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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 October 2011 (20.10.2011)

PCT

(10) International Publication Number
WO 2011/128432 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01) *H04W 84/04* (2009.01)

(21) International Application Number:
PCT/EP2011/055994

(22) International Filing Date:
15 April 2011 (15.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10305392.2 15 April 2010 (15.04.2010) EP

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LONKAR, Anvay** [IN/SG]; n°03-21 Block 694, Jurong West Central 1, Singapore 151076 (SG).

(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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

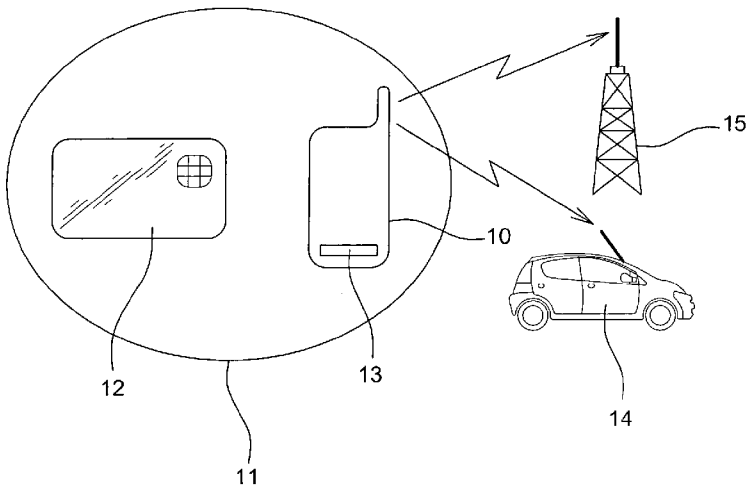
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,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

Published:

— *with international search report (Art. 21(3))*

WO 2011/128432 A1

(54) Title: SYSTEM FOR ACCESSING TO A TELECOMMUNICATION NETWORK, THE SYSTEM INCLUDING A TELECOMMUNICATION TERMINAL INSTALLED IN A VEHICLE



(57) Abstract: The invention concerns a system for accessing to a telecommunication network. The system includes a telecommunication terminal installed in a vehicle, the terminal being able to cooperate with a removable element belonging to a user, such as a card. The access of the terminal to the network is authorized only when a certificate included in the removable element is authenticated by the network. According to the invention, the removable element is the electronic driving license of the user.

System for accessing to a telecommunication network, the system including a telecommunication terminal installed in a vehicle

The present invention relates to a system for accessing to a telecommunication network, the system including a telecommunication terminal installed in a vehicle. The terminal is able to cooperate with a removable element belonging to a user, such as a card or a dongle, the access of the terminal to the network being authorized only when a digital key or certificate included in the removable element is authenticated by the network.

As described in US-2009260057, many automotive accidents are preventable if the vehicle driver is warned of a hazardous driving condition, or the vehicle itself reacts automatically to such a hazardous condition.

For example, a driver may cause a chain reaction accident by rapidly applying his or her brakes in order to avoid a collision. The drivers behind the vehicle are unable to brake sufficiently rapidly in order to avoid an accident thus resulting in a chain reaction accident. However, such an accident may theoretically be prevented, or at least the injuries and/or vehicular damages minimized, if the driver and/or vehicle potentially involved in the accident are able to react sufficiently rapidly to hazardous driving conditions in the vicinity.

For that reason, dedicated short range communications (DSRC) have been proposed to permit communication between automotive vehicles as well as vehicles and infrastructure for safety and other communications.

In managing the wireless communication between different vehicles, as well as between vehicles and infrastructure, the authenticity of the received messages is paramount. Without such authentications, the vehicles may receive wireless communications from parties who intentionally transmit incorrect information for whatever private purpose, as well as vehicles that, through malfunction, transmit incorrect information. Without authentication of the reliability of the received messages, unsafe traffic conditions, traffic congestion, etc. may result.

In order to enable automotive vehicles to communicate between themselves and optionally infrastructure, it has been proposed to form a vehicle ad hoc network (VANET) with the automotive vehicles that are within

range of interest for the automotive vehicle and in which each automotive vehicle forms one node in the network. Such vehicles would then communicate amongst themselves within the network providing safety information, such as the status or status of operation of each vehicle in the network as well as infrastructure adjacent the road.

In order to ensure authenticity of the messages received by vehicle nodes within the network, it has been proposed to use public key infrastructure (PKI) authentication of messages transmitted over the ad hoc network. At the root of a PKI is a trusted Certificate Authority (CA). This certificate authority may be a government agency or its proxy. One of the responsibilities of a CA is to clearly distinguish between trusted and non-trusted nodes. To the trusted nodes, the CA gives one or more certificates (a single vehicle may use more than one certificate in order to improve its privacy) or digital keys. Each certificate imparts the trust of the CA to the owner of the certificate. A node V1 wanting to validate the authenticity of another node (V2)'s messages must have a certificate for V2. Certificates can be pre-installed or exchanged at the time of first meeting. Other certificate exchange methods have also been proposed. Node V1 can authenticate the validity of the certificate of V2. If V2's certificate is valid, V1 can then trust V2.

