(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 December 2008 (11.12.2008)

PCT

(10) International Publication Number
WO 2008/148664 A1

(51) International Patent Classification:
*H04L 29/08* (2006.01)

(21) International Application Number:
PCT/EP2008/056466

(22) International Filing Date: 27 May 2008 (27.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07011126.5 6 June 2007 (06.06.2007) EP

(71) Applicant *(for all designated States except US)*: **AXALTO S.A.** [FR/FR]; 6, rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **JOFFRAY, Olivier** [FR/FR]; 74, résidence De Grasse Village, F-78810 Feucherolles (FR). **SMADJA, Philippe** [FR/FR]; 13, domaine des 3 clés, F-78470 St Remy Les Chevreuse (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

(54) **Title:** METHOD OF MANAGING COMMUNICATION BETWEEN AN ELECTRONIC TOKEN AND A REMOTE WEB SERVER

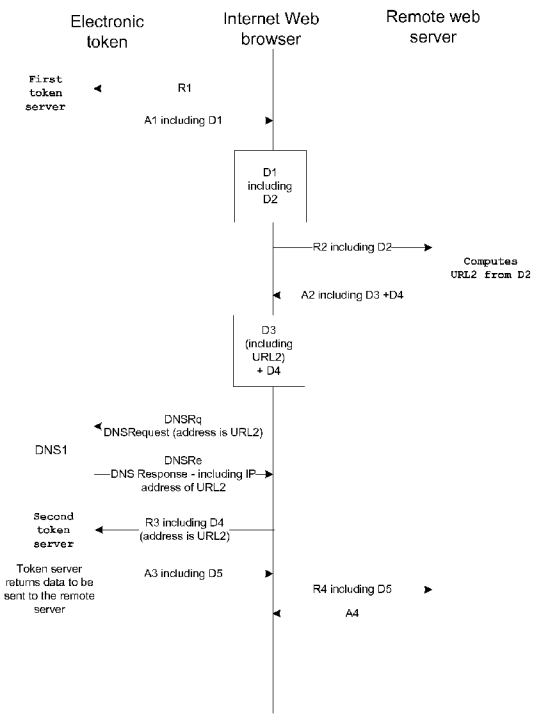


FIG.4

(57) **Abstract:** The invention is a method of managing communication between an electronic token and a remote web server. The token and the server are connected to a same host machine. The token comprises first and second token servers and a memory comprising HTML data. The host machine has an Internet web browser. Said method comprises the steps of : - sending a first request from the Internet web browser to the first token server, - returning a first answer to the Internet browser, said first answer comprising HTML data including a connection information associated to a script, - on the Internet web browser, executing the script associated to the connection information. Script execution establishes a connection to the remote server allowing a two-way communication between the second token server and the remote server through the Internet browser acting as a gateway.

WO 2008/148664 A1

# METHOD OF MANAGING COMMUNICATION BETWEEN AN ELECTRONIC TOKEN AND A REMOTE WEB SERVER

## (Field of the invention)

The present invention relates to methods of managing communication between an electronic token and a remote server. It relates particularly to methods of managing communication between an electronic token comprising a server and a remote web server.

## (Prior art)

Electronic tokens are portable electronic objects like smart cards, portable audio devices, mobile handsets, personal digital assistants or USB tokens. The word "Internet" means "interconnected networks". Electronic tokens may embed a local network comprising a hypertext transfer protocol HTTP server, a local Domain name system DNS server, or a dynamic host configuration protocol DHCP server. Alternatively, the local network can be a combination of these servers. The local network may comprise a unique or several local servers combining the functions of a HTTP and/or DNS and/or DHCP and/or the function of any server or service according to the World Wide Web consortium rules (W3C), said servers having a unique IP address.

An electronic token may be connected to a host machine. A host machine may be connected to a remote

server through Internet. A remote server is a distant server placed on a machine reachable through Internet. When both a remote server and an electronic token are connected to the same host machine, the remote server and the electronic token may communicate through the host machine. Existing host machines connected to Internet have an Internet web browser like Microsoft Internet Explorer ® or Mozilla Firefox ®.

