputo sean conscientes de los datos confidenciales usados para la autenticación, el método comprende lo siguiente:

Un acto de la entidad de cómputo autenticada que adquiere un desafío del autenticado supletorio de la entidad de cómputo;

Un acto del autenticado de la entidad de cómputo que proporciona el desafío al autenticador de la entidad de cómputo;

Un acto del autenticador de la entidad de cómputo que adquiere una respuesta al desafío del autenticador supletorio de la entidad de cómputo;

Un acto del autenticador de la entidad de cómputo que proporciona la respuesta al autenticado de la entidad de cómputo; y

Un acto del autenticado de la entidad de cómputo que usa la respuesta para autenticar el autenticador de la entidad de cómputo.

2. Un método de acuerdo con la Demanda 1, en donde el acto del autenticado de la entidad de cómputo que adquiere un desafío del autenticado supletorio de la entidad de cómputo comprende lo siguiente:

Un acto del autenticado de la entidad de cómputo que proporciona una demanda del desafío al autenticado supletorio de la entidad de cómputo;

Un acto del autenticado supletorio de la entidad de cómputo que genera un desafío en la contestación a la demanda del desafío; y

Un acto del autenticado supletorio de la entidad de cómputo que proporciona el desafío al autenticado de la entidad de cómputo en la contestación a la demanda.

3. Un método de acuerdo con la Demanda 2, en donde el acto del autenticador de la entidad de cómputo que adquiere una respuesta al desafío del autenticador supletorio de la entidad de cómputo comprende lo siguiente:

Un acto del autenticador de la entidad de cómputo que proporciona el desafío al autenticador supletorio de la entidad de cómputo; y

Un acto del autenticador supletorio de la entidad de cómputo que determina una respuesta al desafío; y

Un acto del autenticador supletorio de la entidad de cómputo que proporciona la respuesta al autenticador de la entidad de cómputo.

4. Un método de acuerdo con la Demanda 1, comprendiendo más allá lo siguiente:

2A

Un acto de la entidad de cómputo autenticada que adquiere una respuesta al desafío del autenticado suplitorio de la entidad de cómputo, en qué, el acto del autenticado de la entidad de cómputo que usa la respuesta para autenticar el autenticador de la entidad de cómputo comprende lo siguiente:

Un acto de la entidad de cómputo autenticada que coincide la respuesta como fue adquirida por el autenticado suplitorio de la entidad de cómputo con la respuesta proporcionada por el autenticador de la entidad de cómputo.

5. Un método de acuerdo con Demanda 1, en donde el acto del autenticado de la entidad de cómputo que usa la respuesta para autenticar el autenticador de la entidad de cómputo comprende lo siguiente:

Un acto del autenticado de la entidad de cómputo que proporciona la respuesta al autenticado suplitorio de la entidad de cómputo; y

Un acto del autenticado suplitorio de la entidad de cómputo que proporcionó al autenticado de la entidad de cómputo una indicación de la respuesta proporcionada por el autenticador de la entidad de cómputo es una respuesta apropiada para el desafío adquirido del autenticado suplitorio de la entidad de cómputo.

6. Un método de acuerdo con la Demanda 1, que comprende además:

Un acto del autenticado de la entidad de cómputo generando una clave secreta de datos que no se conocen por el autenticado suplitorio, el autenticador o autenticador suplitorio de las entidades de cómputo;

Un acto del autenticado de la entidad de cómputo que proporciona los datos importantes confidenciales al autenticado suplitorio de la entidad de cómputo que informa al autenticado suplitorio de la entidad de cómputo de los datos confidenciales importantes;

Un acto del autenticado suplitorio de la entidad de cómputo que encripta los datos importantes confidenciales usando datos confidenciales conocidos por el autenticado suplitorio y el autenticador suplitorio de las entidades de cómputo, pero no conocido por el autenticado y autenticador de las entidades de cómputo;

Un acto del autenticado suplitorio de la entidad de cómputo que proporciona los datos importantes confidenciales encriptados al autenticado de la entidad de cómputo;

Un acto del autenticado de la entidad de cómputo que proporciona los datos importantes confidenciales encriptados al autenticador de la entidad de cómputo;

Un acto del autenticador de la entidad de cómputo que proporciona los datos importantes confidenciales encriptados por el autenticador suplitorio de la entidad de cómputo;

Un acto del autenticador suplitorio de la entidad de cómputo que descifra los datos importantes confidenciales usando los datos confidenciales conocidos por el autenticado suplitorio y el autenticador suplitorio de las entidades de cómputo que informan al autenticador suplitorio de la entidad de cómputo de los datos importantes confidenciales;

Un acto del autenticador suplitorio de la entidad de cómputo que proporciona los datos importantes confidenciales al autenticador de la entidad de cómputo que informa el autenticador de la entidad de cómputo de los datos importantes confidenciales.

7. Un método de acuerdo con la Demanda 6, comprendiendo además lo siguiente:

Un acto del autenticado y el autenticador de las entidades de cómputo que se comunican usando mensajes que están al menos parcialmente asegurados usando parcialmente los datos importantes confidenciales.

8. Un método de acuerdo con la Demanda 6, en donde el acto del autenticado de la entidad de cómputo que proporciona el desafío al autenticador de la entidad de cómputo y el acto del autenticado de la entidad de cómputo que proporciona los datos importantes confidenciales encriptados por el autenticador de la entidad de cómputo son realizados por el autenticado de la entidad de cómputo que proporciona un solo mensaje que incluye el desafío y los datos

importantes confidenciales encriptados para el autenticador de la entidad de cómputo.

9. Un método de acuerdo con la Demanda 6, comprendiendo además lo siguiente:

Un acto del autenticado de la entidad de cómputo que genera un compendio de los datos importantes confidenciales combinados con uno o más artículos de los datos;

Un acto del autenticador de la entidad de cómputo que también genera el compendio de los datos importantes confidenciales combinados con uno o más artículos de los datos; y

Un acto del autenticado y autenticador de las entidades de cómputo que se comunican usando mensajes que se afianzan usando parcialmente al menos el compendio.

10. Un método de acuerdo con la Demanda 9, en donde uno o más artículos de datos incluyen el desafío.

11. Un método de acuerdo con la Demanda 10, en donde uno o más artículos de datos incluyen la respuesta.

12. Un método de acuerdo con la Demanda 11, en donde los datos importantes confidenciales son los primeros datos importante confidenciales, en donde uno o más artículos de datos incluyen los segundos datos importantes confidenciales conocidos por el autenticado y autenticador de las entidades de cómputo, pero no conocidos por el autenticado supletorio y el autenticador supletorio que de las entidades de cómputo.

13. Un método de acuerdo con la Demanda 9, en donde uno o más de otros artículos de datos incluyen la respuesta.

14. Un método de acuerdo con la Demanda 13, en donde los datos importantes confidenciales son los primeros datos importante confidenciales, en donde uno o más de otros artículos de datos incluyen los segundos datos importantes confidenciales conocidos por el autenticado y el autenticador de las entidades de cómputo, pero no conocidos por el autenticado supletorio y el autenticador supletorio de las entidades de cómputo.

15. Un método de acuerdo con la Demanda 9, en donde los datos importantes confidenciales son los primeros datos importantes confidenciales, en donde uno o más de otros artículos de datos incluyen los segundos datos importantes confidenciales conocidos por el autenticado y el autenticador de las entidades de cómputo, pero no conocidos por el autenticado supletorio y el autenticador supletorio de las entidades de cómputo.

16. Un método de acuerdo con la Demanda 6, en donde los datos importantes confidenciales son los primeros datos importantes confidenciales, el método además comprende:

Un acto del autenticador de la entidad de cómputo que genera los segundos datos importantes confidenciales;

Un acto del autenticador de la entidad de cómputo que proporciona los segundos datos importantes confidenciales para el autenticador supletorio de entidad de cómputo;

Un acto del autenticador supletorio de la entidad de cómputo que encripta los segundos datos importantes confidenciales usando los datos confidenciales conocidos por el autenticado supletorio y el autenticador supletorio de las entidades de cómputo;

Un acto del autenticador supletorio de la entidad de cómputo que proporciona los segundos datos importantes confidenciales encriptados para el autenticador de la entidad de cómputo;

Un acto del autenticador de la entidad de cómputo que proporciona los segundos datos importantes confidenciales al autenticado que computa la entidad;

142

un acto del autenticado de la entidad de cómputo que proporciona los encriptados segundos datos importantes confidenciales encriptados para el autenticador suplente de la entidad de cómputo;

Un acto del autenticado suplente de la entidad de cómputo que descifra los segundos datos importantes confidenciales encriptados que usan los datos confidenciales conocidos para el autenticado suplente y el autenticador suplente de las entidades de cómputo; y

Un acto del autenticado suplente de la entidad de cómputo que proporciona los segundos datos importantes confidenciales al autenticado de la entidad de cómputo.

17. Un método de acuerdo con la Demanda 16, comprendiendo además lo siguiente:

Un acto del autenticado de la entidad de cómputo que genera un compendio de los primeros y segundos datos importantes confidenciales combinados con uno o más de otros artículos de datos;

Un acto del autenticador de la entidad de cómputo que también genera el compendio de los primeros y segundos datos importantes confidenciales combinados con uno o más de otros artículos de datos; y

Un acto del autenticado y autenticador de las entidades comunicándose usando mensajes que se aseguran usando parcialmente por lo menos el compendio.

18. Un método de acuerdo con la Demanda 17, en donde uno o más de otros artículos de datos incluyen el desafío.

19. Un método de acuerdo con la Demanda 18, en donde uno o más de otros artículos de datos incluyen la respuesta.

20. Un método de acuerdo con la Demanda 19, en donde uno o más de otros artículos de datos incluyen terceros datos importantes confidenciales conocidos por el autenticado y autenticador de las entidades de cómputo, pero no conocido por el autenticado suplente y el autenticador suplente de las entidades de cómputo.

21. Un método de acuerdo con la Demanda 17, en donde uno o más de otros artículos de datos incluyen la respuesta.

22. Un método de acuerdo con la Demanda 21, en donde uno o más de otros artículos de datos incluyen los terceros datos importantes confidenciales conocidos al autenticado y autenticador de las entidades, pero no conocidos por el autenticado suplente y el autenticador suplente de las entidades de cómputo.

23. Un método de acuerdo con la Demanda 17, en donde uno o más de otros artículos de datos incluyen los terceros datos importantes confidenciales conocidos por el autenticado y autenticador de las entidades de cómputo, pero no conocidos por el autenticado suplente y el autenticador suplente de las entidades de cómputo.

24. En un ambiente que incluye una entidad de cómputo autenticada, una entidad de cómputo suplente, una entidad de cómputo autenticador, y una entidad de cómputo del autenticador suplente, un método para la entidad de cómputo autenticado para autenticar el autenticador de la entidad de cómputo que usa el desafío basado en la autenticación y sin requerir que el autenticado y autenticador de las entidades de cómputo sean conscientes de los datos confidenciales usados para la autenticación, el método comprende a lo siguiente,:

U acto de adquirir un desafío del autenticado suplente de la entidad de cómputo;

Un acto de proporcionar el desafío al autenticador de la entidad de cómputo, en donde el autenticador de la entidad de cómputo adquiere una respuesta para el desafío del autenticador suplente de la entidad de cómputo;

Un acto de adquirir la respuesta del autenticador de la entidad de cómputo;
y

24

Un acto de usar la respuesta para autenticar el autenticador de la entidad de cómputo.

25. Un método de acuerdo con la Demanda 24, en donde el acto de adquirir un desafío del autenticado suplitorio de la entidad de cómputo comprende lo siguiente:

Un acto de proporcionar un requerimiento de desafío para el autenticado suplitorio de la entidad de cómputo; y

Un acto de adquirir una respuesta para la demanda del desafío del autenticado suplitorio de la entidad de cómputo.

26. Un método de acuerdo con la Demanda 24, que comprende además lo siguiente:

Un acto de adquirir una respuesta al desafío del autenticado suplitorio que de la entidad de cómputo, en donde,

El acto de usar la respuesta para autenticar el autenticador de la entidad de cómputo comprende lo siguiente:

Un acto de coincidir la respuesta como lo adquirido por el autenticado suplitorio de la entidad de cómputo con la respuesta como fue proporcionada por el autenticador de la entidad de cómputo.

27. Un método de acuerdo con la Demanda 24, en donde el acto de usar la respuesta para autenticar el autenticador de la entidad de cómputo comprende lo siguiente:

Un acto de proporcionar la respuesta para el autenticado suplitorio de la entidad de cómputo; y

Un acto de recibir del autenticado suplitorio de la entidad de cómputo una indicación de la respuesta proporcionada por el autenticador de la entidad de cómputo es una respuesta apropiada para el desafío adquirido por el autenticado suplitorio de la entidad de cómputo.

28. Un método de acuerdo con la Demanda 24, además comprende:

Un acto de generación de los datos clave confidenciales que no se conocen por el autenticado suplitorio, autenticador o autenticador suplitorio de las entidades de cómputo;

Un acto de proporcionar los datos importantes confidenciales al autenticado suplitorio de la entidad de cómputo que informa al autenticado suplitorio de la entidad de cómputo de los datos importantes confidenciales;

Un acto del autenticado suplitorio de la entidad de cómputo que encripta los datos importantes confidenciales que usan los datos confidenciales conocidos por el autenticado suplitorio y el autenticador suplitorio de las entidades de cómputo, pero no conocidos por el autenticado y autenticador de las entidades de cómputo;

Un acto de adquirir los datos importantes confidenciales encriptados del autenticado suplitorio de la entidad de cómputo, los datos importantes confidenciales encriptados que son los datos importantes confidenciales encriptados usando datos confidenciales conocidos por el autenticado suplitorio y el autenticador suplitorio de las entidades de cómputo, pero no conocidos por el autenticado y autenticador de las entidades de cómputo; y

Un acto de proporcionar los datos importantes confidenciales encriptados por el autenticador de la entidad de cómputo, en donde el autenticador de la entidad de cómputo proporciona los datos importantes confidenciales encriptados para el autenticador suplitorio de la entidad de cómputo para ser descifradas por el autenticador suplitorio de la entidad de cómputo, y recibe los datos importantes confidenciales.

29. Un método de acuerdo con la Demanda 28, comprendiendo además lo siguiente:

Un acto de comunicarse con el autenticador de la entidad de cómputo que usa mensajes que se afianzan usando parcialmente por lo menos los datos importantes confidenciales.

30. Un método de acuerdo con la Demanda 28, en donde el acto de proporcionar el desafío al autenticador de la entidad de cómputo y el acto de proporcionar los datos importantes confidenciales encriptados para el autenticador de la entidad de cómputo son realizados proporcionando un solo mensaje que incluye ambos: el desafío y los datos importantes confidenciales encriptados para el autenticador de la entidad de cómputo.

31. Un método de acuerdo con la Demanda 28, comprendiendo además lo siguiente:

Un acto de generar un compendio de los datos importantes confidenciales combinado con uno o más de los otros artículos de los datos;

Un acto de comunicación con el autenticador de la entidad de cómputo que usa mensajes que se afianzan usando parcialmente por lo menos el compendio.

32. Un programa de computadora para el uso en un ambiente que incluye una entidad de cómputo autenticada, una entidad de cómputo suplitorio, una entidad de cómputo autenticador, y una entidad de cómputo autenticador suplitorio, el producto de programa de computadora para llevar a cabo un método para la entidad de cómputo autenticada para autenticar la entidad de cómputo autenticador que usa el desafío basado en la autenticación y sin requerir que las entidades de cómputo autenticado y autenticador sean conscientes de los datos confidenciales usados para la autenticación, el producto del programa de computadora que comprende uno o más medios de comunicación legibles por computadora que tienen el conjunto de instrucciones ejecutables por la computadora que cuando son ejecutadas por la entidad de cómputo autenticada, causa la entidad de cómputo para realizar el método, el método comprende lo siguiente:

Un acto de adquirir un desafío de la entidad de cómputo autenticada suplitoria;

Un acto de proporcionar el desafío para la entidad de cómputo autenticador, en donde la entidad de cómputo autenticador adquiere una respuesta al desafío de la entidad de cómputo autenticador suplitoria;

Un acto de adquirir la respuesta de la entidad de cómputo autenticador; y

Un acto de usar la respuesta para que la entidad de cómputo autentique el autenticador.

33. Un producto de programa de computadora de acuerdo con la Demanda 32, en donde el acto de adquirir un desafío del autenticado suplitorio de la entidad de cómputo comprende lo siguiente:

Un acto de proporcionar una demanda del desafío al autenticado suplitorio de la entidad de cómputo; y

Un acto de adquirir una respuesta a la demanda del desafío del autenticado suplitorio de la entidad de cómputo.

34. Un producto de programa de computadora de acuerdo con Demanda 33, en donde el método más allá comprende a lo siguiente:

un acto de adquirir una respuesta al desafío del autenticado suplitorio que computa la entidad, en qué,

el acto de usar la respuesta para autenticar el autenticador que computa la entidad comprende a lo siguiente:

un acto de coincidir la respuesta como adquirido del autenticado suplitorio que computa la entidad con la respuesta como con tal de que por el autenticador que computa la entidad.