In one example, the certificate comprises (at least) a certificate ID, which for all practical purposes, also becomes a pseudonym for the certificate owner, as well as a public key associated with this certificate ID, as well as the certificate authority's digital signature binding this association.

In order to ensure the trustworthiness of inter-vehicle messages received within the VANET, it is necessary that a list of all certificates that have been revoked not only be maintained, but also rapidly propagated throughout the entire vehicle communication system which includes all of the VANETs.

One previously known proposal to accomplish this has been to provide roadside equipment (RSE) at numerous locations along the roads throughout the entire area encompassing the vehicle communication system, e.g. the United States. Such RSEs would transmit repeatedly a list identifying the certificate authentications or signatures that have been revoked by the certificate authority. This list would then be received by vehicles passing

nearby the RSE and those vehicles would then update their list of certificate revocations so that any subsequent message received from a vehicle node having a revoked certificate will be disregarded.

The certificates are typically stored in a removable element such as a card or a dongle belonging to the driver of the vehicle. This card or dongle can be inserted in a telecommunication terminal installed in the car or inserted in a card or dongle reader connected to the telecommunication terminal. The access of the telecommunication terminal to the network is authorized only when the certificate included in the removable element is authenticated by the network.

The invention has the purpose to identify securely the sender of information in a telecommunication network, such as a VANET, thanks to its certificate, and to distribute, as a trusted CA (government body, vehicle association) the certificates that are required to secure the identity of the sender.

To this end, the invention proposes to store the certificate used to access the telecommunication network in the driving license of the driver of the vehicle. This means that the CA would be the driving license issuing authority.

As already mentioned, the telecommunication terminal installed in the vehicle cooperates then with the driving license of the user (driver) of the vehicle and the access of the terminal to the network is only authorized when the certificate included in the driving license is authenticated by the network.

Preferably, the telecommunication network is a VANET network or any network based on the 802.11 set of standards.

In another embodiment, the telecommunication network is a GSM, UMTS, WiFi, WiMax, Ad Hoc or LTE network.

Preferably, the telecommunication terminal is fixedly embarked in the vehicle.

The present invention will now be described in reference of the accompanying unique figure representing a system according to the present invention.

In the unique figure, a system for accessing to a telecommunication network is represented. The system includes a telecommunication terminal 10

installed in a vehicle schematized by 11. Preferably, the terminal 10 is fixedly embarked in the vehicle 11. The terminal 10 is able to cooperate with a removable element 12 belonging to a user. This removable element 12 is, according to the invention, the electronic driving license of the user of the vehicle (i.e. the vehicle driver). It can be in the form of a chip card, with or without contacts, or in the form of a dongle, like a USB dongle. The cooperation between the terminal 10 and the removable element 12 can be obtained by inserting the element 12 in a slot 13 provided in the terminal 10. The terminal 10 comprises classical reading means of the content of the driving license 12 and is able to read a certificate that has been stored therein by the driving license issuing authority. The terminal 10 reads this certificate and sends it to the network comprising mobiles stations 14 and/or fixed stations 15 (RSE). These stations proceed to the authentication of the certificate. If the authentication is positive, the driver of vehicle 11 is authorized to communicate with them, otherwise not.

The telecommunication network constituted by the vehicles 11, 14 and the RSE 15 is typically a VANET network. It can also be any network based on the 802.11 set of standards.

In another embodiment, the telecommunication network is a GSM, UMTS, WiFi, WiMax, Ad Hoc or LTE network.

Thus, the system of the invention proposes to distribute the keys for security in the driving license of its owner and then use them for whatever applications as deemed necessary. Giving an example, if we want to identify someone who has broken a law, it is possible to identify this person by sending out his name and driving license ID in addition to the license plate number, all secured by the keys present in his driving license. Since this fact can be standardized by the application, which will have a module running on the vehicle, one running at a RSE and another module running at a server (typically at an authority) - it will know what data to expect from this message.

The driving license can also be used as a key for running the vehicle: without driving license, the vehicle would not start. In addition, an automatic connection to the telecommunication network can be established. This permits to detect easily law brokers since their certificates are broadcasted in the

telecommunication network. It permits also to detect their position since RSEs can be installed in many places, for instance at road crossings.

With RSEs having a very small coverage, like micro-cells in the GSM system for example, it is possible to detect, with the help of radars, drivers who are driving too fast, to identify them thanks to their certificates and to send them directly fines. It is then no more possible to a driver to say to the police that someone else has committed the infraction since his certificate identifies him directly (it is no more possible for him to say that his grand-father for example was driving his vehicle).