At present for establishing a communication between an electronic token and a remote server the host machine must be customized using the Internet connection sharing mechanism or by installing dedicated software ensuring the same function. However customization of a host machine may be limited or forbidden by administration rights.

**(Summary of the Invention)**

The invention aims at allowing communication between an electronic token and a remote server through a host machine without customization of said host machine. The invention aims at allowing the communication connection and the automatic routing of data between the electronic token and the remote server in both directions.

The object of the present invention is a method of managing communication between an electronic token and a remote web server. The electronic token is connected to a host machine and comprises a

microprocessor, a communication interface and a memory. Said memory comprises an operating system and at least a first HTML data. Said electronic token comprises at least first and second token servers. The remote web server is connected to the same host machine. The host machine has an Internet web browser. Said method comprises the steps of:

- sending a first request from the Internet web browser to the first token server,
- returning a first answer from the first token server to the Internet web browser, said first answer comprising a first HTML data, said first HTML data comprising connection information associated to a script,
- on the Internet web browser, executing the script associated to the connection information,

characterized in that execution of said script establishes a connection to the remote web server allowing a two-way communication between the second token server and the remote web server through the Internet web browser acting as a gateway.

The first HTML data may comprise second data and said method may comprise the further steps of:

- sending a second request from the Internet web browser to the remote web server, wherein said second request comprises the second data,
- on the remote web server, computing a specific URL based on the second data, said specific URL allowing connecting to the second token server,

- returning a second answer from the remote web server to the Internet web browser, said second answer including a third data comprising the specific URL,

- on the Internet web browser, routing said second answer received from the remote web server with a third request to the second token server.

The step of returning the second answer may be performed by a HTTP redirect function or by an HTML automatic submission function.

The electronic token may comprise a virtual local network comprising a local domain name server. The method may comprise the further steps of:

- sending a DNS request from the Internet web browser to the local domain name system DNS server, said DNS request comprising the specific URL,

- receiving a DNS answer comprising an IP address corresponding to the specific URL sent to the Internet web browser by the local domain name system DNS server.

The second answer may comprise a fourth data and the third request may comprise the fourth data.

The method may comprise the further steps of:

- in response to the third request, sending a third answer from the second token server to the Internet web browser, said third answer comprising a fifth data,

- routing said fifth data from the Internet web browser to the remote web server.

The second data may comprise a variable part which may be randomly set or computed according to a predefined sequence.

Each of said first and second token servers may be a HTTP server or a HTTPS server.

Said first and second token servers may be merged in a unique token server.

The connection information may comprise the script, or a script URL from where the script may be downloaded.

The script may be a javascript.

Another object of the invention is an electronic token which is intended to be connected to a host machine. The token contains a microprocessor, a communication interface and a memory. The memory comprises an operating system and at least a first HTML data. The token contains at least first and second token servers. The host machine has an Internet web browser and is connected a remote web server. The token is characterized in that the first HTML data comprises connection information associated to a script, said connection information being intended to be sent by the first token server. Execution of said script by the Internet web browser of the host machine establishes a connection to the remote web server allowing a two-way communication between the second token server and the remote web server through the Internet web browser acting as a gateway.

The token may be a smart card, a portable audio device, a mobile handset, a personal digital assistant or a USB token.

## (Brief description of the drawings)

Other characteristics and advantages of the present invention will emerge more clearly from a reading of the following description of a number of preferred embodiments of the invention with reference to the corresponding accompanying drawings in which:

- Figure 1 depicts schematically the architecture of an electronic token of smart card type according to the invention;
- Figure 2 depicts schematically the interaction between an electronic token, a host machine and a remote web server, according to the invention;
- Figure 3 is an example of sequence of steps for managing communication between an electronic token and a remote web server, according to the invention; and
- Figure 4 is an example of data exchanges between an electronic token, a host machine and a remote web server, according to the invention.