35. Un producto de programa de computadora de acuerdo con la Demanda 32, en donde el acto de usar la respuesta para autenticar el autenticador de la entidad de cómputo comprende lo siguiente:

Un acto de proporcionar la respuesta al autenticado suplitorio de la entidad de cómputo; y

Un acto de recibir del autenticado suplitorio de la entidad de cómputo una indicación de que la respuesta proporcionada por el autenticador de la entidad de

145
cómputo es una respuesta apropiada para el desafío adquirido desde el autenticado supletorio de la entidad de cómputo.

36. Un producto de programa de computadora de acuerdo con la Demanda 32, en donde el método además comprende:

Un acto de la generación de los datos importantes confidenciales que no se conocen por el autenticado supletorio, autenticador o autenticador supletorio de las entidades de cómputo;

Un acto de proporcionar los datos importantes confidenciales al autenticado supletorio de la entidad de cómputo que informa al autenticado supletorio de la entidad de cómputo de los datos importantes confidenciales;

Un acto del autenticado supletorio de la entidad de cómputo que encripta los datos importantes confidenciales que usa los datos confidenciales conocidos para las entidades de cómputo autenticado supletorio y autenticador supletorio, pero no conocidos por las entidades de cómputo autenticado y autenticador que computan las entidades;

Un acto de adquirir datos importantes confidenciales encriptados del autenticado supletorio de la entidad de cómputo, los datos importantes confidenciales encriptados que son los datos importantes confidenciales encriptados usando datos confidenciales conocidos por el autenticado supletorio y por el autenticador supletorio de las entidades de cómputo, pero no conocidos por las entidades de cómputo autenticado y autenticador; y

Un acto de proporcionar los datos importantes confidenciales encriptados para la entidad de cómputo autenticador, en donde la entidad de cómputo autenticador proporciona los datos importantes confidenciales encriptados para la entidad de cómputo autenticador supletorio para la descencipción por la entidad de cómputo autenticador supletorio, y recibe los datos importantes confidenciales.

37. Un producto de programa de computadora de acuerdo con la Demanda 36, en donde el método además comprende lo siguiente:

Un acto de comunicarse con el autenticador de la entidad de cómputo que usa mensajes que se afianzan usando parcialmente por lo menos los datos importantes confidenciales.

38. Un producto de programa de computadora de acuerdo con la Demanda 36, en donde el acto de proporcionar el desafío a la entidad de cómputo autenticador y el acto de proporcionar los datos importantes confidenciales encriptados para la entidad de cómputo autenticador que sean realizados proporcionando un solo mensaje que incluye el desafío y los datos importantes confidenciales encriptados para la entidad de cómputo autenticador.

39. Un producto de programa de computadora de acuerdo con la Demanda 36, en donde el método además comprende lo siguiente:

Un acto de generar un compendio de los datos importantes confidenciales combinado con uno o más de otros artículos de los datos;

Un acto de comunicarse con la entidad de cómputo autenticador que usa mensajes que se afianzan usando parcialmente por lo menos el compendio.

40. Un producto de programa de computadora de acuerdo con la Demanda 36, en donde uno o más medios legibles por computadora son medios físicos.

77

RESUMEN DEL DESCUBRIMIENTO

Un desafío basado en el mecanismo de autenticación que no requiere que la autenticación de las entidades de cómputo sean concientes de los datos confidenciales usados por la autenticación inicial. Una entidad de cómputo autenticador es para autenticar a la entidad de cómputo autenticada. Primero, la entidad de cómputo autenticada adquiere un desafío de la entidad de cómputo suplitorio autenticada. La entidad de cómputo autenticada proporciona un desafío para la entidad de cómputo autenticador, la cual tiene una entidad de cómputo autenticador suplitorio que resuelve el desafío. La entidad de cómputo autenticador envía la respuesta a la entidad de cómputo autenticada, la cual usa la respuesta para autenticar la entidad de cómputo autenticador.

147

PA 1229631



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

September 27, 2004

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: 60/515,461

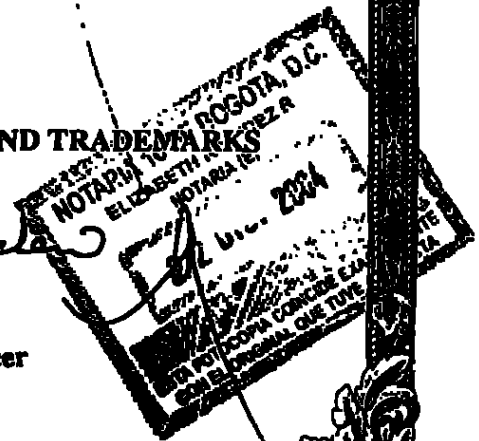
FILING DATE: October 29, 2003

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS



L. Edelen

L. EDELEN
Certifying Officer



15541 U.S. PTO

Please type a plus sign (+) inside this box



PTO/5916 (5-03)
Approved for use through 04/30/2003. OMB 0851-0032
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.63(c).

INVENTOR(S)					
Given Name (first and middle (if any))		Family Name or Surname		Residence (City and either State or Foreign Country)	
Max G. Christopher G.		Morris Kaler		Seattle, Washington Bainbridge, Washington	
☐ Additional inventors are being named on the _____ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (250 characters max)					
WEB SERVICES FOR BILLING AND SIGNING					
Direct all correspondence to: CORRESPONDENCE ADDRESS					
☒ Customer Number <u>022913</u> Place Customer Number Bar Code Label here					
OR Type Customer Number here					
☒ Firm or Individual Name <u>WORKMAN NYDEGGER</u>					
Address <u>1000 Eagle Gate Tower</u>					
Address <u>80 East South Temple</u>					
City <u>Salt Lake City</u>		State <u>UT</u>	ZIP <u>84111</u>		
Country <u>USA</u>		Telephone <u>801-533-8800</u>	Fax <u>801-328-1707</u>		
ENCLOSED APPLICATION PARTS (check all that apply)					
☒ Specification Number of Pages <u>23</u>		☐ CD(s), Number <u> </u>			
☐ Drawing(s) Number of Sheets <u> </u>		☐ Other (specify) <u> </u>			
☐ Application Data Sheet. See 37 CFR 1.76					
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)					
☒ A check or money order is enclosed to cover the filing fees				FILING FEE AMOUNT (\$) <u>\$160.00</u>	
☒ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number <u>23-3178</u>					
☐ Payment by credit card. Form PTO-2038 is attached.					
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,

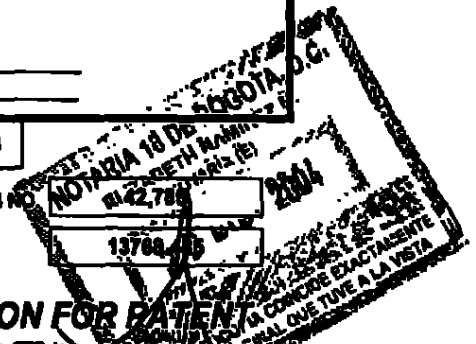
SIGNATURE

TYPED or PRINTED NAME ADRIAN J. LEE

TELEPHONE 801-533-8800

Date 10/28/03

REGISTRATION NO.
(if appropriate)
Docket Number: 13788-115



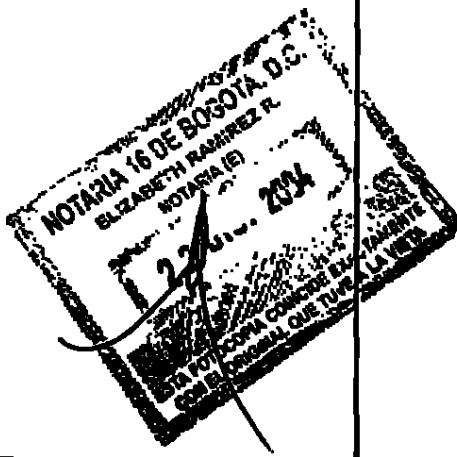
USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering information and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1460, Alexandria, VA 22313-1460. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PYLADEMENTS

149

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): Max G. Morris, et al.			Docket No. 13768.485
Serial No. Not Yet Assigned	Filing Date October 29, 2003	Examiner Not Yet Assigned	Group Art Unit Not Yet Assigned
Invention: WEB SERVICES FOR BILLING AND SIGNING			
I hereby certify that the following correspondence: Provisional Cover Sheet (1 page); Provisional Transmittal (1 Page); Provisional Application (23 pages); Check No.: 134173 for \$160.00; Postcard <i>(Identify type of correspondence)</i> is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on <u>October 29, 2003</u> <i>(Date)</i> <u>ADRIAN J. LEE</u> <i>(Typed or Printed Name of Person Mailing Correspondence)</i> <u></u> <i>(Signature of Person Mailing Correspondence)</i> <u>EV 302233329 US</u> <i>("Express Mail" Mailing Label Number)</i> Note: Each paper must have its own certificate of mailing. 			

FOR REVIEW

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>	Application Number	Not Yet Assigned
	Filing Date	October 29, 2003
	First Named Inventor	Max G. Morris
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Total Number of Pages in This Submission	Attorney Docket Number	13768.485

ENCLOSURES (check all that apply)		
☐ Fee Transmittal Form	☐ Drawing(s)	☐ After Allowance communication to Group
☒ Fee Attached	☐ Licensing-related Papers	☐ Appeal Communication to Board of Appeals and Interferences
☐ Amendment / Reply	☐ Petition	☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
☐ After Final	☐ Petition to Convert a Provisional Application	☐ Proprietary Information
☐ Affidavit/Declaration(s)	☐ Power of Attorney, Revocation Change of Correspondence	☐ Status Letter
☐ Extension of Time Request	☐ Terminal Disclaimer	☒ Other Enclosure(s) (please identify below):
☐ Express Abandonment Request	☐ Request for Refund	☐ Provisional Application
☐ Information Disclosure Statement	☐ CD, Number of CD(s) _____	☐ Provisional Cover Sheet
☐ Certified Copy of Priority Document(s)	Remarks	
☐ Response to Missing Parts/Incomplete Application		
☐ Response to Missing Parts under 37 CFR 1.62 or 1.63		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or individual name	ADRIAN J. LEE WORKMAN NYDEGGER
Signature	
Date	October 29, 2003

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			
Typed or printed name		Date	
Signature			

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to be (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time may vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9198 and select option 2.

151

UNITED STATES PROVISIONAL PATENT APPLICATION

of

Max G. Morris

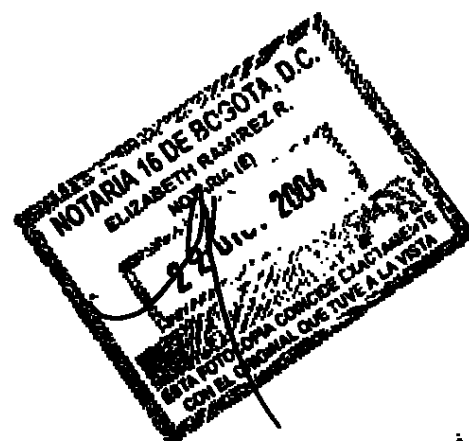
and

Christopher G. Kaler

for

WEB SERVICES FOR BILLING AND SIGNING

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



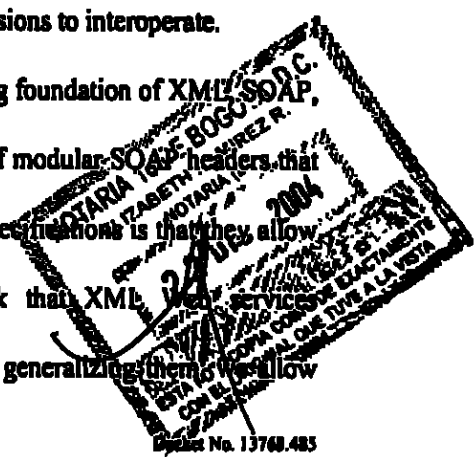
152

BACKGROUND OF THE INVENTION

[0001] Computing technology has transformed the way we work and play. Much of the functionality of computing systems is derived from the ability of computing systems to communicate one with another over a network. Computing systems are now commercially available in a wide variety of forms including desktop computers, laptop computers, Personal Digital Assistants (PDAs), tablet PCs, telephones, household devices and other forms. These computing systems have varying levels of mobility ranging from none whatsoever to being highly mobile. Regardless of the mobility, the use of such computing systems continues to grow and become ubiquitous. The functionality of such computing systems is greatly enhanced by their ability to communicate over networks with other computing systems. For example, e-mail, instant messaging, Web navigation, and many other common applications rely on network communication.

[0002] One conventional networking technology is often referred to as "Web Services". The Web Services architectures contains protocols and interfaces to enable secure reliable communications in an asynchronous messaging network that is vendor, platform, and device independent. The architecture is effective and supports composition with other standards to provide the functions that customers, software developers, platform providers, and mobile network operators need. The architecture is also extensible, thereby allowing the specifications to evolve and thereby allowing subsequent extensions to interoperate.

[0003] The Web Service specifications build on the existing foundation of XML, SOAP, and WSDL. The specifications typically provide for the use of modular SOAP headers that each accomplish specific tasks. The key advantage to these specifications is that they allow for protocol-level reuse to accomplish the common work that XML implementations do over and over. By separating them, and generalizing them, they allow



WORKMAN, NYDEGGER & SHELLEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

24

158

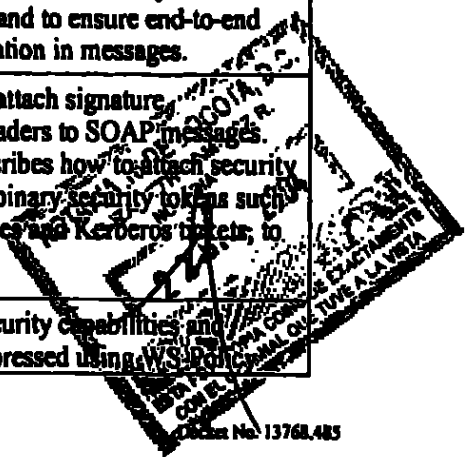
153

them to be optimized and combined for appropriate solutions rather than requiring a single monolithic protocol. As well, by using common building blocks we are more likely to achieve interoperability, increase productivity, increase performance, and increase reliability. The design principles used in these specifications are: general-purpose, standards-based, federated, and modular. The goals are to (respectively) be agnostic to application domain; achieve multi-vendor interoperability; avoid any central point of administration, control, and failure; and be factored to stand alone or work together.

[0004] The table below presents a summary of each specification organized by category:

	Specification	Summary
Description	WS-Policy	Describes a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of requirements, preferences, and capabilities of service interfaces.
	WS-PolicyAttachment	Describes a set of mechanisms for associating policies within WSDL, UDDI, or with arbitrary endpoints.
	WS-PolicyAssertions	Describes a base set of assertions about services using the framework described in WS-Policy.
Messaging	WS-Addressing	Describes a framework to identify Web service endpoints and to ensure end-to-end endpoint identification in messages.
Security	WS-Security	Describes how to attach signature and encryption headers to SOAP messages. In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages.
	WS-SecurityPolicy	Describes how security capabilities and constraints are expressed using WS-Policy.

WORKMAN, NYDEBUER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

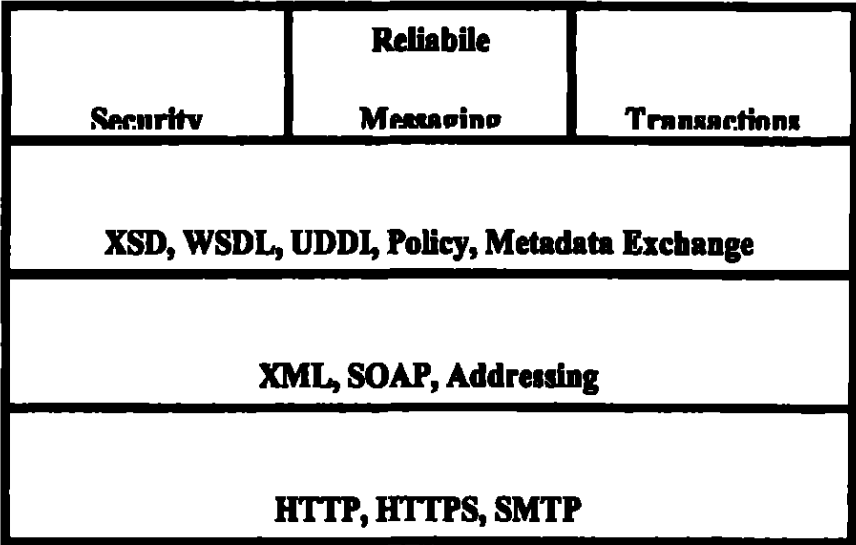


85

154

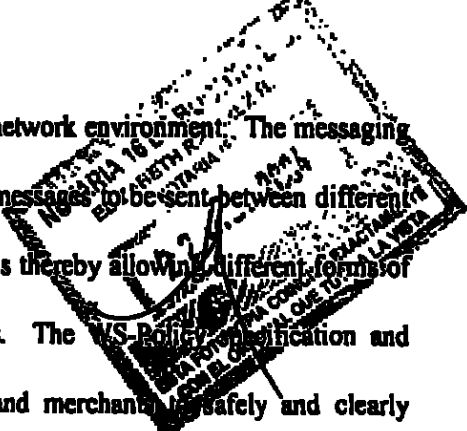
		(e.g. required security tokens, supported encryption algorithms, privacy rules).
	WS-Trust	Describes a framework for trust models that enables Web services to securely interoperate.
	WS-SecureConversation	Describes how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys.