The present invention also concerns a driving license comprising a certificate for accessing to a telecommunication network.

CLAIMS

1. A system for accessing to a telecommunication network, said system including a telecommunication terminal installed in a vehicle, said terminal being able to cooperate with a removable element belonging to a user, such as a card, the access of the said terminal to said network being authorized only when a certificate included in said removable element is authenticated by said network, characterized in that said removable element is the electronic driving license of the said user.

2. A system according to claim 1, wherein said telecommunication network is a VANet network or any network based on the 802.11 set of standards.

3. System according to claim 1, wherein said telecommunication network is a GSM, UMTS, WiFi, WiMax, Ad Hoc or LTE network.

4. System according to one of the claims 1 to 3, wherein said terminal is fixedly embarked in said vehicle.

5. Driving license comprising a certificate for accessing to a telecommunication network.

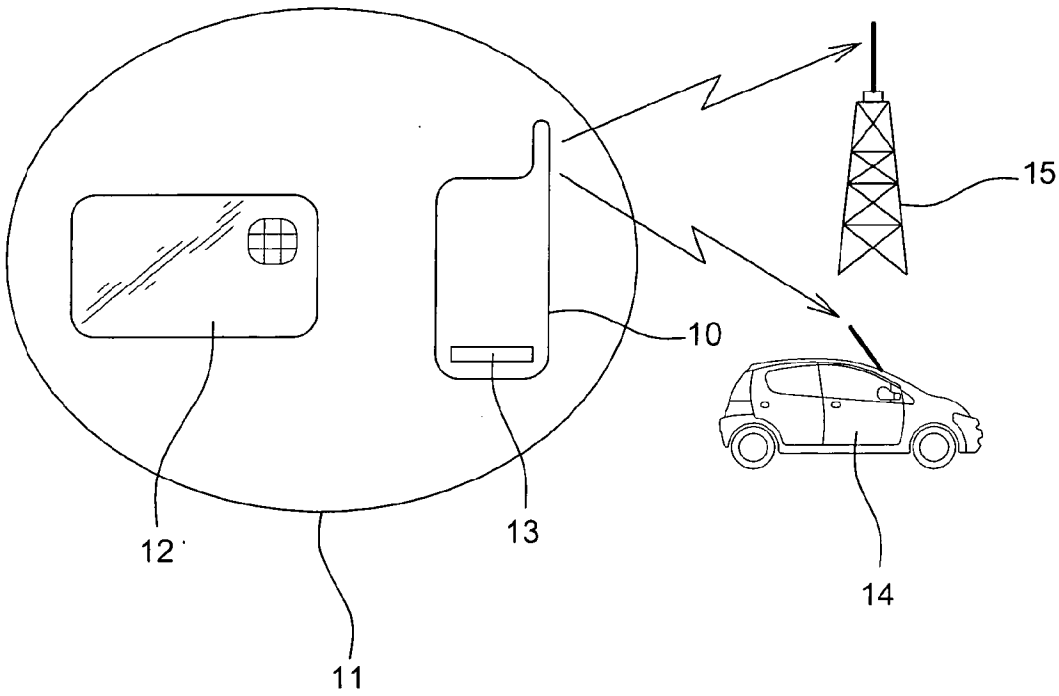


Figure unique

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/055994

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04L29/08
ADD. H04L29/06 H04W84/04

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 H04W

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	US 2002/188851 A1 (MIYAZAKI TATSUYA [JP]) 12 December 2002 (2002-12-12) abstract figures 1,7,10 paragraph [0008] paragraph [0012] paragraph [0014] paragraph [0020] paragraph [0023] paragraph [0027] - paragraph [0031] paragraph [0090] - paragraph [0093] -----	1-5
A	US 4 982 072 A (TAKIGAMI HIROSHI [JP]) 1 January 1991 (1991-01-01) abstract figure 1 column 1, line 7 - line 62 -----	1,5

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
5 July 2011	20/07/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kopp, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/055994

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/260057 A1 (LABERTEAUX KENNETH P [US] ET AL) 15 October 2009 (2009-10-15) cited in the application abstract paragraph [0008] - paragraph [0029]; figure 1 -----	1-5
X	US 2009/036164 A1 (ROWLEY PETER A [US]) 5 February 2009 (2009-02-05) abstract paragraph [0002] paragraph [0006] - paragraph [0009] paragraph [0012] paragraph [0016] paragraph [0018] - paragraph [0029] claim 1 figures 1,2 -----	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/055994

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002188851 A1	12-12-2002	JP 2002366675 A	20-12-2002
US 4982072 A	01-01-1991	JP 2556501 B2	20-11-1996
		JP 63195048 A	12-08-1988
US 2009260057 A1	15-10-2009	NONE	
US 2009036164 A1	05-02-2009	NONE	