(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
24. Oktober 2002 (24.10.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/084455 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/DE02/01167

(22) Internationales Anmeldedatum:
30. März 2002 (30.03.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 18 267.8 12. April 2001 (12.04.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Suttgart (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KOECHLING, Christian** [DE/DE]; Comeniusstrasse 4, 38102 Braunschweig (DE). **MAY, Thomas** [DE/DE]; Gruener Platz 7c, 38302 Wolfenbuettel (DE).

(81) Bestimmungsstaaten *(national)*: JP, US.

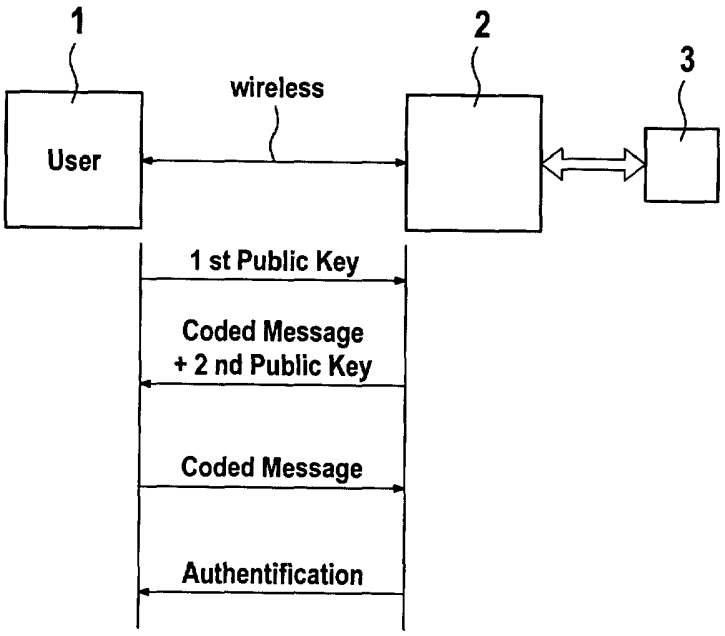
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR AUTHENTICATION OF A USER ON ACCESS TO A SOFTWARE-BASED SYSTEM BY MEANS OF AN ACCESS MEDIUM

(54) Bezeichnung: VERFAHREN ZUR AUTHENTIFIZIERUNG EINES ANWENDERS BEI EINEM ZUGANG ZU EINEM SOFTWAREBASIERTEN SYSTEM ÜBER EIN ZUGANGSMEDIUM



(57) Abstract: A method for authentication of a user on access to a software-based system by means of an access medium is disclosed, serving to simplify and speed up the authentication of a user. The user thus transmits his public code to the software-based system, which checks whether said user is already registered by means of said code. That being the case, the software-based system then transmits a character string, encoded with the first public code, to the user, said user decodes the same with a private key, and encodes the same with a key from the service server, then replies with the above to the service server. If the sent character string corresponds to the received character string, the software-based system recognises the user as authenticated.

(57) Zusammenfassung: Es wird ein Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium vorgeschlagen, das dazu dient, die Authentifizierung eines Anwenders einfacher und schneller zu gestalten. Dabei überträgt der Anwender seinen öffentlichen Schlüssel an das softwarebasierte System, das überpüft, ob anhand dieses Schlüssels der Anwender bereits registriert wurde. Ist das der Fall, dann überträgt das softwarebasierte System eine mit dem ersten öffentlichen Schlüssel codierte Zeichenkette zu dem Anwender, die dieser mit seinem privaten Schlüssel decodiert und mit einem Schlüssel des Diensteservers codiert und dann wieder zum diensteserver zurück überträgt. Entspricht nun die Zeichenkette, die gesendet wurde der, die empfangen wurde, dann erkennt das softwarebasierte System, dass der Anwender authentifiziert wurde.

WO 02/084455 A2

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium

Stand der Technik

Die Erfindung geht aus von einem Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System nach der Gattung des unabhängigen Patentanspruchs.

Es ist bereits bekannt, dass die Kommunikation über einen zugänglichen Kommunikationskanal zwischen zwei Parteien, wenn die Kommunikation geschützt sein soll, durch die Verwendung von öffentlichen und privaten Schlüsseln realisiert sein kann. Dabei ist es so, dass der öffentliche Schlüssel zur Codierung verwendet wird und dann der private Schlüssel zur Decodierung. Jede Partei weist also einen öffentlichen Schlüssel und dazugehörigen privaten Schlüssel auf, wobei die öffentlichen Schlüssel dann zur Kommunikation ausgetauscht werden. Dies wird auch und vor allem bei softwarebasierten Systemen eingesetzt.