[0005] The following diagram illustrates several key focus areas and their relationships:



[0006] This framework enables the description and interoperability of secure reliable transacted Web services in a synchronous or asynchronous messaging environment that is built on the XML foundations.

[0007] In the context of enabling commerce in a network environment: The messaging layer (e.g. WS-Addressing specification), allows for messages to be sent between different devices and intermediaries using a variety of protocols thereby allowing different forms of communication over a variety of physical mediums. The WS-Policy specification and related discovery specifications allows purchasers and merchants to safely and clearly



WORKMAN, NYDEGGER & SHELLEY
ATTORNEYS AT LAW
1800 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

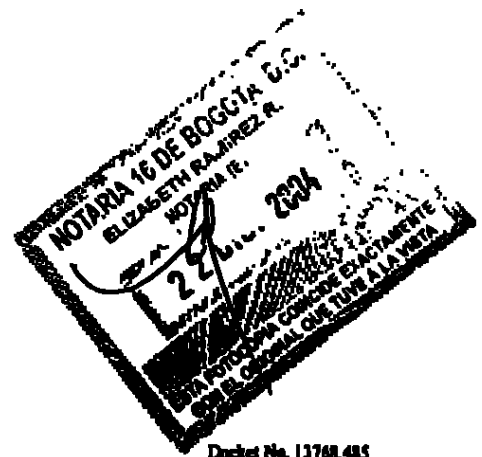
86

155

indicate their policies for communication and secure commerce. The WS-Security and WS-Trust specifications provide mechanisms for securing messages to and from the mobile Web services clients. When combined with WS-Federation and WS-SecureConversation, federated identities can have secure authenticated exchanges of messages. The WS-ReliableMessaging and WS-Transaction specifications complement the secure messaging infrastructure allowing, as desired, secure reliable transacted messages.

[0008] Accordingly, the Web Services architecture provides an effective platform for secure and reliable communications in a manner that is vendor, platform and device independent. Nevertheless, the Web Services architecture has limited ability to facilitate billing or signing related to commerce. Accordingly, what would be advantageous would be mechanisms for using the Web Services architecture to support billing and signing over a network. As mobile devices are becoming more popular for engaging in network commerce, it would be particularly advantageous if the mechanism supported commerce using mobile devices, while not being limited to application in a mobile environment.

WORKMAN, NYDEBUER & SERLE
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



- Page 5 -

Docket No. 13768.485

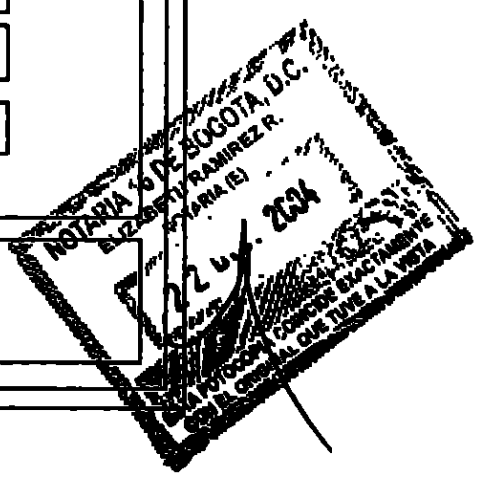
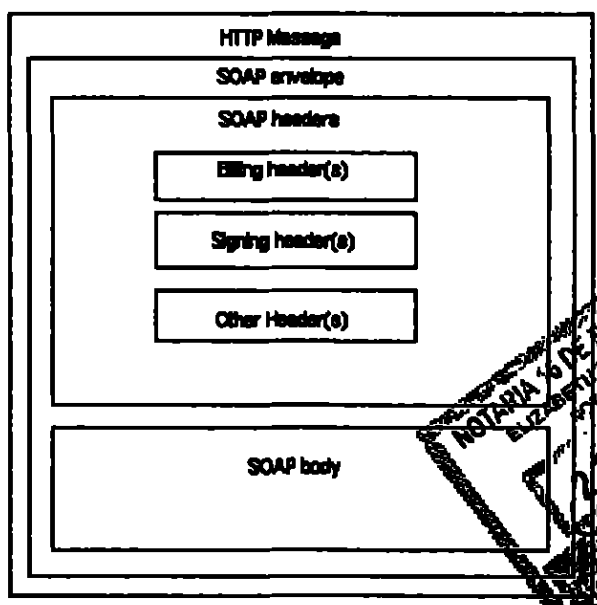
87

156

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0009] The principles of the present invention relate to the use of billing and signing information in a network message. In one embodiment, the billing and signing information are provided as additions to the Web Services specifications. In particular, the billing and signing information may be included as part of a Simple Object Access Protocol (SOAP) header. The exact form of the billing and signing information is not important for the principles of the present invention. Any structure for representing the billing and signing information will suffice so long as the computing systems that are communicating the information recognize a common schema so that the significance of the billing and signing information may be mutually recognized.

[0010] The following illustrates an electronic message in accordance with the principles of the present invention in which the billing and signing information is included as part of the SOAP header of a SOAP envelope. The SOAP envelope may be contained as part of, for example, a HyperText Transport Protocol (HTTP) message.



WURKMAN, NY DEGUEN & DESLOIS
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE CANYON TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

88

162
157

[0011] The SOAP headers include one or more header elements that include billing information, one or more headers that include signing information, and one or more other elements that represent headers defined by conventional Web Services specifications (e.g., WS-addressing, WS-Trust, WS-Policy, and the like). The billing and signing information may be provided in separate headers as illustrated, or in a single header.

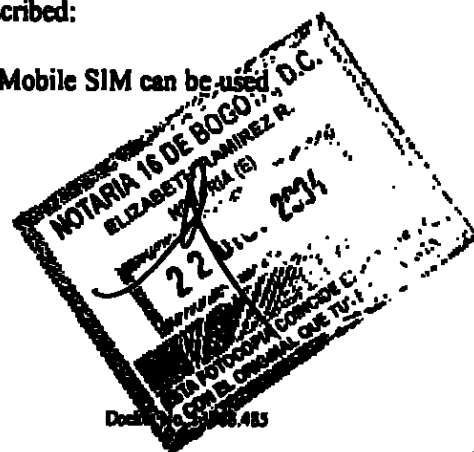
[0012] As previously mentioned, the exact structure of the billing and signing information is not important to the principles of the present invention. In addition, the precise naming of the data fields is also not important. However, the billing information may include for generalized billing including credit and debit functions that can operate in micro- and macro-payment environments as well as requesting and supplying quotes, invoices, and purchase orders. The signing information may include information for signing, escrow, notarizations, and audit recording for arbitrators.

[0013] The type of information represented by the billing and signing information may best be understood with reference to a number of commerce scenarios which are now described. Although specific scenarios are provided by way of illustration, the principles of the present invention are not limited to these specific scenarios, but apply to any scenarios in which the communication of billing and/or signing information may be useful.

[0014] Here is a brief overview of each scenario that will be described:

[0015] *Authentication using Mobile SIM* – Here we see how a Mobile SIM can be used to provide strong authentication for mobile Web services client.

WURMAN, AT & DONALDSON &
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



89

[0016] *Federated Access and Central Billing* – In this scenario the mobile Web services client is used to access federated data in different security domains and engage in m-commerce activities which are centrally billed to the mobile network operator.

[0017] *Mobile Wallet* – An alternative commerce scenario is described where the mobile Web services client is used as an electronic wallet.

[0018] *Electronic Ticket* – This scenario demonstrates commerce centered on the mobile Web services client as a common billing source. In this scenario the mobile Web services is used as a secure wallet.

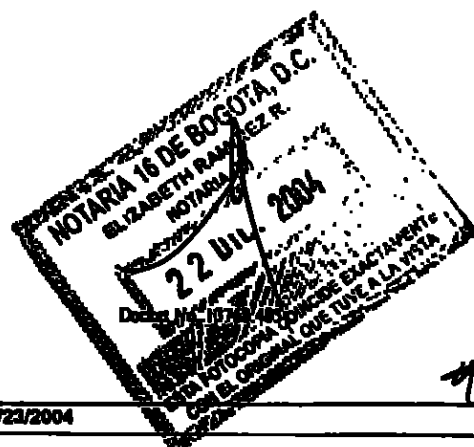
[0019] *Remote PIM* – A scenario is described where mobile users take advantage of federated PIM data across multiple mobile Web services clients.

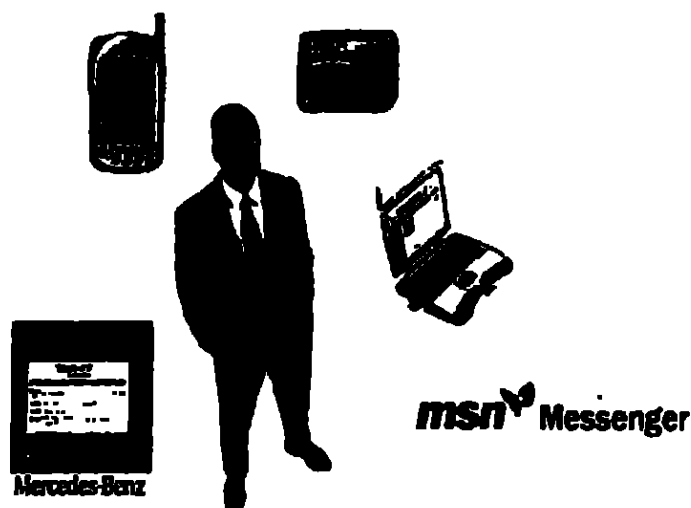
[0020] These four various scenarios will now be described in further detail.

Authentication using Mobile SIM

[0021] The mobile device provides a new option in authentication by providing a dynamic platform for access to principals. For mobile principals, there are now a variety of mechanisms for touching the principal such as cellular phones, PDAs, automotive PCs, instant messenger, wireless PCs, etc.

WOLKMAN, IV & ASSOCIATES, P.C.
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

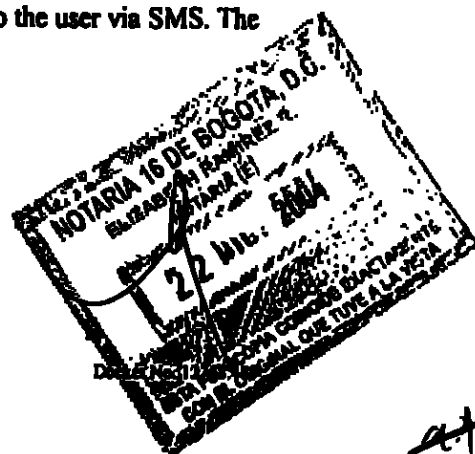


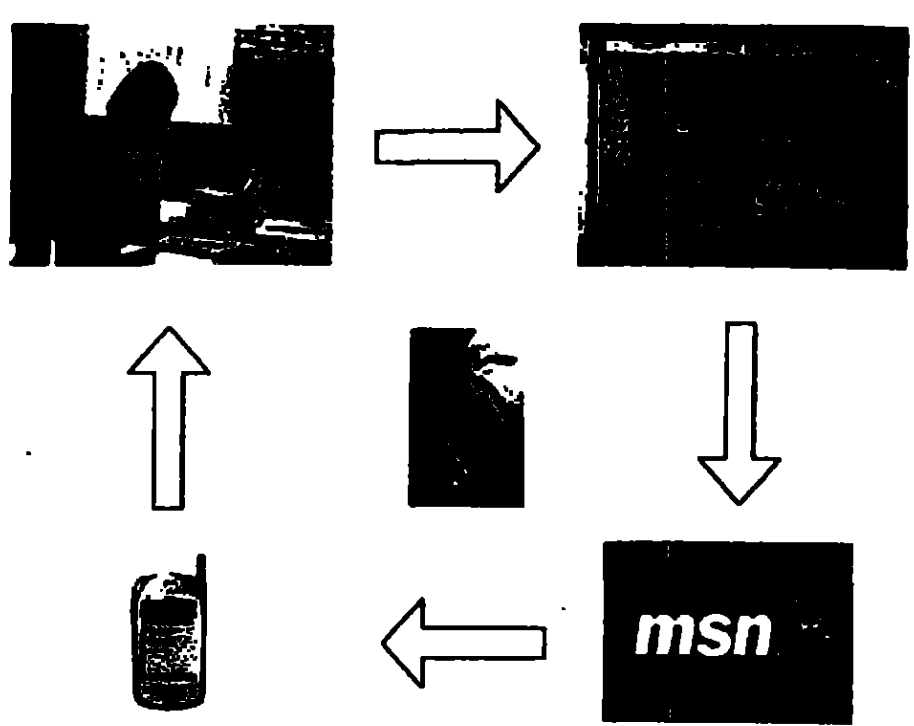


[0022] Within a federation attribute store, a principal registers their mobile access information such as their phone or Instant Messaging (IM) address. When a principal accesses their identity provider either via a mobile device, a kiosk, or any device, the identity provider (IP) for the principal is accessed to obtain a security token. As part of the authentication process, the identity provider contacts the principal. For example, the IP might send an SMS message to the principal's cell phone asking them to confirm identification by entering a specific PIN at the cell phone or into the application requesting the security token.

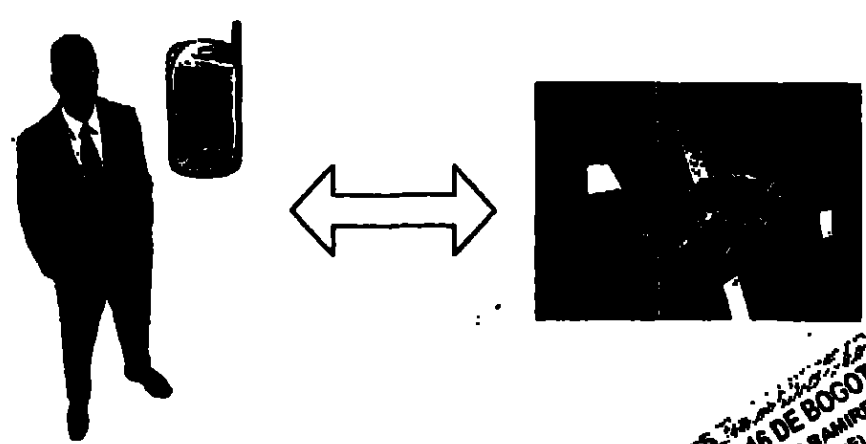
[0023] The following figure illustrates this scenario. A user is accessing a site from their PC while on the Internet. The store requests authentication from her identity provider. The IP sees that the user prefers mobile confirmation and sends a code to the user via SMS. The user receives the code and enters it into the application.

A FEDERAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

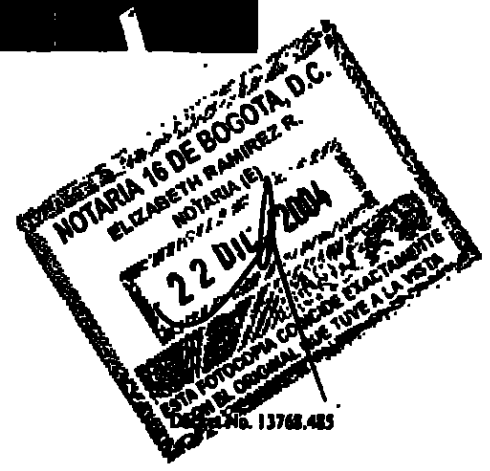




[0024] This approach can be used for all types of authenticated access such as VPN access or cross-firewall access to corporate assets. Similarly, this could all happen over a wireless infrastructure such as (e.g. IrDA, Bluetooth, or 802.11x). For example, the figure below illustrated using such wireless authentication as a cash machine.