## (Detailed description of the preferred embodiments)

The invention may apply to any types of electronic token connected to a host machine. In this specification, the electronic token is a smart card but it could be any other kind of electronic token or portable device embedding a server.

An advantage of the invention is to allow an automatic treatment of data exchanged between an

electronic token and a remote web server thanks to a gateway managed by the Internet web browser of a connected host machine.

Figure 1 shows the architecture of a smart card as an example of an electronic token according to a preferred embodiment of the invention. The smart card ET contains a microprocessor MP, a communication interface INT and a memory MEM. The memory MEM contains an operating system OS and a first HTML data D1. The first HTML data D1 may corresponds to an HTML page content. The first HTML data D1 contains a connection information CI and a second data D2. The memory MEM may consist of a unique circuit or several circuits that may be of different types.

As shown in Figure 2, the smart card ET contains a first server CS1, a second server CS2 and a local domain name system DNS server DNS1. A host machine HM contains an Internet web browser WB. The Internet web browser WB has a script engine EN. A script engine is able to execute a script. In the below part of this document, when a script is executed by the Internet web browser WB, the script is executed by the script engine of the Internet web browser WB.

The smart card ET is connected to the host machine HM such as a personal computer by a card reader or a dedicated interface. The electronic token may be connected to the host machine by a contact link or a wireless link.

A remote web server RS is connected to the host machine HM by Internet only or by a combination of

several communication channels like Internet and an Over The Air (OTA) Telecom communication. A second domain name system DNS server DNS2 may be available on the Internet. DNS2 may returns IP address of server related names such as "***.MyCompany.com".

Figure 3 shows an example of a step sequence for managing the connection and data exchanges between an electronic token and a remote web server. First a user launches the Internet web browser WB on the host machine HM. In step S1, the user selects the first token server CS1 by typing the corresponding address in the Internet web browser WB. For example, the address to be reached may be http://john.smith.secure or https://john.smith.secure. A first request R1 is then sent to the server CS1 of the connected electronic token ET at step S2. Then a first answer A1 is returned to the Internet web browser WB of the host machine HM at step S3. This first answer A1 contains a first HTML data D1 corresponding to a first HTML page. The first HTML data D1 contains a connection information CI and a second data D2. The second data D2 is related to the second token server CS2. The first HTML page is displayed by the Internet web browser WB. This first HTML page offers to connect the remote server RS. Then the user chooses connecting the remote server RS. This connection may be automatic through HTTP redirect or HTML automatic submission function. During step S4, the Internet web browser WB extracts a script SC1 from the previously received connection information CI. Then the Internet web browser WB

executes the script SC1. The script execution sends a second request R2 to the remote server RS at step S6. This second request R2 contains the previously received second data D2. This second data D2 includes information identifying the server to be reached in the electronic token ET. At the step S7, the remote server RS computes a specific URL URL2 thanks to the second data D2. For example the second data D2 may contain the first part of the URL2 and the remote server RS may complete the computed specific URL by adding a complementary data specific to the token ET. Thus if the second data D2 provides "smartcard192_168_1_1" and the remote server RS adds "MyCompany.com" then the computed URL2 refers to "smartcard192_168_1_1.MyCompany.com". Then the computed URL2 may be resolved by DNS1 to the real IP address of the server CS2 in the token ET. For example, the real IP address of the server CS2 may be equal to 192.168.1.1.

Alternatively the computed URL2 may be resolved by the remote DNS2.

Then at step S8, the remote web server RS send a second answer A2 to the Internet web browser WB of the connected host machine HM. The second answer A2 contains third data D3 including the computed specific URL URL2.

The sending of the second answer A2 may be performed with a HTTP redirect function or with an HTML automatic submission function.

Alternatively, other functions of the Internet web browser may be embezzled as long as their use allows the automatic connection functions.

A remote URL URL1 is used for the second request R2. In a preferred embodiment, the remote URL URL1 belongs to the same domain as the computed specific URL URL2.