Vorteile der Erfindung

Das erfindungsgemäße Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangssystem mit den Merkmalen des unabhängigen Patentanspruchs hat demgegenüber dem Vorteil, dass die Authentifizierung beim Zugang zu softwarebasierten Systemen, die im Folgenden auch als Diensteserver bezeichnet werden, verwendet wird. Dabei werden folgende Vorteile realisiert: Der Anwender ruft nur den Dienst auf und braucht kein Paßwort oder PIN (Persönliche Identifikationsnummer) einzugeben. Es wird keine sichere Kommunikationsverbindung benötigt, d.h. es ist nicht notwendig, sicherzustellen, dass die Verbindung nicht abgehört werden kann. Dies ist insbesondere beim Funkzugriff, beispielsweise über Bluetooth wichtig. Auf diese Weise müssen keine nachträglichen Änderungen in Standards wie Bluetooth vorgenommen werden. Das erfindungsgemäße Verfahren ermöglicht weiterhin eine Verschlüsselung der Kommunikation mit dem Dienst, so dass persönliche Daten nicht abgehört werden können. Der Diensteserver kann die Ermittlung der Identität des Nutzers und die damit verbundene Datenspeicherung an ein zentrales System, also einen Registrierungsserver delegieren, auf das beispielsweise verschiedene voneinander unabhängige Diensteserver Zugriff haben. Dadurch braucht der Nutzer sich nicht bei jedem Dienst mit einer neuen Kennung zu identifizieren, sondern er kann dieselbe Kennung für unterschiedliche Dienste verwenden. Der Diensteserver kann bei der weiteren Kommunikation mit dem Nutzer selbst sicherstellen, dass er immer mit demselben Nutzer kommuniziert. Der gegebenenfalls in Anspruch genommene Registrierungsserver ist in die weitere Kommunikation dann nicht mehr involviert.

Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen und Weiterbildungen sind vorteilhafte Verbesserungen des im unabhängigen Patentanspruch angegebenen Verfahrens zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium möglich.

Besonders vorteilhaft ist, dass als Zugangsmedium das Internet verwendet wird. Damit ist es möglich, beispielsweise mit einem tragbaren elektronischen Begleiter einen sicheren Zugang zu einem Dienst, der im Internet angeboten wird, zu erlangen. Solche Dienste sind beispielsweise Bankdienste oder auch Einkaufsmöglichkeiten im Internet, die einen Zahlvorgang, beispielsweise über Kreditkarte verlangen. Der elektronische Begleiter kann vorteilhafterweise ein Mobiltelefon, ein persönlicher digitaler Assistent, ein Smartphone oder eine Fernbedienung sein. Der elektronische Begleiter wird im Folgenden auch als Terminal bezeichnet. Der Diensteserver kann ein Steuergerät in einem Kraftfahrzeug, z.B. ABS-Steuergerät oder ESP-Steuergerät, ein Bordcomputer im Fahrzeug, ein Autoradio, ein Navigationssystem, ein Gateway-Modul in einem Fahrzeug, das über ein beliebiges Bussystem, z.B. der an CAN, MOST oder IEEE1394 angeschlossen ist, oder ein zentrales Navigationssystem bei einem Serviceprovider außerhalb des Kraftfahrzeugs sein. Der Bordcomputer in einem Fahrzeug kann auch als Terminal verwendet werden, um dann über die Verbindung über einen Dienstserver ein softwarebasiertes System anzuwählen.

Das Zugangsmedium kann dabei vorteilhafterweise zumindest teilweise über eine Funkstrecke realisiert sein, beispielsweise über Bluetooth oder eine Infrarotübertragungsstrecke.

Weiterhin ist es von Vorteil, dass ein Registrierungsserver vorhanden ist, der mit dem Dienstserver verbindbar ist und der überprüft, ob der öffentliche Schlüssel des Anwenders bereits registriert ist oder nicht.

Durch die Verwendung einer Chipkarte ist es möglich, dass unabhängig vom Terminal ein Nutzer seine Verschlüsselungsinformationen auf der Chipkarte mit sich führt und dann auch stationäre Terminals, die allgemein zugänglich sind, verwenden kann.

Zeichnung

Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und werden in der nachfolgenden Beschreibung näher erläutert. Es zeigt
Figur 1 ein Blockschaltbild der erfindungsgemäßen Vorrichtung und
Figur 2 ein Flußdiagramm des erfindungsgemäßen Verfahrens.