A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1600 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

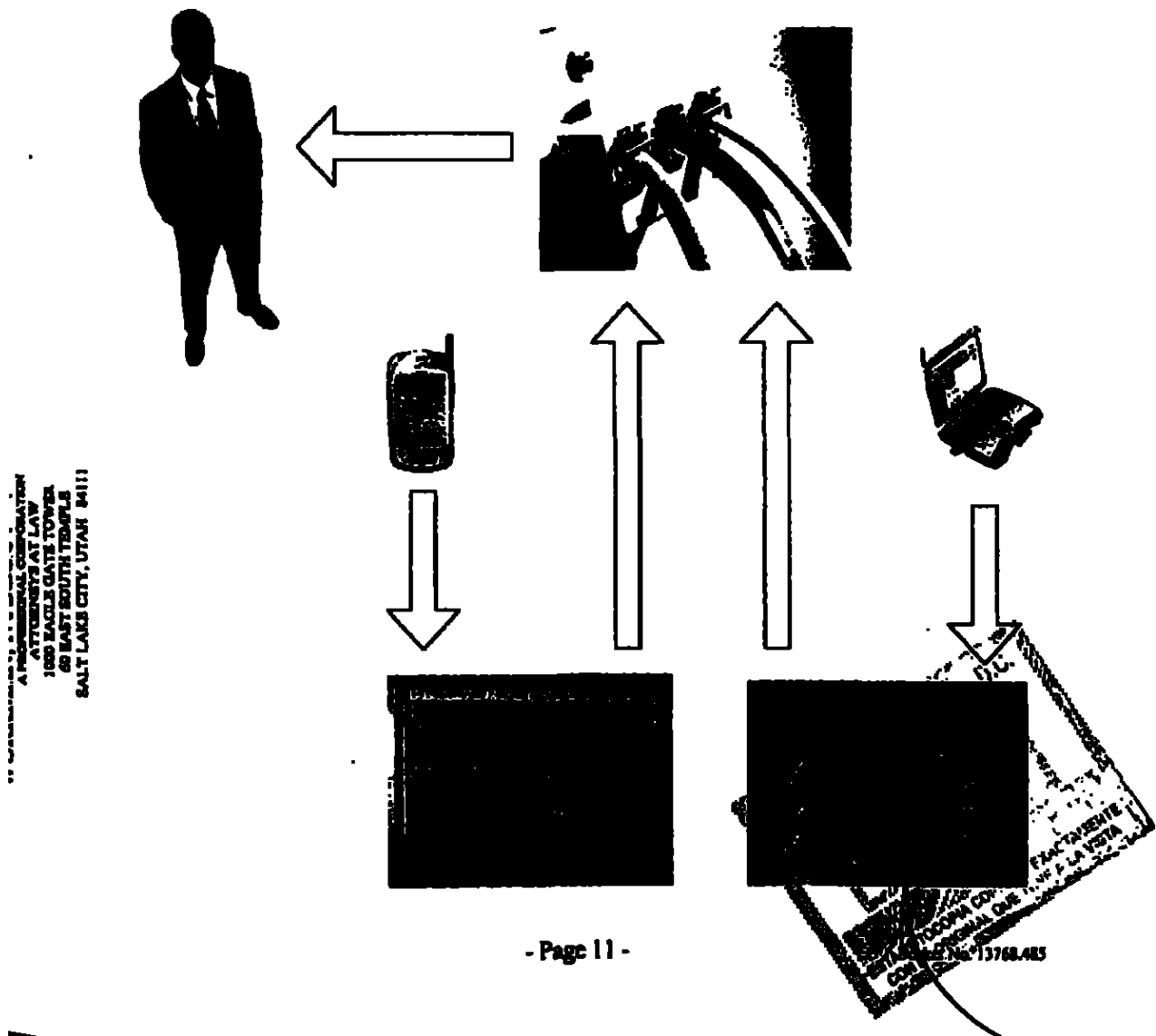


166
161

[0025] In the Authentication using Mobile SIM scenario, the billing and signing information in the SOAP header may be, for example, the security token provided by the identity provider, the PIN.

Federated Access to Resources and Centralized Billing

[0026] In this scenario, a mobile client uses its mobile identity provider to access a set of commerce sites, some from their mobile client and others from their PC (having authenticated with their mobile IP). As business transactions take place, the merchants bill to the mobile IP, which acts as a pseudo-bank consolidating charges to the mobile user on their monthly bill.



ATTORNEYS AT LAW
1000 EAST GATE TOWER
60 EAST SOUTH TOWER
SALT LAKE CITY, UTAH 84111

163
162

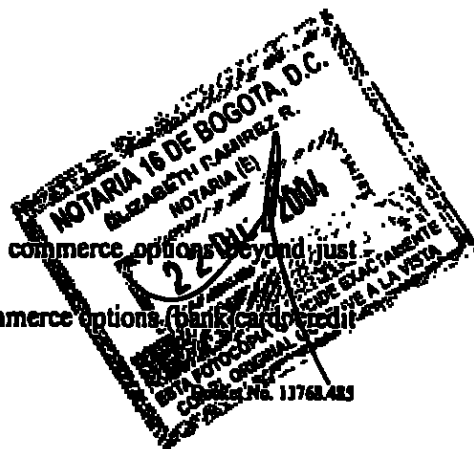
[0027] Again one key aspect to this scenario is that the client's monthly statement integrates their mobile charges along with any other charges billed to their mobile client providing a single integrated billing cycle which might also include transactions using traditional physical charging mechanisms (cards, etc.).

[0028] Let's consider how the Web services specification could be used to enable this scenario. A mobile user establishes a connection with the desired service and obtains the WS-Policy for communicating with the service. Based on the policy, the mobile client attempts to obtain a security token to access the service by providing the appropriate identity information registered on the mobile device (or in an associated attribute/pseudonym service as described in WS- Federation) using WSTrust. After successful authentication, the mobile client is issued an access token to the service. The client then performs secure transactions with the machine using WS-Reliability and WS- Transaction (based on desired reliability requirements) and submits orders for products and services. The mobile client and the service use information in the billing and signing headers to process the order, provide billing information, and generate invoices or debit requests. The mobile carrier acts as the bank for the invoices and debit requests and adds them to the client's monthly statement.

[0029] Accordingly, in this scenario, the billing and signing headers may include billing address, amount to be debits, account to be debited, invoice identifier, order identifier, confirmation number, or any other billing information or other information useful to process the order to generate invoice or debit request.

Mobile Wallet

[0030] The mobile client can also act as a wallet for commerce options beyond just centralized billing. That is, electronic forms of different commerce options (bank card, credit

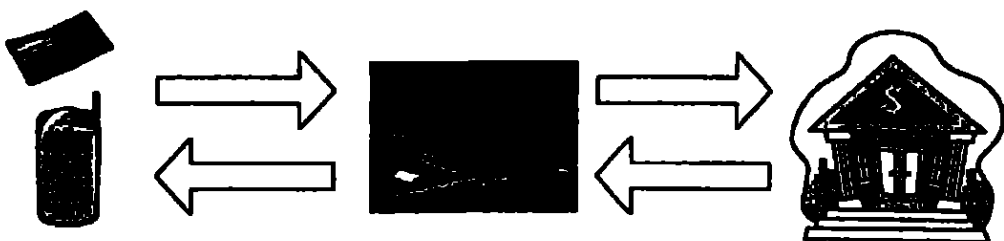


1000 EAGLE GATE TOWER
ATTORNEYS AT LAW
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

162
163

card, store card, pre-paid cards, etc.) can be stored on the mobile client and be securely used when needed.

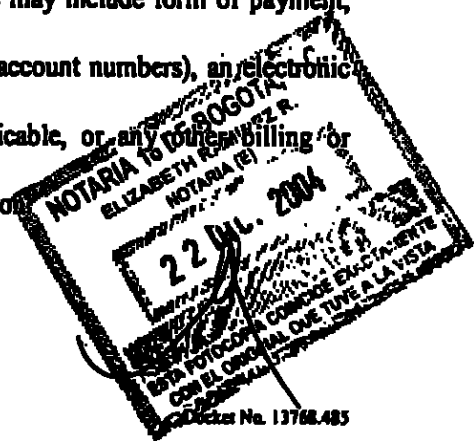
[0031] Consider the scenario where a mobile user goes into a store and selects merchandise and services they wish to purchase. The cashier totals the purchase while the mobile user selects the payment method they desire and send the payment information to the register for the cashier over PAN (e.g. IrDA, Bluetooth, or 802.11x). As appropriate, an authentication step can also take place. The transaction is accepted and the specified payment mechanism is used to complete payment (e.g. a commonly used credit card). This is illustrated in the figure below:



[0032] The use of the Web services protocols in this scenario is very similar to those in the previous section except that the debit processor is not the mobile carrier, but another merchant such as a credit card company or a bank. For credit card companies the charge appears on their monthly bill and for banks it may appear as a direct debit from, for example, a checking account.

[0033] In this scenario, the billing and signing headers may include form of payment, account numbers (such as credit, debit, checking or other account numbers), an electronic signature authorizing the charge, a PIN number if applicable, or any other billing or authorization information useful for completing the transaction.

Electronic Ticket



1000 EAGLE GATE TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

95

162
164

[0034] The mobile client can also take enable new forms of authentication and ticketing. Since the authentication mechanism is also a smart processing and storage system. That is, ticketing is the process by which one form of authentication, in addition to some commercial transaction, result in a new authentication which is good for only restricted uses. For example, a plain ticket, a train ticket, access to the zoo, etc.

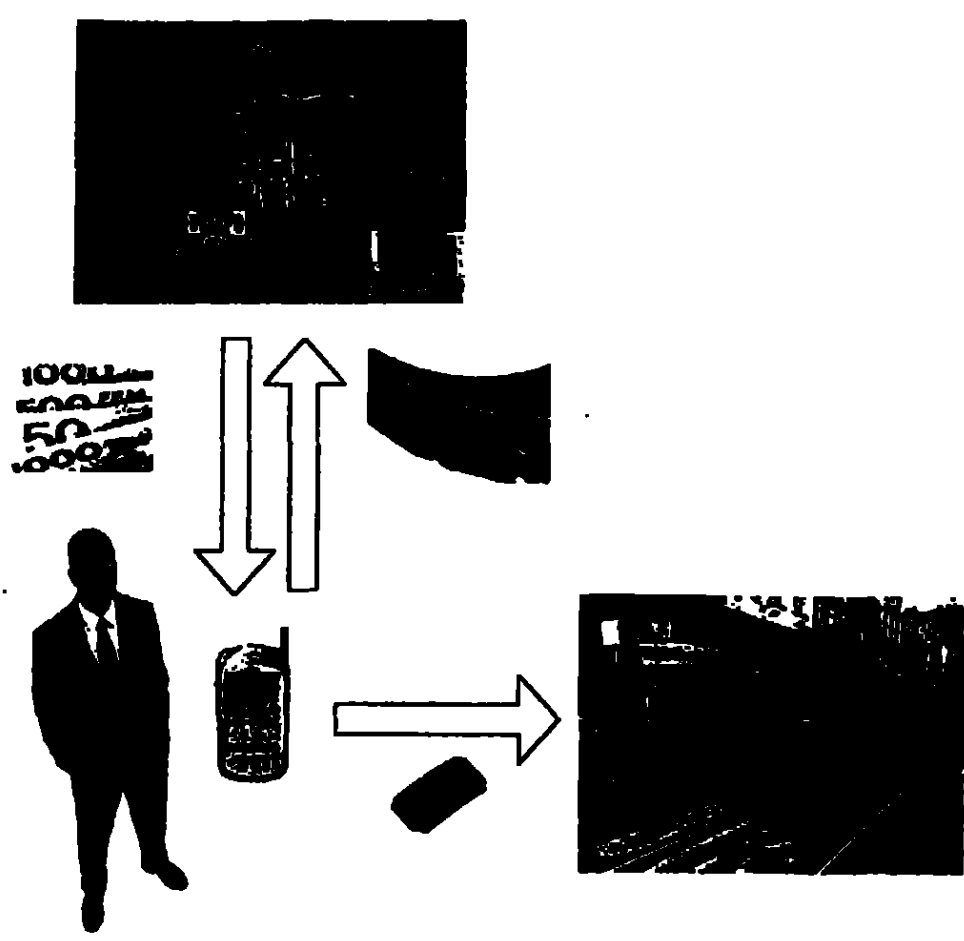
[0035] A scenario that integrates all of this together is an electronic train ticket. In this scenario a mobile client uses their device to purchase a set of tickets for their commuter train and, as a result, the transaction is billed to their mobile provider and the tickets are issued electronically to the mobile device. When the mobile user enters the train station they use the PAN (e.g. IrDA, Bluetooth, or 802.11x) to issue the ticket to the security system which then authorizes them to enter the train area. This is illustrated in the figure below:

WORKMAN, NYLUND & SIBLER
ATTORNEYS AT LAW
1600 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



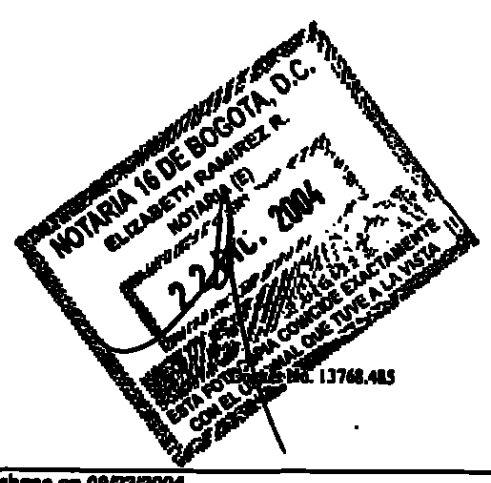
46

770
165



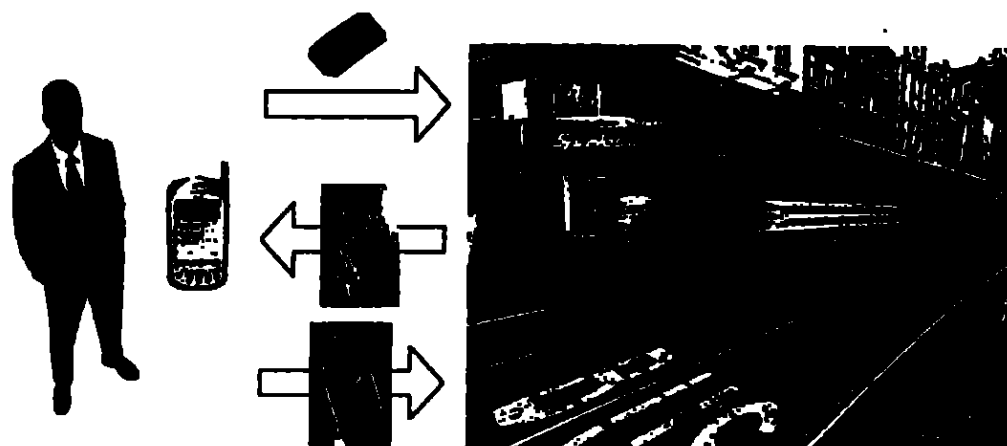
[0036] In some scenarios authentication is required in addition to the ticket and for this reason the mobile user may need to provide confirmation of identity by entering a code into their mobile device as illustrated in the figure below:

WORKMAN, NYDERGER & SHELLEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TENDLE
SALT LAKE CITY, UTAH 84111



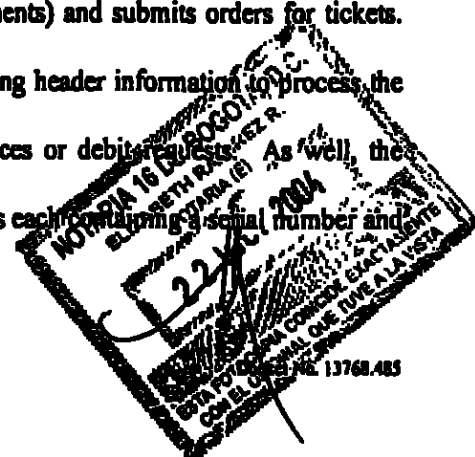
99

77
156



[0037] An alternative scenario would allow the mobile user access to the train and then perform the ticket exchange and authentication with the conductor more closely paralleling some existing ticketing mechanism.

[0038] Again the Web service interactions here are quite similar to those previously discussed. A mobile user establishes a connection with the desired ticket service and obtains the WS-Policy for communicating with the ticket service. Based on the policy, the mobile client attempts to obtain a security token to access the service by providing the appropriate identity information registered on the mobile device (or in an associated attribute/pseudonym service as described in WS-Federation) using WS-Trust. After successful authentication, the mobile client is issued an access token to the ticket service. The client then performs secure transactions with the machine using WS-Reliability and WS-Transaction (based on desired reliability requirements) and submits orders for tickets. The mobile client and the service use billing and signing header information to process the order provide billing information, and generate invoices or debit requests. As well, the ticket service returns a set of one-time single use tickets each containing a serial number and usage/validity information.



WORKMAN, NYDEGGER & SHERLEY
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

98

[0039] When the mobile client approaches the ticket receipt service (after obtaining policy information and optionally authenticating) it can then securely transmit the ticket using WS-Security and/or WS-SecureConversation.

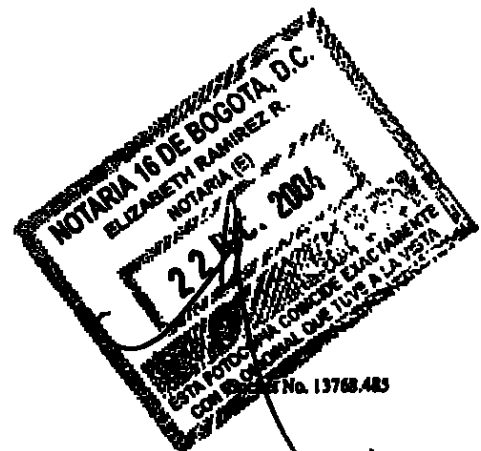
[0040] In this scenario, the billing and signing header may include any information helpful to process the order, provide billing information, or generate an invoice or debit request.