After receiving the second answer A2, the Internet web browser WB may send a request DNSRq to the domain name system DNS server DNS1 of the electronic token ET at step S9. This request DNSRq allows getting the IP address corresponding to the received URL2. Then, at step S10, the DNS1 server send back the IP address corresponding to URL2. This IP address corresponds to the second token server CS2.

Then the Internet web browser WB routes the second answer A2 to the second token server CS2 by sending a third request R3 to the token ET at step S11.

Additionally and as shown in Figure 4, the second answer A2 may contain a fourth data D4 intended to be used by the second token server CS2. In this case, the third request R3 contains the fourth data D4. For example, the fourth data D4 may be related to a new service available for the user. After reception of the third request R3, the first HTML data D1 may be updated in order to declare a new service according to the fourth data D4 content.

Alternately, a third answer A3 containing fifth data D5 may be sent to the Internet web browser WB by the second token server CS2 during step S12. This third

answer A3 may be routed to the remote web server RS by the Internet web browser WB of the host machine HM.

Thus two connections are established on the Internet web browser WB: one to the remote web server RS and another to the second token server CS2 using URL2.

Advantageously, the first token server CS1 may be a HTTP server or a HTTPS server. The second token server CS2 may be a HTTP server or a HTTPS server

Advantageously, first and second token servers CS1 and CS2 may be merged in a unique token server.

In the above example, the token ET comprises a virtual local network comprising a local domain name system DNS server DNS1. The invention also applies to electronic tokens ET not embedding a virtual local network.

Alternately, the Internet web browser WB may extracts a script URL URL3 from the received connection information CI during step S4. URL3 corresponds to an address where the script SC1 may be found. The script SC1 is then downloaded from URL3 and executed by the Internet web browser WB.

In a preferred embodiment the script SC1 is a javascript. The script SC1 may use the XMLHttpRequest API.

Advantageously, the second data D2 may comprise a variable part. The variable part may be randomly set or computed according to a predefined sequence. The variable part is made available for the DNS1.

An additional advantage of the invention is to secure the specific URL URL2 used for reaching the second token server CS2. The URL2 may change each time a connection to a remote web server RS is engaged. In all cases, both the remote web server RS and the DNS1 dynamically calculates URL2 from the same information.

Alternately a second domain name system DNS server DNS2 may be reachable from the host machine HM. When the sending of the second answer A2 is performed with a HTTP redirect function, DNS2 may be used if the electronic token has no DNS1. Moreover, DNS2 may be used if the electronic token is not an IP token and is accessed via a software proxy localized on the connected host machine HM. In such a case, the first request R1 may be addressed to the host machine address such as http://127.0.0.1:4116 instead of http://john.smith.secure and URL2 refers to name like "smartcard.MyCompagny.com" that is resolved to "127.0.0.1" by remote DNS2.

## CLAIMS (GEM2232)

1. A method of managing communication between an electronic token (ET) and a remote web server (RS), said electronic token (ET) being connected to a host machine (HM) and comprising a microprocessor (MP), a communication interface (INT) and a memory (MEM) comprising an operating system (OS) and at least a first HTML data (D1), said electronic token (ET) comprising at least first and second token servers (CS1, CS2), said remote web server (RS) being connected to the host machine (HM), said host machine (HM) having an Internet web browser (WB), said method comprises the following steps:

- sending (S2) a first request (R1) from the Internet web browser (WB) to the first token server (CS1),

- returning (S3) a first answer (A1) from the first token server (CS1) to the Internet web browser (WB), said first answer (A1) comprising a first HTML data (D1), said first HTML data (D1) comprising connection information (CI) associated to a script (SC1),

- on the Internet web browser (WB), executing (S5) the script (SC1) associated to the connection information (CI),

characterized in that execution of said script (SC1) establishes a connection to the remote web server (RS) allowing a two-way communication between the second token server (CS2) and the remote web server

(RS) through the Internet web browser (WB) acting as a gateway.