Beschreibung

Anwender, die Dienste über softwarebasierte Systeme, also über Diensteserver angeboten bekommen, brauchen, um diese Dienste zu nutzen, ein Verfahren zur Authentifizierung. Der Anwender hat dabei selbst ein softwarebasiertes System, d.h. ein Terminal, zur Verfügung, über das er auf den Dienst zugreift und das die direkte Kommunikation mit dem Dienst übernimmt. Beispiele hierfür sind ein Mobiltelefon oder ein Rechner mit Zugriff auf das Internet, wobei der Rechner entweder nur dem Anwender zugänglich ist und/oder mit einem Chipkarten-Lesegerät oder Ähnlichem ausgestattet ist. Auf diesem Chipkarten-Lesegerät können dann die persönlichen Zugangsdaten gespeichert sein.

In Figur 1 ist als Blockschaltbild die erfindungsgemäße Vorrichtung dargestellt. Ein Anwenderterminal 1, das mit User bezeichnet ist, weist hier nichtdargestellte Eingabevorrichtungen und Darstellungsvorrichtungen auf, mit denen ein Anwender Dienste auswählt und die Dienste dann nutzt. Dieses Anwenderterminal 1 ist hier über eine drahtlose Verbindung, die mir Wireless gekennzeichnet ist, mit einem Diensteserver 2 verbunden. Der Diensteserver 2 ist über einen zweiten Datenein-/-ausgang mit einem Registrierungsserver 3 verbunden.

Wenn sich nun der Anwender mit seinem Terminal 1 bei dem Diensteserver 2 anmeldet, werden folgende Botschaften übertragen. Zunächst überträgt der Anwender mit seinem Terminal seinen ersten öffentlichen Schlüssel, hier mit Public Key gekennzeichnet. Der Diensteserver 2 überträgt diesen Public Key zum Registrierungsserver 3, der überprüft, ob ein Anwender anhand dieses Public Keys bereits registriert wurde. Ist das der Fall, dann überträgt der Registrierungsserver 3 dem Diensteserver 2, dass der Anwender bereits registriert ist. Ist das nicht der Fall, dann überträgt der Registrierungsserver 1 eine Fehlermeldung an den Diensteserver 2, der daraufhin dem Terminal 1 ebenfalls eine Fehlermeldung überträgt. Optional ist es hier dann möglich, dass sich der Anwender über eine entsprechende Prozedur registrieren lässt.

Ist nun der Anwender als registriert erkannt, dann überträgt der Diensteserver 2 eine mit dem öffentlichen Schlüssel des Anwenders codierte Zeichenkette, die dem Diensteserver 2 allein bekannt ist, und zusätzlich einen zweiten öffentlichen Schlüssel, der für den Diensteserver 2 charakteristisch ist, d.h. der Diensteserver 2 weist einen zweiten privaten Schlüssel auf, mit dem der Diensteserver 2

die mit dem zweiten öffentlichen Schlüssel codierten Nachrichten dekodieren kann.

Der Anwender wird dann mit seinem Terminal 1 und seinem privaten Schlüssel die Zeichenkette decodieren und dann mit dem zweiten öffentlichen Schlüssel wieder codieren und schließlich dem Diensteserver 2 zurückschicken. Der Diensteserver 2 führt nun die Dekodierung mit dem zweiten privaten Schlüssel durch. Stimmt nun die Zeichenkette, die ursprünglich gesendet wurde, mit der empfangenen bei dem Diensteserver 2 überein, dann ist der Anwender authentifiziert und die Nutzung des Dienstes durch den Anwender mit seinem Terminal 1 kann beginnen. Dabei wird dann auch weiterhin die Codierung mit den jeweiligen öffentlichen Schlüsseln, die hier verwendet wurden, eingesetzt, um die Kommunikation sicher zu gestalten, wenn es insbesondere um finanzielle Transaktionen geht.

Figur 2 zeigt als Flußdiagramm das erfindungsgemäße Verfahren. In Verfahrensschritt 4 überträgt nun das User-Terminal 1 seinen öffentlichen Schlüssel über die drahtlose Verbindung zu dem Diensteserver 2. In Verfahrensschritt 5 überprüft der Registrierungsserver 3 für den Diensteserver 2, ob der Anwender 1 bereits registriert wurde. Dafür wird der öffentliche Schlüssel mit einer Datenbank des Registrierungsservers 3 abgeglichen. Alternativ ist es hier möglich, dass diese Überprüfung auch vom Diensteserver 2 selbst anhand einer entsprechenden Datenbank durchgeführt wird.