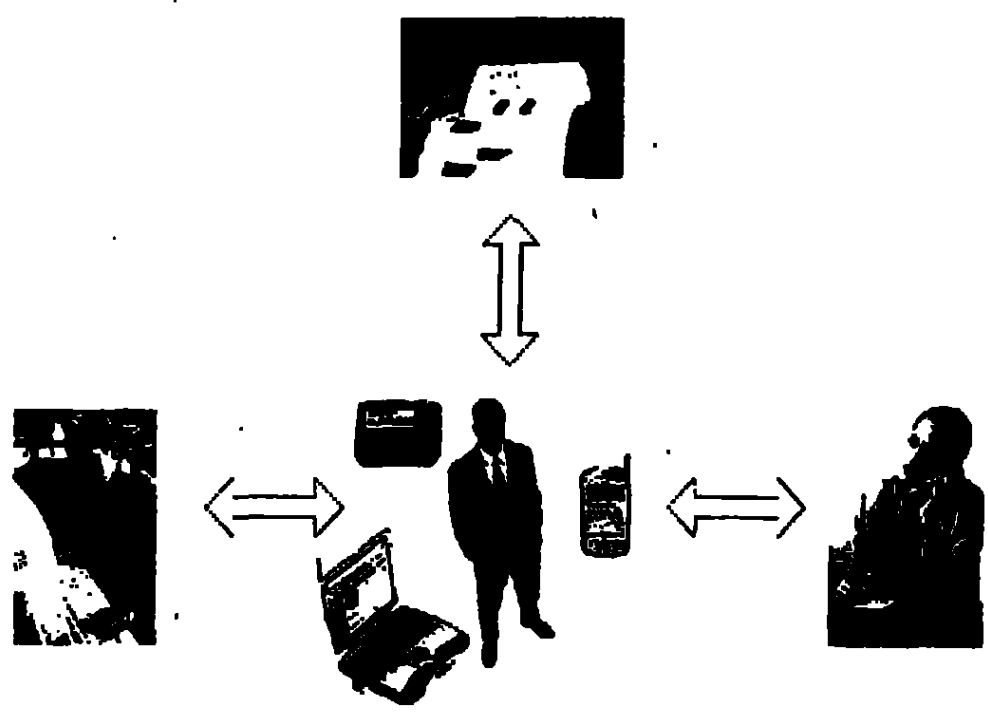
Remote PIM

[0041] The use of personal information managers (PIMs) is ubiquitous, however, they often lack federation and the ability to enable true mobility in that some mobile users have multiple mobile devices - that is, mobile users want access to their federated data any time, any where, and from any device.

[0042] For example, a mobile user, Joe, is on the road and uses his cell phone to call a colleague, Beth. The number may be cached on the phone, but it came from a federated PIM. In a meeting, another colleague, Jill, locates Joe using IM to a different mobile device. Later, Joe uses his laptop to send email to Jill and Beth from a mobile access point.

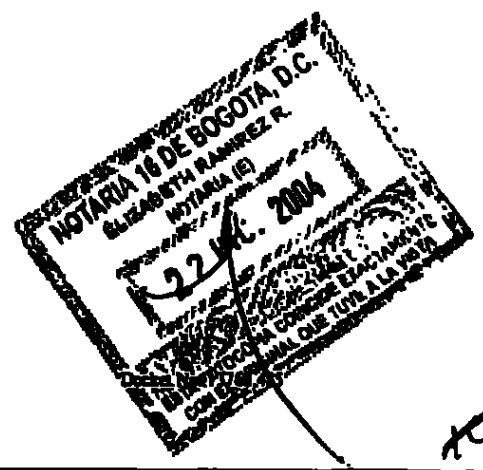
WORKMAN, NYDEGGER & SHELLEY
ATTORNEYS AT LAW
1000 EAGLE OATS TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



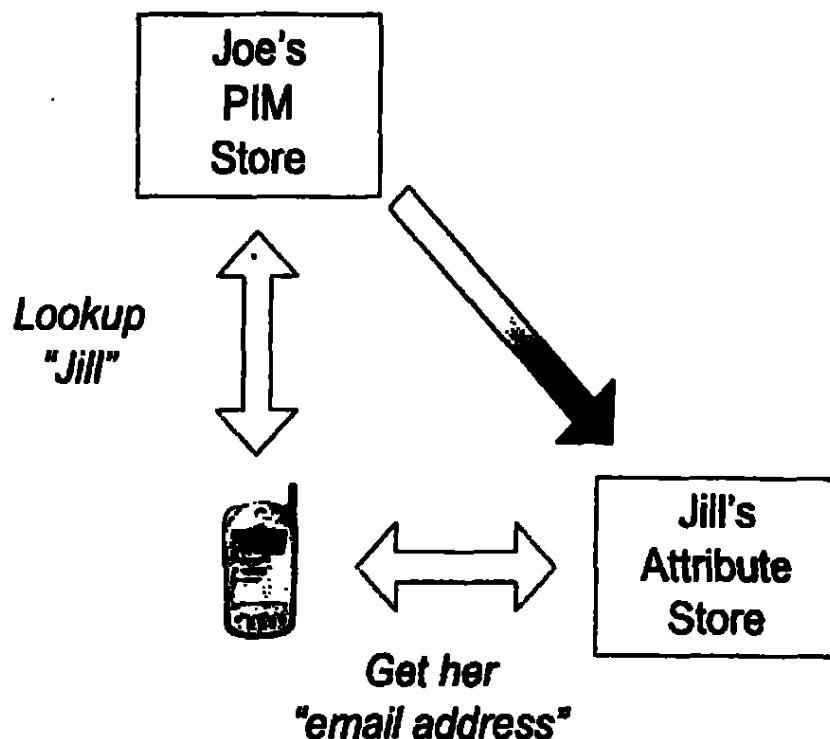


[0043] This scenario illustrates the value of centrally accessible PIM data. However, in a federated environment, the data is actually distributed. For example, Joe stores all of his PIM data at his mobile access provider. He has a contact list, but rather than having it contain the actual contact data, which can quickly become stale, it uses federation to point at the contact's attribute stores. Consequently, Jill's email address is found by looking up "Jill" as a contact in Joe's list, and then asking for the "email address" attribute for Jill.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1800 EAGLE GATE TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



170
169

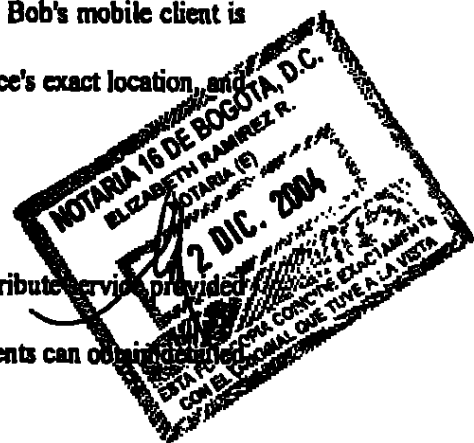


[0044] This approach also allows general sharing of more detailed attributes such as physical location which can be determined from their mobile client. An example scenario involves a set of five people who work together and have allowed general location information to be visible as illustrated in the figure below.

[0045] Alice notices that she and Bob are located in the same general area (say city), so Alice requests the exact location of Bob. Bob hasn't authorized Alice to see this information, but has indicated that verification should be obtained. Consequently, Bob's mobile client is told that Alice is requesting his exact location, possibly providing Alice's exact location, and requests approval to provide the information.

[0046] Bob authorizes this and the information is sent to Alice.

[0047] Contact and presence information are maintained in the attribute service provided by I WS-Federation. Using the presence specifications, authorized clients can obtain details



WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
40 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

107

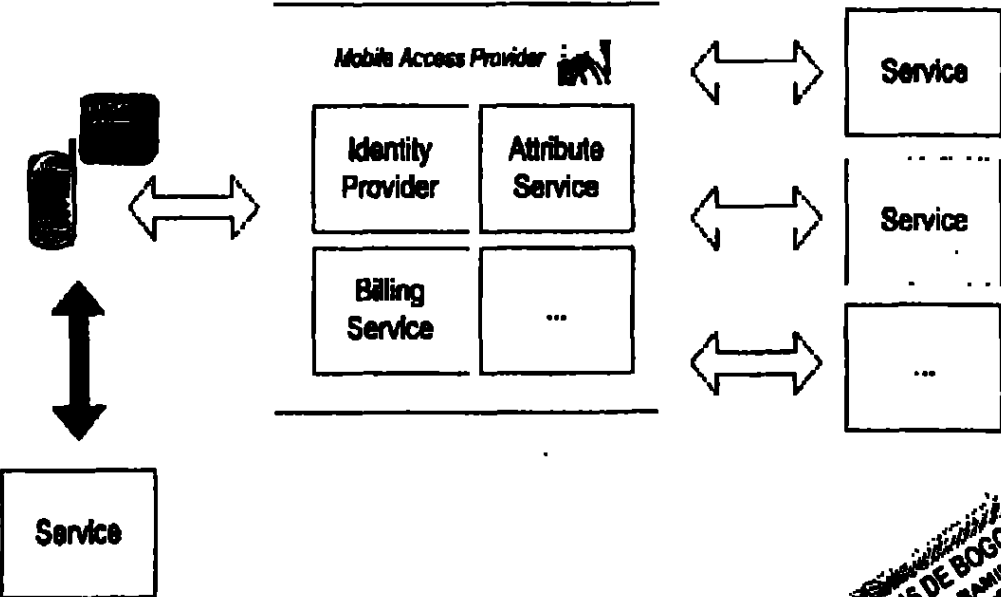
495
170

information on presence and location information (when authorized and available). For cases where access is not generally authorized, temporary or onetime access to presence/location (or potentially any federated attribute) can be granted.

[0048] In this scenario, the billing and signing information may include a PIM, billing information, or the like.

[0049] Accordingly, the Web Services architecture is extended to allow for billing and signing information to be included in the network messages in addition to, and independent of, other conventional Web Services specifications. Accordingly, the richness of Web Services may obtain addition functionality that enables commerce in a networked environment.

[0050] The architecture below illustrates one possible deployment in which mobile devices may engage in trusted transactions with mobile service providers.



[0051] However, as previously mentioned, the principles of the present invention are not limited to deployment in a mobile environment.

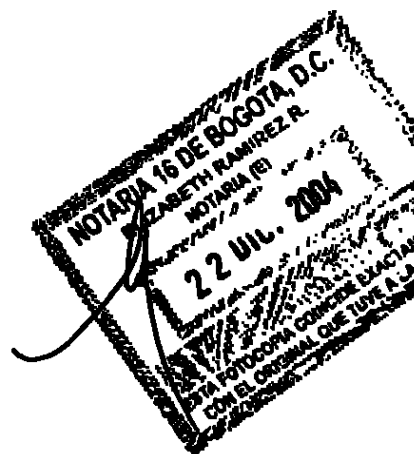
NOTARIA 16 DE BOGOTA, D.C.
ELEANOR RAMIREZ R.
24 JUL. 2004
FOTO OPCIIONAL QUE TUTE A LA FOTO
Docket No. 1700-1000

WORKMAN, NYDEGGER & SEELEY
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

176
171

[0052] The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

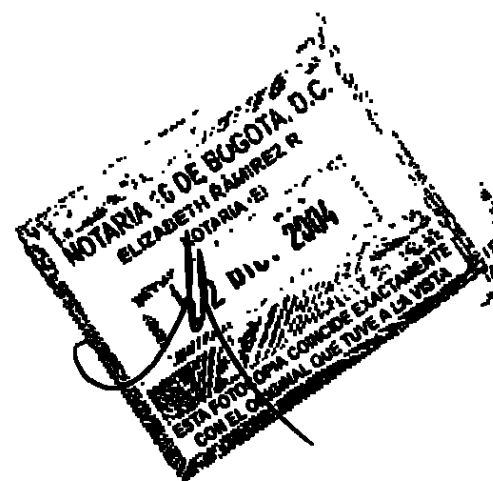


777
172

CLAIMS

1. One or more computer-readable media having thereon a SOAP envelope comprising the following:
 - a SOAP body portion; and
 - a SOAP header portion, wherein the SOAP header portion includes the following:
 - a header that includes billing information.
2. One or more computer-readable media in accordance with Claim 1, wherein the SOAP header portion includes that following:
 - a header that includes signing information.
3. One or more computer-readable media having thereon a SOAP envelope comprising the following:
 - a SOAP body portion; and
 - a SOAP header portion, wherein the SOAP header portion includes the following:
 - a header that includes signing information.

WORKMAN, NYDEGGER & SEEBLEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111



187.

193

4. One or more computer-readable media having thereon an electronic message comprising the following:

- a body portion; and
- a header portion that includes billing information.

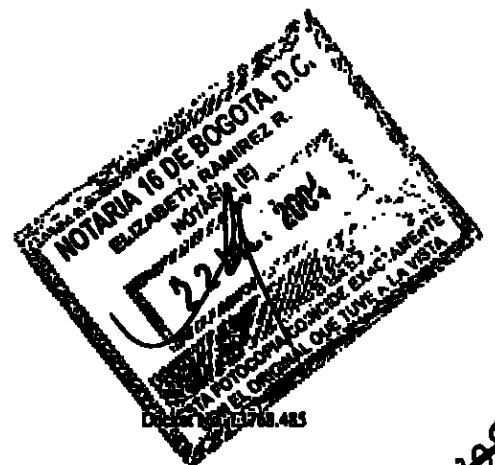
5. One or more computer-readable media in accordance with Claim 4, wherein the header portion further includes a header that includes signing information.

6. One or more computer-readable media having thereon an electronic message comprising the following:

- a body portion; and
- a header portion that includes signing information.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

W:\10422\1098\A\1.0000000327V001.doc



195

73
124

LOS ESTADOS UNIDOS DE AMERICA
A todos aquellos a los que se presente este documento:
EL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS
La Oficina de Patentes y Marcas de los Estados Unidos

Septiembre 27, 2004.

ESTO CERTIFICA QUE EL ANEXO A LA PRESENTE ES UNA COPIA AUTENTICA DE LOS REGISTROS DE LA OFICINA DE PATENTES Y MARCAS DE LOS ESTADOS UNIDOS DE AMERICA CORRESPONDIENTES A LOS DOCUMENTOS DE LA SOLICITUD DE PATENTE IDENTIFICADA A CONTINUACIÓN LOS CUALES CUMPLIERON CON LOS REQUERIMIENTOS PARA OTORGARLE UNA FECHA DE PRESENTACIÓN BAJO EL 35 USC 111.

NUMERO DE SOLICITUD: 60/515,461
FECHA DE SOLICITUD: Octubre 29 de 2003.

(SELLO) Por la autoridad del
Comisionado de Patentes y Marcas

Firmado (illegible)
L. EDELEN
Oficial de Certificación



106

Por favor marque un signo de más (+) dentro de este cuadro



PTO/SB716 (5-03)

Aprobado para uso hasta el 04/30/2003 CP# 0621-0032

Oficina de Patentes y Marcas de los Estados Unidos, Departamento de Comercio de los Estados Unidos.
Bajo la normalidad de reducción de papel de 30%. Los usuarios no están requeridos para contestar a la información a menos que esta sea declarada válida por un agente de control de CPB.