2. A method according to claim 1, wherein first HTML data (D1) comprises second data (D2) and wherein said method comprises the further steps of:

- sending (S6) a second request (R2) from the Internet web browser (WB) to the remote web server (RS), wherein said second request (R2) comprises the second data (D2),

- on the remote web server (RS), computing (S7) a specific URL (URL2) based on the second data (D2), said specific URL (URL2) allowing connecting to the second token server (CS2),

- returning (S8) a second answer (A2) from the remote web server (RS) to the Internet web browser (WB), said second answer (A2) including a third data (D3) comprising the specific URL (URL2),

- on the Internet web browser (WB), routing (S11) said second answer (A2) received from the remote web server (RS) with a third request (R3) to the second token server (CS2).

3. A method according to claim 2, wherein the step of returning (S8) the second answer (A2) is performed by a HTTP redirect function or by an HTML automatic submission function.

4. A method according to claims 2 or 3, wherein the electronic token (ET) comprises a virtual local

network comprising a local domain name server (DNS1), and wherein said method comprises the further steps of:

- sending (S9) a DNS request (DNSRq) from the Internet web browser (WB) to the local domain name system DNS server (DNS1), said DNS request (DNSRq) comprising the specific URL (URL2),
- receiving (S10) a DNS answer (DNSRe) comprising an IP address corresponding to the specific URL (URL2) sent to the Internet web browser (WB) by the local domain name system DNS server (DNS1).

5. A method according to claims 2, 3 or 4, wherein said second answer (A2) comprises a fourth data (D4), and wherein said third request (R3) comprises the fourth data (D4).

6. A method according to claims 2, 3, 4 or 5, wherein said method comprises the further steps of:

- in response to the third request (R3), sending (S12) a third answer (A3) from the second token server (CS2) to the Internet web browser (WB), said third answer (A3) comprising a fifth data (D5),
- routing (S13) said fifth data (D5) from the Internet web browser (WB) to the remote web server (RS).

7. A method according to claims 2, 3, 4, 5 or 6, wherein second data (D2) comprises a variable part, said variable part being randomly set or computed according to a predefined sequence.

8. A method according to any one of the previous claims, wherein each of said first and second token servers (CS1, CS2) is a HTTP server or a HTTPS server.

9. A method according to any one of the previous claims, wherein said first and second token servers (CS1, CS2) are merged in a unique token server.

10. A method according to any one of the previous claims, wherein said connection information (CI) comprises the script (SC1), or a script URL (URL3) from where the script (SC1) may be downloaded.

11. A method according to any one of the previous claims, wherein said script (SC1) is a javascript.

12. An electronic token (ET) intended to be connected to a host machine (ME), said token (ET) containing

- a microprocessor (MP),
- a communication interface (INT)
- a memory (MEM) comprising an operating system (OS) and at least a first HTML data (D1),
- at least first and second token servers (CS1, CS2),

said host machine (ME) having an Internet web browser (WB) and being connected a remote web server (RS)

said token (ET) being characterized in that the first HTML data (D1) comprises connection information (CI) associated to a script (SC1), said connection

information (CI) being intended to be sent by the first token server (CS1), and in that execution of said script (SC1) by the Internet web browser (WB) establishes a connection to the remote web server (RS) allowing a two-way communication between the second token server (CS2) and the remote web server (RS) through the Internet web browser (WB) acting as a gateway.

13. An electronic token (ET) according to claim 12, wherein said token is a smart card, a portable audio device, a mobile handset, a personal digital assistant or a USB token .