In Verfahrensschritt 6 wird nun überprüft, ob der Anwender registriert ist oder nicht. Ist das nicht der Fall, dann wird in Verfahrensschritt 7 die Authentifizierung abgebrochen und dies dem Anwender 1 mitgeteilt. Ist das jedoch der Fall, dann wird in Verfahrensschritt 8 von dem

Diensteserver 2 eine nur dem Diensteserver 2 bekannte Zeichenkette mit dem ersten öffentlichen Schlüssel codiert an den Anwender 1 übertragen und zusätzlich auch noch der zweite öffentliche Schlüssel, der für den Diensteserver 2 charakteristisch ist.

In Verfahrensschritt 9 decodiert nun der Anwender 1 mit seinem privaten Schlüssel die codierte Zeichenkette und codiert sie erneut mit dem zweiten öffentlichen Schlüssel des Diensteservers 2. Dies sendet der Anwender dann dem Diensteserver 2 wieder zurück. Der Diensteserver 2 wird dann in Verfahrensschritt 10 mit seinem privaten Schlüssel die Zeichenkette erneut decodieren und führt nun einen Vergleich durch, ob die ursprünglich gesendete Zeichenkette uncodiert mit der decodierten Zeichenkette übereinstimmt. Ist das der Fall, dann wird in Verfahrensschritt 11 entschieden, dass in Verfahrensschritt 13 nun der Dienst benutzt werden kann, da der Anwender authentifiziert ist. Wird in Verfahrensschritt 11 jedoch festgestellt, dass der Vergleich nicht zu einer Übereinstimmung führt, dann wird in Verfahrensschritt 12 dem Benutzer mitgeteilt, dass er nicht authentifiziert werden konnte. Gegebenenfalls kann sich hier dann eine Registrierung des Anwenders anschließen.

Benutzt der Anwender als Terminal 1 ein öffentliches Terminal, dann kann die Codierung und Decodierung sowie die Speicherung oder Bereitstellung der Schlüssel über eine Chipkarte erfolgen, die in das Terminal eingeführt wird. Der Zugang zu dem softwarebasierten System kann über das Internet erfolgen. Das Terminal 1 beziehungsweise der Diensteserver 2 und der Registrierungsserver 3 weisen dann entsprechende Schnittstellen auf.

Die Zeichenkette kann der Diensteserver 2 beispielsweise über einen Zufallsgenerator erzeugen. Wird als Terminal 1

ein elektronischer Begleiter verwendet, dann ist es möglich eine drahtlose Verbindung zu dem Zugangsmedium, zum Beispiel das Internet, zu realisieren.

Ansprüche

1. Verfahren zur Authentifizierung eines Anwenders bei einem Zugang zu einem softwarebasierten System über ein Zugangsmedium, wobei anwenderseitig ein erster privater und ein erster öffentlicher Schlüssel bereitgestellt werden, wobei sich der Anwender bei dem softwarebasierten System (2) anmeldet, dadurch gekennzeichnet, dass bei der Anmeldung der erste öffentliche Schlüssel zu dem softwarebasierten System (2) übertragen wird, dass das softwarebasierte System (2) anhand des ersten öffentlichen Schlüssels eine Berechtigung des Anwenders überprüft, dass einem berechtigten Anwender von dem softwarebasierten System (2) eine Zeichenkette mit dem ersten öffentlichen Schlüssel codiert und ein zweiter öffentlicher Schlüssel jeweils übertragen werden, dass anwenderseitig diese Zeichenkette mit dem ersten privaten Schlüssel decodiert wird und mit dem zweiten öffentlichen Schlüssel wieder codiert zu dem softwarebasierten System zurück übertragen wird und dass das softwarebasierte System den Anwender als authentifiziert erkennt, falls die vom Anwender empfangene und mit einem zweiten privaten Schlüssel decodierte Zeichenkette der von dem softwarebasierten System (2) codierten Zeichenkette entspricht.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass nach der Authentifizierung anwenderseitig zu übertragende Daten zu dem softwarebasierten System mit dem zweiten öffentlichen Schlüssel codiert werden und von Seiten des

softwarebasierten Systems (2) zu übertragende Daten mit dem ersten öffentlichen Schlüssel codiert werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass, wenn ein Anwender als nicht berechtigt erkannt wird, dies dem Anwender als Nachricht übertragen wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass als das Zugangsmedium das Internet verwendet wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zugangsmedium zumindest teilweise über eine Funkstrecke realisiert wird.