CUBIERTA PROVISIONAL PARA SOLICITUD DE PATENTE

Este es un requisito para presentar una solicitud provisional para patente bajo el 37 CFR 1.53 (c)

INVENTOR(ES)					
Nombre dado (primero y medio (si hay))	Apellidos		Residencia (ciudad y estado o país extranjero)		
Max G. Christopher G.	Morris Kaler		Seattle, Washington	Sammamish, Washington	
☐ Inventores adicionales son nombrados en _____ hojas anexas separadamente numeradas					
TITULO DE LA INVENCIÓN (280 caracteres max)					
SERVICIOS WEB PARA CERTIFICACION Y FIRMA					
Dirigir toda la correspondencia a: DIRECCION DE CORRESPONDENCIA					
☒ Número de cliente		022913		Coloque el sello del número del código de barras del cliente	
O		Escriba el Número de Cliente aquí			
☒ Firma o nombre individual		WORKMAN NYDEGGER			
Dirección		1000 Eagle Gate Tower			
Dirección		60 East South Temple			
Ciudad		Salt Lake City	Estado	UT	ZIP 84111
País		USA	Telefono	801-533-9800	Fax 801-328-1707
PARTES DE LA SOLICITUD ADJUNTAS (Marque todo lo que aplique)					
☒ Especificación		Numero de páginas	23	☐ CD(s)	Numero
☐ Dibujos		Numero de páginas		☐ Otro (especificar)	
☐ Hoja de Solicitud de datos Ver 37 CFR 1.76					
METODO DE PAGO PARA LAS TASAS DE ESTA SOLICITUD PROVISIONAL PARA PATENTE (Marque uno)					
					VALOR DE LA TASA (\$)
☒ Un cheque u orden de pago incluida para cubrir las tasas					
☒ El director se encuentra autorizado para cargar las tasas o créditos					\$160.00
O cualquier pago en exceso a la Cuenta de depósito número		23-3178			
☐ Pago con tarjeta de crédito. Forma PTO-2038 está anexa.					
La invención fue hecha por una agencia del Gobierno de los Estados Unidos o bajo un contrato con una agencia del Gobierno de los Estados Unidos					
☒ No					
☐ Si, el nombre de la Agencia del Gobierno de los E.U. y el número de contrato de Gobierno es:					

Respetuosamente presentado,

FIRMA (firma ilegible)

NOMBRE DIGITADO O IMPRESO ADRIAN J. LEE

TELEFONO 801-533-9800

Fecha 10/29/03

REGISTRO No. 42,785

(si es apropiado)

Etiqueta No. 13768.485

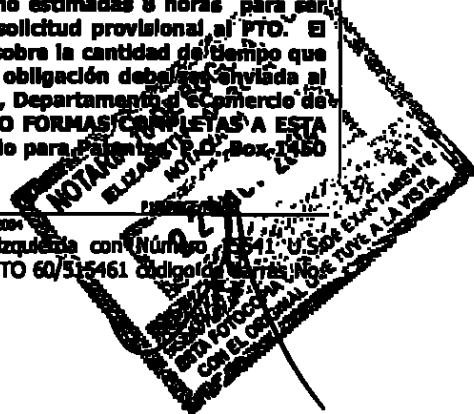
USO EXCLUSIVO PARA PRESENTAR UNA SOLICITUD PROVISIONAL DE PATENTE

Esta colección de información es requerida por 37 CFR 1.51. La información en este formato puede ser pública para archivar (y por el PTO para procesar) una solicitud provisional. La confidencialidad es regulada por el 35 U.S.C. 122 y 37 CFR 1.14. Esta colección tiene como estimadas 8 horas para ser completadas incluyendo recolección, preparación y presentación de la solicitud provisional al PTO. El tiempo puede variar según cada caso individual. Cualquier comentario sobre la cantidad de tiempo que usted requirió para llenar esta forma y/o sugerencias para reducir esta obligación deben ser enviadas al oficial jefe de Información de la Oficina de Marcas y Patentes de los E.U., Departamento de Comercio de los E.U., P.O. Box 1450 Alexandria VA 22313-1450. NO ENVIE CARGOS O FORMAS COMPLETAS A ESTA DIRECCION. ENVIE A: Parada de correo solicitud provisional, Comisionado para Patentes, P.O. Box 1450 Alexandria VA 22313-1450

Si necesita asistencia para llenar esta forma, llame al 1-800-PTO-9199 y solicite la sección 2

Copie proporcionada por USPTO de la base de datos de formas PACR al CP-33-3094

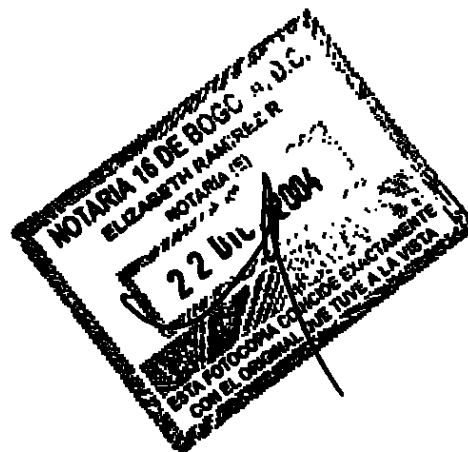
Nota del Traductor: Esta página se encuentra sellada en su parte superior izquierda con Número 13768.485 U.S. Pat. & Tm. Office
PTO/código de barras No.(ILEGIBLE); y en su parte superior derecha 22582 U.S. PTO 60/515461 código de barras No. 102903.






CERTIFICADO DE ENVIO DE CORREO POR "CORREO EXPRESO" (37 CFR 1.10) SOLICITANTES: Pina G. Morris et al.		ETIQUETA No. 13768.485	
Serial No. Aun No Asignado	Fecha de Presentación Octubre 29, 2003	Examinador Aun no asignado	Unidad de Grupo Arte Aun no asignado
Inventón: SERVICIOS WEB PARA CERTIFICACION Y FIRMA			
El aquí firmante certifica que la siguiente correspondencia:			
Hoja provisional de cubierta (1 página); Transmisión provisional (1 página); solicitud provsional (23 páginas); cheque No. 134173 por \$160.00; tarjeta postal (Identificar tipo de correspondencia)			
Ha sido depositado en el Servicio Postal de los Estados Unidos "Oficina de Correo Expreso para el Destinatario" servicio bajo 37 CFR 1.10 en un sobre dirigido a: Comisionado de Patentes, P.O. Box 1450, Alexandria, VA 22313-1450 en <u>Octubre 29, 2003</u> (fecha) <u>ADRIAN J. LEE</u> (Nombre impreso o escrito de la persona remitente de la correspondencia) <u>(ILEGIBLE)</u> (Firma de la persona remitente de la correspondencia) <u>EY 302233329 US</u> (Firma de la persona remitente de la correspondencia)			
Nota: Cada papel debe tener su propio certificado de envío de correo			

PS&A/EV 02



408

FORMA DE TRANSMISION (PARA SER UTILIZADA POR TODA LA CORRESPONDENCIA LUEGO DE SU PRESENTACION INICIAL)		Numero de Solicitud	Aun no asignado
		Fecha de presentación	Octubre 29 de 2003
		Primer Inventor	Max G. Morris
		Unidad de Arte	Aun no asignada
		Nombre del examinador	Aun no asignado
Número total de páginas presentadas		Numero de sello del apoderado	13768.485

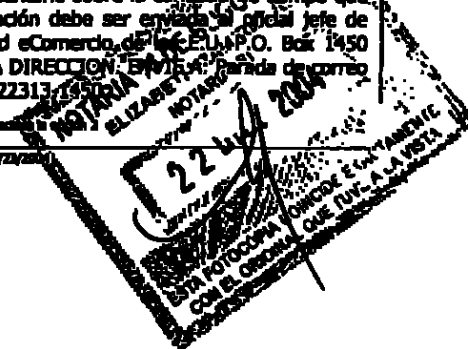
ANEXOS (marque todo lo que aplique)		
☐ Tasa del formato de transmisión ☒ Tasa Incluida ☐ Enmienda/respuesta ☐ Luego del final ☐ Declaración(es) Jurada(s) ☐ Solicitud de extensión de tiempo ☐ Solicitud expresa de cesión ☐ Documento(s) de copia certificada o prioridad ☐ Respuesta para partes perdidas/solicitud incompleta ☐ Respuesta para partes perdidas bajo el 37CFR 1.52 o 1.53	☐ Dibujo(s) ☐ Papeles de licenciamiento relacionados ☐ Solicitud ☐ Solicitud para convertir una solicitud provisional ☐ Poder de abogado, revocación o cambio de correspondencia ☐ Renuncia terminal ☐ Solicitud de reembolso ☐ CD, Número de CD(s) Comentarios .	☐ Comunicación al grupo después de admisión ☐ Comunicación de apelación a la Junta de Apelación e Interferencias ☐ Comunicación de apelación al grupo (aviso de apelación, breve respuesta) ☐ Información de propietario ☐ Carta de estatus ☒ Otros documentos adjunto(s) (por favor identificar abajo) • Solicitud Provisional • Hoja de cubierta provisional
FIRMA DEL SOLICITANTE, APODERADO O AGENTE		
Firma o nombre individual	ADRIAN J. LEE WORKMAN NYDEGGER	
Firma	(Illegible)	
Fecha	Octubre 29 de 2003	

CERTIFICADO DE TRANSMISION /CORREO		
Por la presente, certifico que esta correspondencia está siendo transmitida por facsimil a la USPTO o depositada con el servicio postal, con el suficiente porte como correo de primera clase en un sobre dirigido a: Comisionado de patentes, P.O. Box 1450, Alexandria, VA 22313-1450 en el		
Nombre escrito o Impreso		
Firma		Fecha

Esta colección de información es requerida por el 37CFR 1.5. La información es requerida para obtener o retener un cierto beneficio para el público que será archivada (y procesada por la USPTO para procesar) en solicitud. La confidencialidad está gobernada por 35 USC 122 Y 37 CFR 1.14. Esta solicitud tiene estimados 12 minutos para ser completada, incluido incluyendo recolección, preparación y presentación completa de la forma de la solicitud para la USPTO. El tiempo variará dependiendo de cada caso individual. Cualquier comentario sobre la cantidad de tiempo que usted requirió par llenar esta forma y/o sugerencias para reducir esta obligación debe ser enviada al oficial jefe de Información de la Oficina de Marcas y Patentes de los E.U., Departamento de Comercio, P.O. Box 1450 alexandria VA 22313-1450. NO ENVIE CARGOS O FORMAS COMPLETAS A ESTA DIRECCION. Si se envía la forma de correo solicitud provisional, Comisionado para Patentes, P.O. Box 1450 Alexandria VA 22313-1450.

Si requiere asistencia para llenar esta forma, llame al 1-800-PTO-6198 y solicite la ayuda.

Copia proporcionada por USPTO de la base de datos de Internet en 08/23/2004



Envío No. EV 302233329 US

APLICACIÓN DE PATENTE
Minuta No. 13768.485

185
178

APLICACIÓN DE PATENTE PROVISIONAL DE LOS ESTADOS UNIDOS

De

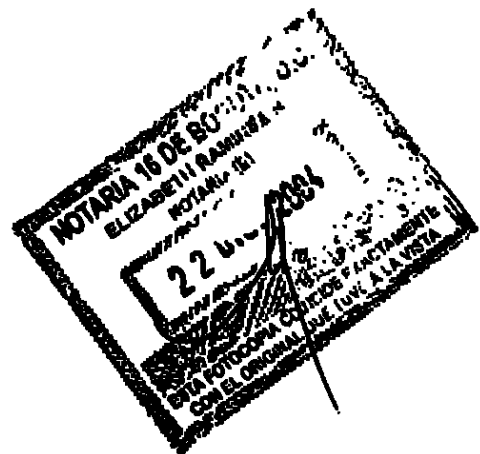
Max G. Morris

And

Christopher G. Kaler

For

SERVICIOS WEB PARA CERTIFICACION Y FIRMA



110

EL FONDO DE LA INVENCION

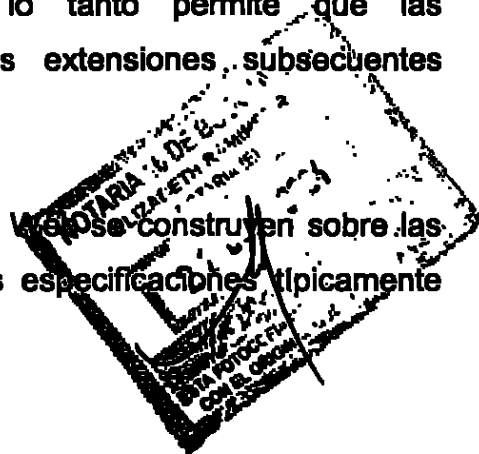
122
171

[0001] La tecnología de cómputo ha transformado la manera que nosotros trabajamos y jugamos. La mayoría de la funcionalidad de los sistemas de cómputo se deriva de la habilidad de los sistemas de cómputo de comunicarse uno con otro sobre una red. Los sistemas de cómputo están ahora comercialmente disponibles en una variedad amplia de formas incluso las computadoras de escritorio, computadoras portátiles, los ayudantes Digitales personales (PDAs), Tablet PCs (computadores de tabla), los teléfonos, los dispositivos de hogar y otros formas. Estos sistemas de cómputo tienen niveles variantes de movilidad que van desde ninguno en absoluto a ser muy móviles. Sin tener en cuenta la movilidad, el uso de tales sistemas continúa creciendo y se vuelve ubicuo. La funcionalidad de tales sistemas son reforzados grandemente por su habilidad de comunicarse sobre las redes con otros sistemas de cómputo. Por ejemplo, correo electrónico, mensajería instantánea, la navegación de Web, y muchas otras aplicaciones comunes confían en la comunicación de la red.

[0002] Una tecnología de la gestión de redes convencional es a menudo llamada "Servicios de Web". Las arquitecturas de los Services Web contienen protocolos e interfaces para habilitar seguras y fiables comunicaciones en una red de mensajería asíncrona que es vendedor, plataforma, y dispositivo independiente. La arquitectura es eficaz y la composición de apoyos con otros estándares para proporcionar las funciones que clientes, diseñadores de software, proveedores de plataforma, y operadores móvil de la red necesitan.

La arquitectura es también extensible, por lo tanto permite que las especificaciones evolucionen y permite que las extensiones subsecuentes interactúen.

(0003] Las especificaciones de los Servicios Web se construyen sobre las bases existentes de XML, SOAP, y WSDL. Las especificaciones típicamente

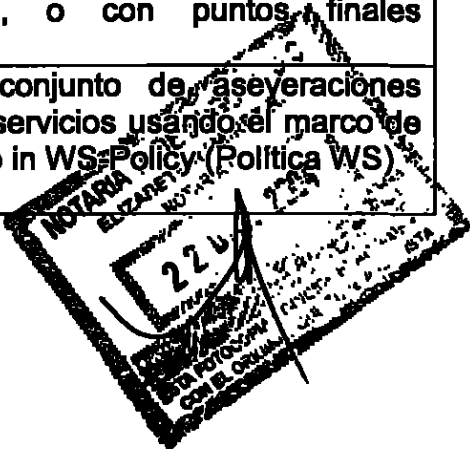


TTT

proporcionan para el uso modular de SOAP encabezados que acometen tareas específicas. La ventaja importante de estas especificaciones es que ellas permiten la reutilización de los protocolos de nivel para lograr el trabajo común que las implementaciones de servicios Web de XML hacen repetidas veces. Separándolos, y generalizándolos nosotros permitimos ser perfeccionados y combinados para las soluciones apropiadas que requieren un solo protocolo monolítico. Así, usando ladrillos comunes de construcción nosotros somos probablemente más interoperativos, aumentando la productividad, aumentando el rendimiento, y aumentando la fiabilidad. Los principios de diseño usados en estas especificaciones son: de uso general, basado en estándares, aliados, y modulares. Las metas son (respectivamente) para ser agnóstico al dominio de aplicación; lograr la interoperabilidad de multi-vendedor; evitar cualquier punto central de administración, controlar, y fallar; y ser factorizado para estar solo exclusivamente o trabajar juntos.

[0004] La tabla de abajo presenta un resumen de cada especificación organizada por categoría:

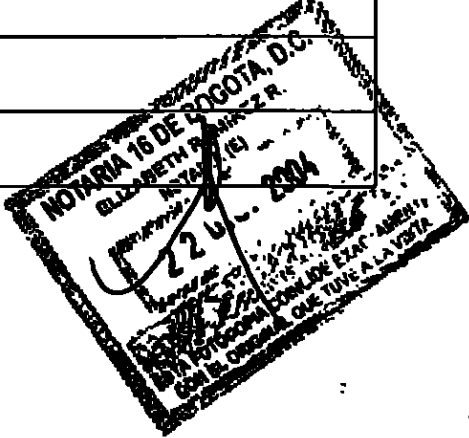
	Especificación	Resumen
Descripción	Política WS (WS-Policy)	Describe un conjunto base de estructuras que pueden ser usado y extendido por otras especificaciones de servicios Web para describir un amplio rango requerimientos, preferencias, y capacidades de interfaces de servicio.
	Adjunto de Política WS (WS-Policy Attachment)	Describe un conjunto de de mecanismos para la sociación de políticas dentro de WSDL, UDDI, o con puntos finales arbitrarios.
	Aserciones de la política WS (WS-policy Assertions)	Describe un conjunto de aseveraciones acerca de los servicios usando el marco de trabajo descrito in WS-Policy (Política WS)



Intercambi de Mensaj s (Messaging)	Direccionamiento- WS (WS- Addressing)	Describe un marco de trabajo para identificar los puntos finales del servicio WEB y para asegurar la identificación de los mensajes de extremo a extremo.
Seguridad	Seguridad WS (WS- Security)	Describe como adjuntar la firma y los encabezados de encriptación a los mensajes SOAP. Adicionalmente, este describe como adjuntar testigos ó fichas (tokens) seguros, incluyendo testigos de seguridad binarios como certificados X.509 y tiquetes Kerberos para los mensajes.
	Política de Seguridad WS - (WS-SecurityPolicy)	Describe como las capacidades de seguridad y las obligaciones son expresadas usando WS-Policy. (Es decir tokens de seguridad requeridos, algoritmos de encriptación soportados, reglas de privacidad)
	Confianza de WS - (WS - Trust)	Describe un marco de trabajo para los modelos de confianza que posibilitan que los servicios WEB interactúen con seguridad.
	Conversación Segura de WS (WS- SecureConversation)	Describe como administrar y autenticar el intercambio de mensajes entre las partes incluyendo el intercambio del contexto de seguridad y estableciendo y derivando claves de sesión.