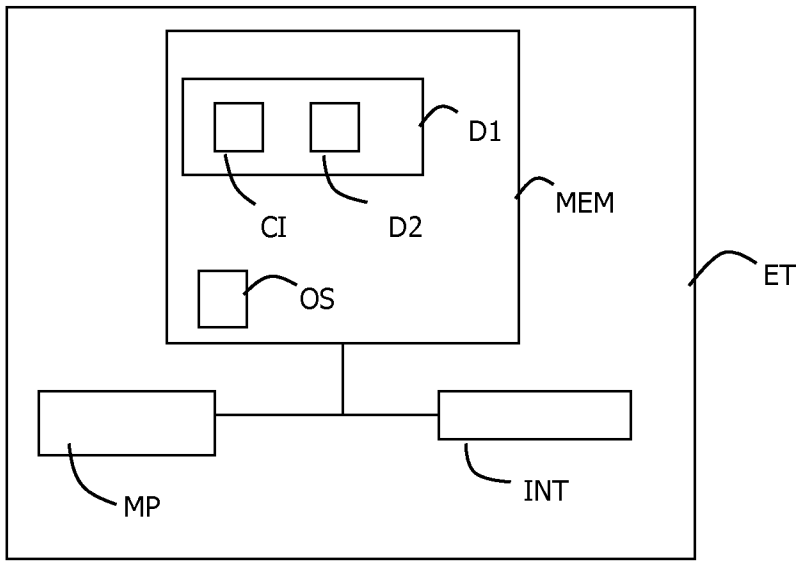


FIG.1

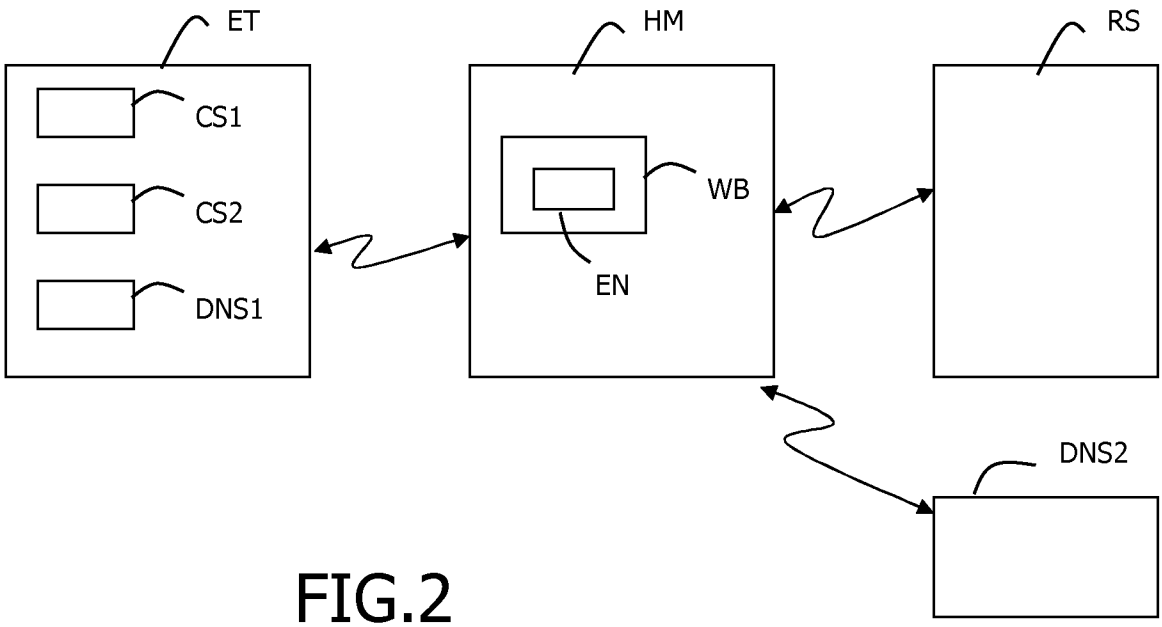


FIG.2

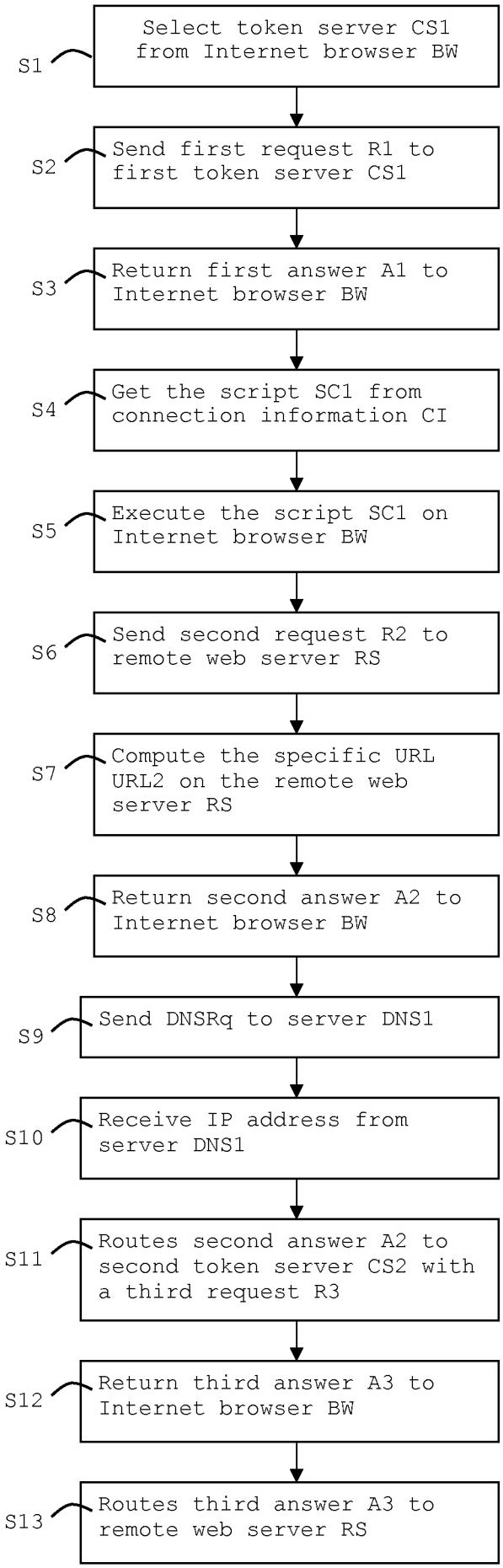
S1
Select token server CS1 from Internet browser BW
S2
Send first request R1 to first token server CS1
S3
Return first answer A1 to Internet browser BW
S4
Get the script SC1 from connection information CI
S5
Execute the script SC1 on Internet browser BW
S6
Send second request R2 to remote web server RS
S7
Compute the specific URL URL2 on the remote web server RS
S8
Return second answer A2 to Internet browser BW
S9
Send DNSRq to server DNS1
S10
Receive IP address from server DNS1
S11
Routes second answer A2 to second token server CS2 with a third request R3
S12
Return third answer A3 to Internet browser BW
S13
Routes third answer A3 to remote web server RS