[0005] El diagrama siguiente ilustra varias áreas de enfoque de clave y sus relaciones:

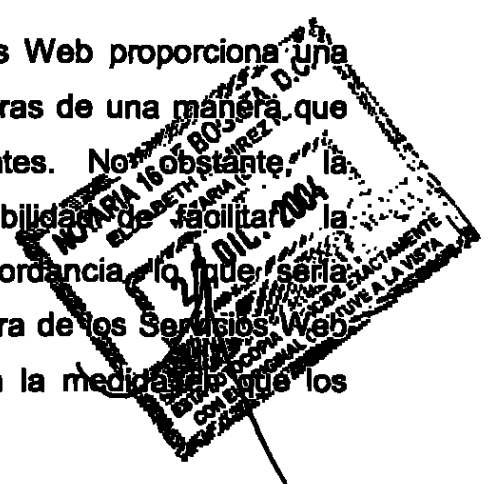
Seguridad (Security)	Mensajería Segura - (Reliable Menssaging)	Transacciones - Transactions
XSD, WSDL, UDDI, Policy, MetadataEchange – (Intercambio de Metadata)		
XML, SOAP, Addressing		
http, HTTPS, SMTP		



[0006] Este marco de trabajo habilita la descripción e interoperabilidad de los servicios Web seguros y fiables llevados a cabo en un ambiente de la mensajería síncrono o asíncrono que es construido en las bases de XML.

[0007] En el contexto de habilitar el comercio en un ambiente de red: La capa de mensajería (por ejemplo, especificación WS-direccionamiento), permite que los mensajes sean enviados entre diferentes dispositivos e intermediarios, usando una variedad de protocolos que permiten formas diferentes de comunicación sobre de una variedad de medios físicos. La especificación de la política WS y las características técnicas del descubrimiento relacionadas permiten a compradores y comerciantes seguramente y claramente a indicar sus políticas para la comunicación y el comercio seguro. La seguridad WS y las especificaciones de confianza WS proporcionan mecanismos para asegurar mensajes hacia y desde clientes de servicios WEB móviles. Cuando son combinados con las identidades de federación WS (WS- Federation) y la Conversación Segura de WS (WS-SecureConversation), pueden tener intercambios de mensajes autenticados y seguros. La Mensajería Segura de WS – (WS-ReliableMessaging) y las especificaciones de las Transacciones WS (WS-Transaction) complementan la infraestructura de mensajería segura, permitiendo, como es deseado, la transacción segura y fiable de mensajes.

[0008] En concordancia, la arquitectura de los Services Web proporciona una plataforma eficaz para las comunicaciones fiables y seguras de una manera que son vendedor, plataforma y dispositivo independientes. No obstante, la arquitectura de los Servicios WEB ha limitado la habilidad de facilitar la facturación o firma relacionada al comercio. En concordancia, lo que sería ventajoso serían los mecanismos para usar la arquitectura de los Servicios Web para apoyar la facturación y la firma sobre la RED. En la medida que los

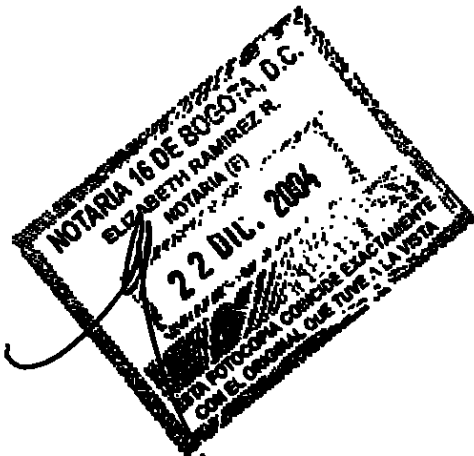


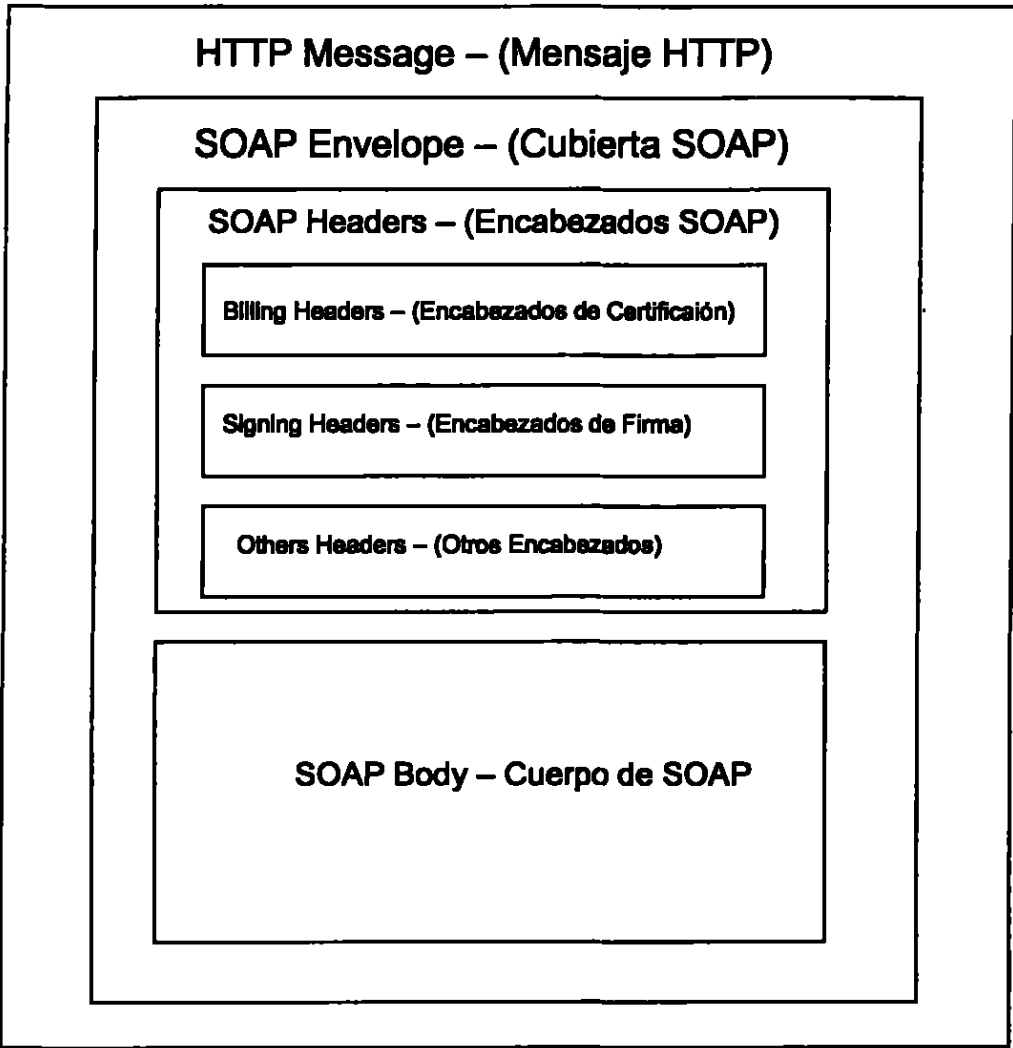
dispositivos móviles están volviéndose más populares comprometiendo en la red el comercio, debería ser particularmente ventajoso que el mecanismo apoyara el comercio usando los dispositivos móviles, mientras no se limite a la aplicación en un ambiente móvil.

DESCRIPCION DE TALLADA DE LAS PERSONALIZACIONES PREFERIDAS

[0009] Los principios de la invención presente relacionan el uso de certificar y firmar la información en un mensaje de la red. En una personalización, la facturación y la firma de la información se proporcionan como la suma de las especificaciones de los Servicios Web. En particular, la facturación y la firma de la información pueden ser incluidas como parte del encabezado de un Protocolo de Acceso de Objeto Simple (SOAP). La forma exacta de la facturación y firmando de la información no es importante para los principios de la invención presente. Cualquier estructura para representar la facturación y firma de la información bastará tanto así como los sistemas de informática que están comunicando la información reconocen un esquema común para que la importancia de la facturación y firmando de la información pueda reconocerse mutuamente.

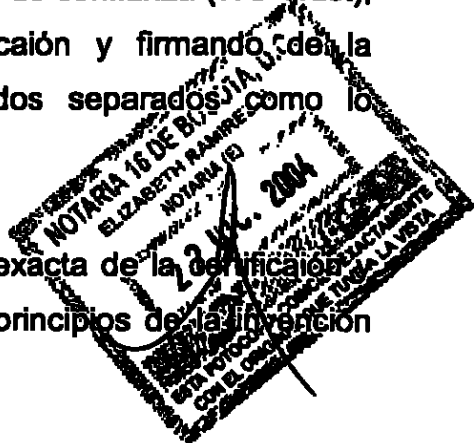
[0010] Lo siguiente ilustra un mensaje electrónico de acuerdo con los principios de la invención presente en que la facturación y firmado de la información está incluida como parte del encabezado SOAP de una cubierta SOAP. La cubierta SOAP puede contenerse como parte de, por ejemplo, un mensaje de Protocolo de Transporte de Hipertexto (HTTP).





[0011] Los encabezados SOAP incluyen uno o más elementos del encabezado que incluyen la facturación de la información, uno o más encabezados que incluyen la firma de la información, y uno o más elementos otros que representan los títulos definidos por las especificaciones de Servicios Web convencionales (por ejemplo, direccionamiento de WS (WS-addressing), WS de confianza (WS-Trust), política de WS (WS-policy), y similares). La certificación y firmando de la información puede proporcionarse en los encabezados separados como lo ilustrado, o en un solo encabezado.

[0012] Como previamente se mencionó, la estructura exacta de la certificación firmado de la información no es importante para los principios de la invención



TTG.

presente. Además, el la denominación precisa de los campos de los datos tampoco es importante. Sin embargo, la información de facturación puede incluir para la facturación generalizada incluso el crédito y funciones del débito en que pueden operar el micro - y macro ambientes de pago así como pidiendo y proporcionando las cuotas, las facturas, y las órdenes de compra. La información de la firma puede incluir la información para el firmando, la plica, autorizaciones, y registro de auditoria para árbitros.

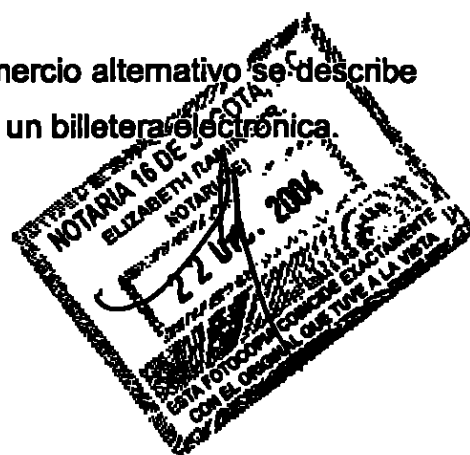
[0013] El tipo de información representado por la facturación y la información de firma pueden ser mejor entienda con la referencia a varios escenarios del comercio que son ahora descritos. Aunque se proporcionan los escenarios específicos para ilustración, los principios de la presente invención no son limitados a estos específicos escenarios, pero aplican a cualquier escenario en que la comunicación de facturación y/o la información de firma puede ser útil.

[0014] Aquí está una apreciación global breve de cada guión que se describirá:

[0015] *Autenticación usando Mobile SIM* - Aquí nosotros vemos cómo un SIM Móvil puede usarse para proporcionar una autenticación fuerte para los Servicios WEB de cliente móvil.

[0016] *El Acceso federado y la Facturación Central* - En este escenario los servicios Web de cliente móvil se usan para acceder a los datos federados en los dominios de seguridad diferentes y comprometer en actividades del comercio m (móvil) que son centralmente certificadas al operador móvil de la red.

[0017] *La Billetera Móvil* - Un escenario del comercio alternativo se describe donde el cliente de Servicios WEB móvil se usa como un billetera electrónica.



194
186

[0018] *El Boleto electrónico* - Este escenario demuestra el comercio centrado en el cliente de los Servicios WEB móvil como un recurso común de facturación. En este escenario los servicios Web móviles son usados como una billetera segura.

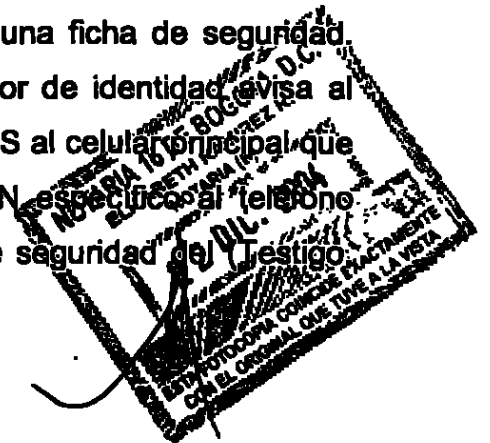
[0019] *PIM Remoto* - Un escenario se describe donde los usuarios móviles toman ventaja de los datos de PIM federados por múltiples clientes de Servicios Web móviles.

[0020] Estos cuatro diferentes escenarios serán descritos en mayor detalle.

Autenticación Usando SIM Móvil

[0021] El dispositivo móvil proporciona una nueva opción en la autenticación proporcionando una plataforma dinámica para el acceso a los principales. Para los principales móviles, hay una variedad ahora de mecanismos referentes al principal como los teléfonos celulares, PDAs, PCs automotores, mensajería instantánea, PCs inalámbrico, etc.

[0022] Dentro de una tienda de atributo de federación, un principal registra su información de acceso móvil como su teléfono o dirección de Mensajería Instantánea ((IM address). Cuando un principal acceda su proveedor de identidad vía un dispositivo móvil, un kiosco, o cualquier dispositivo, el proveedor de identidad (IP) para el principal se accede para obtener una ficha de seguridad. Como la parte del proceso de autenticación, el proveedor de identidad avisa al principal. Por ejemplo, la IP podría enviar un mensaje SMS al celular principal que les pide que confirmen la identificación entrando un PIN específico al teléfono celular o en requerimiento de la aplicación del Token de seguridad de Testigo Ficha.



102
187

[0023] La figura siguiente ilustra este escenario. Un usuario está accediendo un sitio de su PC mientras está en la Internet. La tienda pide la autenticación de su proveedor de identidad. La IP ve que el usuario prefiere la confirmación móvil y envía el código al usuario vía SMS. El usuario recibe el código y lo entra en la aplicación.

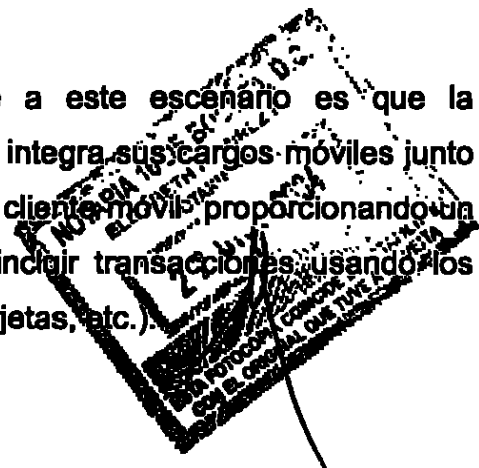
[0024] Este acercamiento puede usarse para todos los tipos de acceso autenticado como acceso VPN el acceso a través de Firewall (Cortafuegos) a la corporación segura. De forma similar, esto pudo pasar sobre una infraestructura inalámbrica como (por ejemplo IrDA, Bluetooth, o 802.11x). Por ejemplo, la figura debajo ilustrada usando tal autenticación inalámbrica como un cajero automático para retiro de efectivo.

[0025] En la Autenticación que usa el escenario de SIM Móvil. La información de la facturación y firmado en el encabezado de SOAP puede ser, por ejemplo, la ficha de seguridad proporcionada por el proveedor de identidad. EL PIN.

Acceso Federado a Los Recursos y a la Centralización de Facturación.

[0026] En este escenario, un cliente móvil usa su proveedor de identidad móvil para acceder a un conjunto de sitios de comercio, algunos de sus clientes móviles y otros de su PC (teniendo autenticados con su IP móvil). En la medida en que las transacciones comerciales tengan lugar, los comerciantes certifican la IP móvil, que actúa como un pseudo-banco que consolida los cargos al usuario móvil en la facturación mensual.

[0027] De nuevo un aspecto importante a este escenario es que la declaración de la publicación mensual del cliente integra sus cargos móviles junto con cualquier otro cargo cargado en cuenta a su cliente móvil proporcionando un solo ciclo de facturación integrado que puede incluir transacciones usando los mecanismos de cobro físicos tradicionales (las tarjetas, etc.).



111

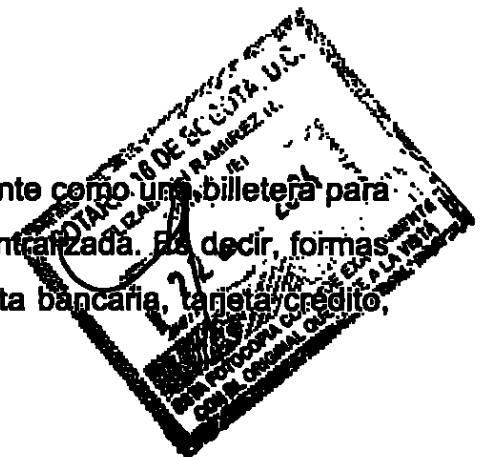
193
188

[0028] Consideremos cómo la especificación de los Servicios Web podría usarse para habilitar este escenario. Un usuario móvil establece una conexión con el servicio deseado y obtiene la política WS (WS-policy) para comunicarse con el servicio. Basado en la política, el cliente móvil, intenta obtener una ficha de seguridad para acceder al servicio proporcionando la identidad apropiada de la información registrada en el dispositivo móvil (o en un servicio pseudónimo de atributo asociado como es descrito en la federación WS). Usando WSTrust, después de la autenticación exitosa, el cliente móvil está permitido para acceder un ficha de acceso (token) para el servicio. El cliente realiza las transacciones seguras entonces con la máquina que usa WS-Reliability (WS fiable) y WS-Transaction (WS de Transacción) basado en los requerimientos de fiabilidad deseada y envía las órdenes para los productos y servicios. El cliente móvil y el servicio usan la información en la facturación y firma de los títulos para procesar el orden, proporcionan la información de facturación, y genera facturas o requerimiento débito. El portador móvil actúa como el banco para las facturas y demandas del débito y los agrega a la declaración de la publicación mensual del cliente.

[0029] En concordancia, en este escenario, la facturación y firma de los encabezados pueden incluir la dirección de la factura, la suma para ser debitada, la cuenta a ser debitada, el identificador de la factura, el identificador de la orden, el número de confirmación, o cualquier otra información de facturación u otra información útil para procesar la orden para generar la factura o el requerimiento del débito.

Billetera Móvil

[0030] El cliente móvil también puede actuar simplemente como una billetera para las opciones de comercio más allá de la facturación centralizada. Es decir, formas electrónicas de opciones del comercio diferentes (tarjeta bancaria, tarjeta crédito,



120

tarjeta del almacén, las tarjetas pre-pagadas, etc.) pueden guardarse en el cliente móvil y puede usarse seguramente cuando sea necesario.

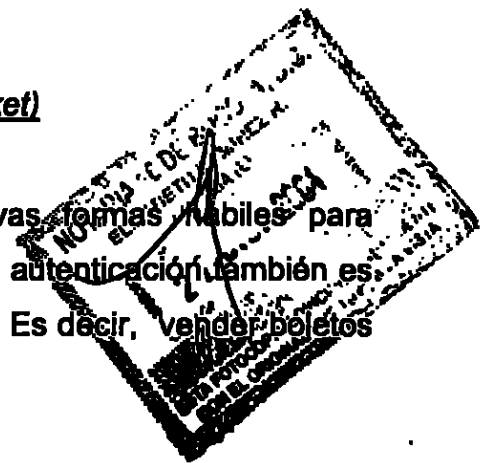
[0031] Considere el escenario dónde un usuario móvil entra en una tienda y selecciona la mercancía y servicios que ellos desean comprar. El cajero suma la compra mientras el usuario móvil selecciona el método de pago ellos deciden y envían la información del pago al cajero sobre PAN (por ejemplo, IrDA, Bluetooth, ó 802.11 x). Como es apropiado, un paso de autenticación también puede tener lugar. La transacción se acepta y el mecanismo de pago especificado se usa para completar el pago (por ejemplo una tarjeta de crédito normalmente usada). Esto se ilustra en la figura de abajo:

[0032] El uso de los protocolos de los Servicios Web en este escenario es muy similar a aquéllos en la sección anterior sólo que el procesador del débito no es el portador móvil, pero otro comerciante como una compañía de tarjeta de crédito o un banco. Para las compañías de tarjeta de crédito el cargo aparece en su factura mensual y para los bancos puede aparecer como un débito directo, por ejemplo, una cuenta corriente.

[0033] En este escenario, el factura y firma de los títulos pueden incluir forma de pago, los números de cuenta (como crédito, débito, cuenta corriente u otros números de cuenta), una firma electrónica que autoriza el cargo, un número PIN si aplica, o cualquier otra facturación o información de autorización útil para completar la transacción.

Boleto Electrónico (Electronic Ticket)

[0034] El cliente móvil también puede tomar nuevas formas móviles para autenticación y etiquetado. Desde que el mecanismo de autenticación también es un proceso inteligente y un sistema de almacenamiento. Es decir, vender boletos



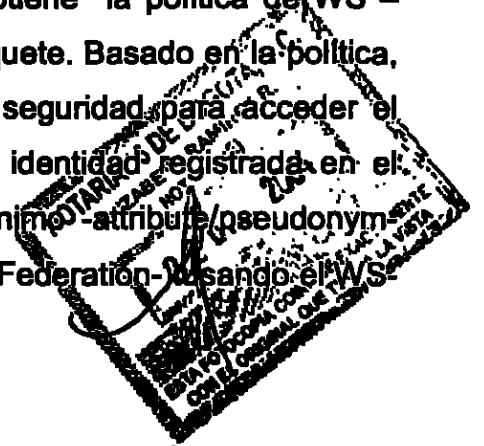
es el proceso por cuál una forma de autenticación, además de alguna transacción comercial, produce una nueva autenticación que es buena solo para los usuarios restringidos. Por ejemplo, un boleto plano, un boleto de tren, accede al parque zoológico, etc.

[0035] Un escenario que integra todo esto junto es un boleto de tren electrónico. En este escenario un cliente móvil usa su dispositivo para comprar un grupo de boletos fijo para su tren conmutador y, como resultado, la transacción se carga en cuenta a su proveedor móvil y los boletos se emiten electrónicamente al dispositivo móvil. Cuando el usuario móvil entra en la estación del tren ellos usan el PAN (por ejemplo IrDA, Bluetooth, o 802.11x) para emitir el boleto al sistema de seguridad que entonces autoriza que ellos entren en el área del tren. Éste es ilustrado en la figura de abajo.

[0036] En algunos escenarios se requiere además del boleto y por esta razón el usuario móvil puede necesitar proporcionar confirmación de identidad entrando un código dentro de su dispositivo móvil como lo ilustrado en la figura de abajo:

[0037] Un escenario alternativo permitiría el acceso del usuario móvil al tren y entonces realizar el intercambio del boleto y autenticación con el conductor que más estrechamente en paralelo para algún mecanismo de etiquetado existente.

[0038] De nuevo las interacciones de los servicios Web aquí son previamente bastante similares a aquéllos discutidos. Un usuario móvil establece una conexión con el servicio del boleto deseado y obtiene la política de WS – (WS-policy) para la comunicación con el servicio del tiquete. Basado en la política, el cliente móvil intenta obtener una ficha (token) de seguridad para acceder el servicio proporcionando la apropiada información de identidad registrada en el dispositivo móvil (ó en un servicio de atributo/seudónimo -attribute/pseudonym asociado como se describe en la federación WS -WS-Federation- usando el WS-



de confianza (WS-Trust). Después de la autenticación exitosa, el cliente móvil emite una ficha de acceso al servicio del boleto. El cliente realiza las transacciones seguras entonces con la máquina que usa la WS de fiabilidad (WS-Reliability) y WS de Transacción -WS-Transaction- (basado en los requerimientos de fiabilidad deseados) y somete las órdenes para los boletos. El cliente móvil y el servicio usan los encabezados de la facturación y firma la información para procesar la orden de información de facturación, y genera facturas o requerimientos débito. También, el servicio de boleto retorna un conjunto de -uno en tiempo- tiquetes de un solo uso cada uno conteniendo un número de serie y la información de validación y uso (usage/validity).

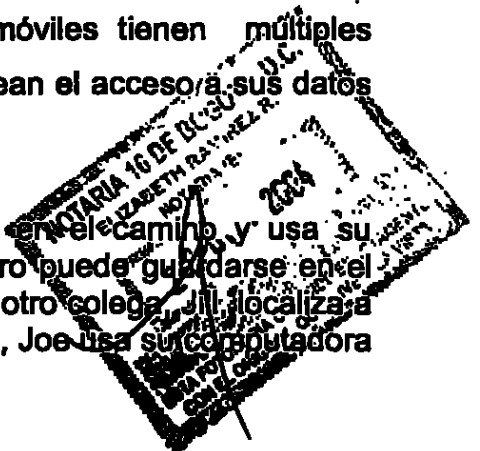
[0039] Cuando el cliente móvil se acerca el servicio de recibo de boleto (después de obtener la información de la política y de autenticación opcional) puede transmitir entonces firmemente el boleto usando WS de seguridad (WS-Security) y/o WS de Conversación (WS-SecureConversation).

[0040] En este escenario, la facturación y firmando del encabezado pueden incluir cualquier información útil para procesar la orden, proporcionar la información de facturación, o generar una factura o requerimiento débito.

PIM Remoto

[0041] El uso de administradores de información personales (PIMs) es ubicuo, sin embargo, ellos a menudo carecen de la federación y de la habilidad de habilitar la verdadera movilidad en eso caso algunos usuarios móviles tienen múltiples dispositivos móviles - es decir, los usuarios móviles desean el acceso a sus datos federados cuando quieran, y desde cualquier dispositivo.

[0042] Por ejemplo, un usuario móvil, Joe, está en el camino y usa su teléfono celular para llamar a un colega, Beth. El número puede guardarse en el teléfono, pero vino de un PIM federado. En una reunión, otro colega, Jill, localiza a Joe que usa IM a un dispositivo móvil diferente. Después, Joe usa su computadora



123

portátil para enviar el correo electrónico a Jill y Beth desde un punto de acceso móvil.

[0043] Este escenario ilustra el valor de los datos PIM centralmente accesibles. Sin embargo, en un ambiente federado, los datos son realmente distribuidos. Por ejemplo, Joe guarda todos sus datos de PIM en su proveedor móvil. Él tiene una lista de contactos, pero más que tener un contenedor de contactos real, que pueden envejecer rápidamente, usa la federación para apuntar al almacén de atributos del contacto. Por consiguiente, la dirección del correo electrónico de Jill se encuentra buscando "Jill" como un contacto en la lista de Joe, y preguntando entonces para el la "dirección del correo electrónico" atributo para Jill.

[0044] Este acercamiento también permite compartir en general atributos más detallados como ubicación física que puede determinarse de su cliente móvil. Un escenario de ejemplo involucra un conjunto de cinco personas que trabajan juntos y han permitido la situación general de la información para ser visible como se ilustra en la figura de abajo.

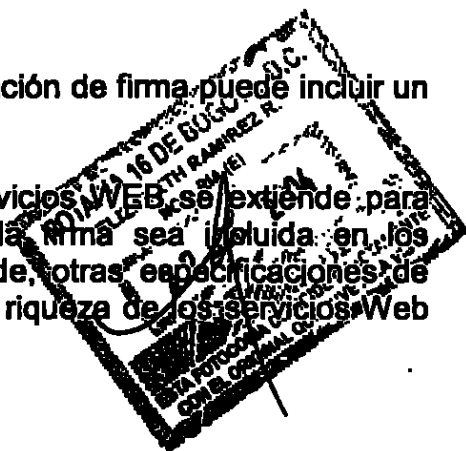
[0045] Alice nota que ella y Bob están en la misma área ("say city"), entonces Alice requiere la ubicación exacta de Bob. Bob no ha autorizado que Alice vea esta información, pero ha indicado que esa comprobación debe obtenerse. Por consiguiente, el cliente móvil de Bob ah dicho que Alice está requiriendo su localización exacta de Alice posiblemente, y la aprobación del requerimiento para proporcionar el información.

[0046] Bob autoriza esto y la información se envía a Alice.

[0047] Se mantienen el contacto e información de la presencia en el servicio del atributo proporcionado por WS-federado. Usando las especificaciones presentes, los clientes autorizados pueden obtener información detallada sobre la presencia y ubicación de la información (cuando es autorizado y disponible). Para casos dónde el acceso generalmente no es autorizado, temporalmente o el acceso a tiempo para la presencia/ubicación (o potencialmente cualquiera atributo federado) puede concederse.

[0048] En este escenario, la facturación y la información de firma puede incluir un PIM, mientras cargando en cuenta, o similares.

[0049] En concordancia, la arquitectura de los Servicios WEB se extiende para permitir que la facturación y la información de la firma sea incluida en los mensajes de la red además de, e independiente de, otras especificaciones de Servicios Web convencionales. En concordancia, la riqueza de los servicios Web

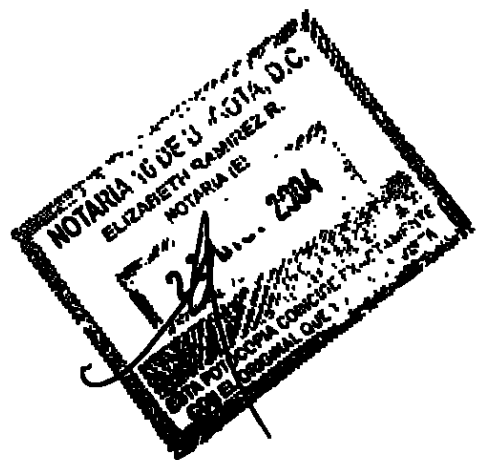


192
193
pueden obtener funcionalidad que habilita el comercio en un ambiente de red de computadoras interconectadas.

[0050] La arquitectura abajo del ilustra una posible operación en la cual los dispositivos móviles pueden comprometer las transacciones confiadas con los proveedores de servicio móviles.

[0051] Sin embargo, como previamente se mencionó, los principios de la invención presente no están limitados a la operación de un ambiente móvil.

[0052] La invención presente puede ser incluida en otras formas sin partir de su espíritu o las características esenciales. Las personalizaciones descritas serán consideradas en todos los aspectos sólo como ilustrativo y no restrictivo. El alcance de la invención es, por consiguiente, indicado por las demandas añadidas en lugar de por la descripción anterior. Todos los cambios que vienen dentro del significado y rango de equivalencia de las demandas son para ser incluidos dentro de su alcance.



DEMANDAS

222
194

1. Uno o más medios de comunicación legibles por computadora que tienen incluida la cubierta SOAP comprenden lo siguiente:

una porción de cuerpo de SOAP; y

un porción del encabezado de SOAP, en donde la porción del encabezado de SOAP incluye lo siguiente:

un encabezado que incluye la información de la factura.

2. Uno o más medios de comunicación legibles por computadora de acuerdo con la Demanda 1, en qué, el encabezado de SOAP incluye lo siguiente:

un encabezado que incluye la información de la firma.

3. Uno o más medios de comunicación legibles por computadora que tienen incluida la cubierta SOAP comprendiendo lo siguiente:

una porción de cuerpo de SOAP; y

una porción del encabezado de SOAP, en donde la porción de título de SOAP incluye lo siguiente:

un encabezado que incluye la información de la firma.

4. Uno o más medios de comunicación legibles por computadora que tiene por lo tanto un mensaje electrónico comprendiendo lo siguiente:

una porción del cuerpo; y

una porción del encabezado que incluye la información de la factura.

5. Uno o más medios de comunicación legibles por computadora de acuerdo con Demanda 4, en qué, la porción del encabezado incluye un título que incluye más allá la información de la firma.

6. Uno o más medios de comunicación legibles por computadora que tiene por lo tanto un mensaje electrónico

comprendiendo lo siguiente:

una porción del cuerpo; y

un porción del título que incluyen la información de la firma.



172

2° EXAMEN DE FORMA, PATENTE DE INVENCION

195

Radicación N° **04-106330**

Folio ~~200~~

Concepto Técnico N° **757**

Clasificación Internacional de Patentes: **G06F 17/60**

Practicado el examen de acuerdo a lo establecido en el Art. 38 de la Decisión 486, se determinó que esta solicitud de Patente:

- SI ☒ NO ☐ Contiene un resumen de la invención (Art. 26-e)
- SI ☒ NO ☐ Contiene el título o nombre de la invención (Art. 27-d)
- SI ☒ NO ☐ Contiene la descripción de la invención (Art. 26-b)
- SI ☒ NO ☐ NO ES APLICABLE ☐ Contiene los dibujos necesarios para comprender la invención (Art. 26-d)
- SI ☒ NO ☐ Contiene una o más reivindicaciones (Art. 26-c)
- SI ☐ NO ☐ NO ES APLICABLE ☒ Han sido desarrollados los productos a partir de recursos genéticos o de sus productos derivados de los que cualquiera de los Países Miembros es país de origen (Art. 26-h)
- SI ☐ NO ☐ NO ES APLICABLE ☒ Los productos y o procedimientos han sido obtenidos o desarrollados a partir a partir de los conocimientos tradicionales de las comunidades indígenas, afro americanas, o locales de los Países Miembros, de acuerdo a lo establecido en la Decisión 391 y sus modificaciones y reglamentaciones vigentes (Art. 26-i)
- SI ☐ NO ☒ La invención se refiere a un producto relativo a un material biológico (Art. 26-j)
- SI ☒ NO ☐ NO ES APLICABLE ☐ La prioridad coincide con la materia reivindicada.
- SI ☒ NO ☐ **CUMPLE LOS REQUISITOS TÉCNICOS**

OBSERVACIONES Y OTROS: SI ☐ NO ☐ Ver hoja(s) anexa(s)

EXAMINADOR TÉCNICO: 202051

Bogotá D C, octubre 07 de 2005.

2020
Bogotá D C

Doctor(a):
DARIO CARDENAS NAVAS.
Apoderado (a)

REFERENCIA:	Radicación N°	04-106330
	Trámite	002
	Evento	001
	Actuación	416
	Oficio N°	1011
	Folios	001

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, conforme lo establece el artículo 40 de la Decisión 486, a partir del 22 de abril de 2006.

Cúmplase
Dado en Bogotá D C,

11 OCT. 2005


ALIX CARMENZA CÉSPEDES DE VERGEL
Jefe División de Nuevas Creaciones.

202051