FIG.3

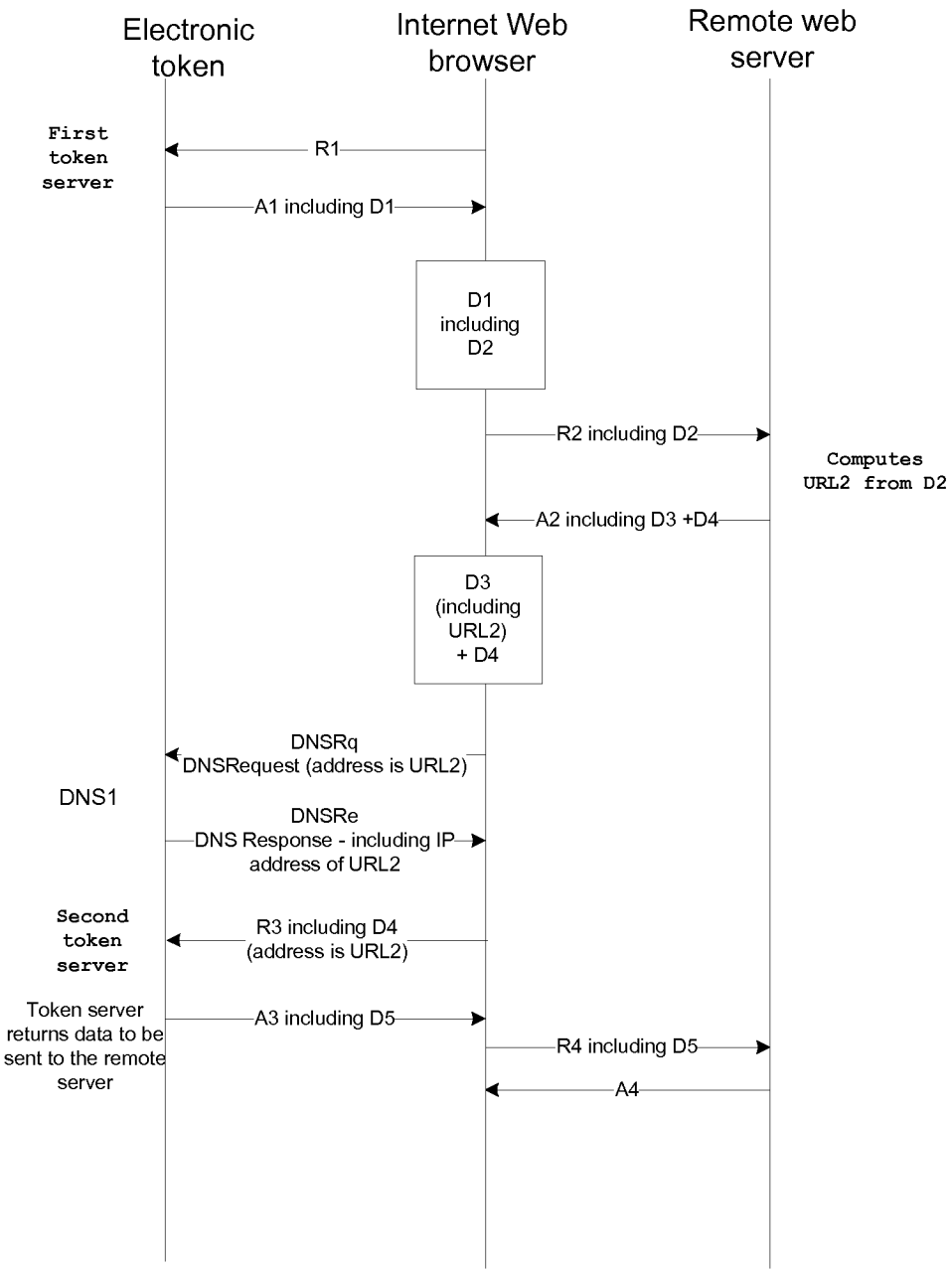
Electronic token
Internet Web browser
Remote web server
First token server
R1
A1 including D1
D1 including D2
R2 including D2
Computes URL2 from D2
A2 including D3 +D4
D3 (including URL2) + D4
DNSRq
DNSRequest (address is URL2)
DNS1
DNSRe
DNS Response - including IP address of URL2
Second token server
R3 including D4 (address is URL2)
Token server returns data to be sent to the remote server
A3 including D5
R4 including D5
A4

FIG.4

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/056466

**A. CLASSIFICATION OF SUBJECT MATTER**
INV. H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 2005/064889 A (AXALTO SA [FR]; JOFFRAY OLIVIER [FR]) 14 July 2005 (2005-07-14)<br>page 1, line 4 - line 6<br>page 3, line 24 - page 4, line 16<br>page 7, line 25 - page 9, line 4<br>page 11, line 1 - line 26<br>figures 4-11 | 1-13 |
| A | URIEN P: "Internet card, a smart card as a true Internet node"<br>COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL,<br>vol. 23, no. 17,<br>1 November 2000 (2000-11-01), pages 1655-1666, XP004238469<br>ISSN: 0140-3664<br>* section 2. on pages 1655-1656 *<br>* section 5. on page 1658 *<br>figure 2 | 1-13 |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 21 July 2008 | 29/07/2008 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Homan, Peter |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/056466

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 2005064889 A | 14-07-2005 | NONE | |