6. Vorrichtung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das softwarebasierte System einen Diensteserver (2) aufweist und anwenderseitig ein Terminal (1) vorhanden ist, wobei sowohl der Diensteserver (2) als auch der Terminal (1) jeweils eine Schnittstelle zu dem Zugangsmedium aufweisen.

7. Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass der Diensteserver (2) mit einem Registrierungsserver (3) verbindbar ist, wobei der Registrierungsserver (3) überprüft, ob der Anwender anhand des ersten öffentlichen Schlüssels berechtigt ist.

8. Vorrichtung nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass der Terminal (1) als elektronischer Begleiter ausgebildet ist.

9. Vorrichtung nach Anspruch 6, 7 oder 8, dadurch gekennzeichnet, dass der Diensteserver (2) als Multimediakomponente in einem Kraftfahrzeug ausgebildet ist.

10. Vorrichtung nach Anspruch 6, 7 oder 8, dadurch gekennzeichnet, dass der Diensteserver (2) ein Steuergerät in einem Kraftfahrzeug ist.

11. Vorrichtung nach einem der Ansprüche 6 bis 10, dadurch gekennzeichnet, dass die Vorrichtung eine Aufnahmevorrichtung für eine Chipkarte aufweist.

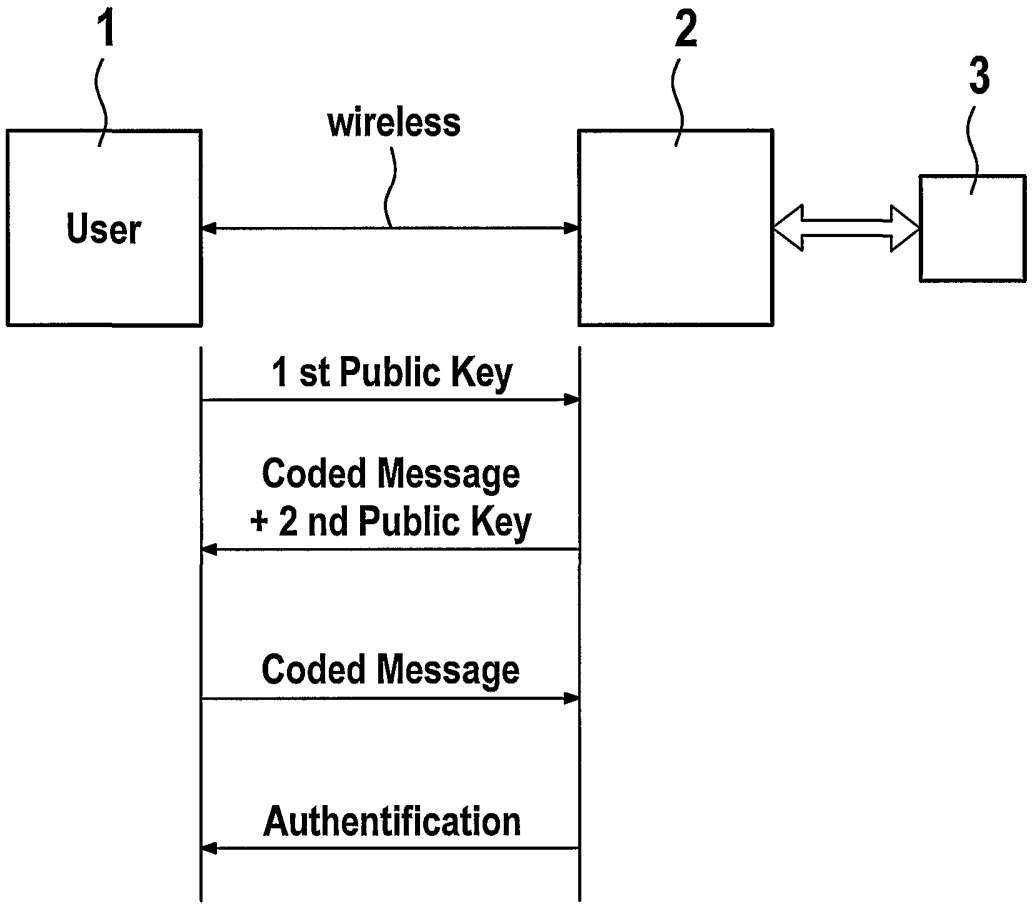

1
2
3
wireless
User
1 st Public Key
Coded Message
+ 2 nd Public Key
Coded Message
Authentification

FIG. 1

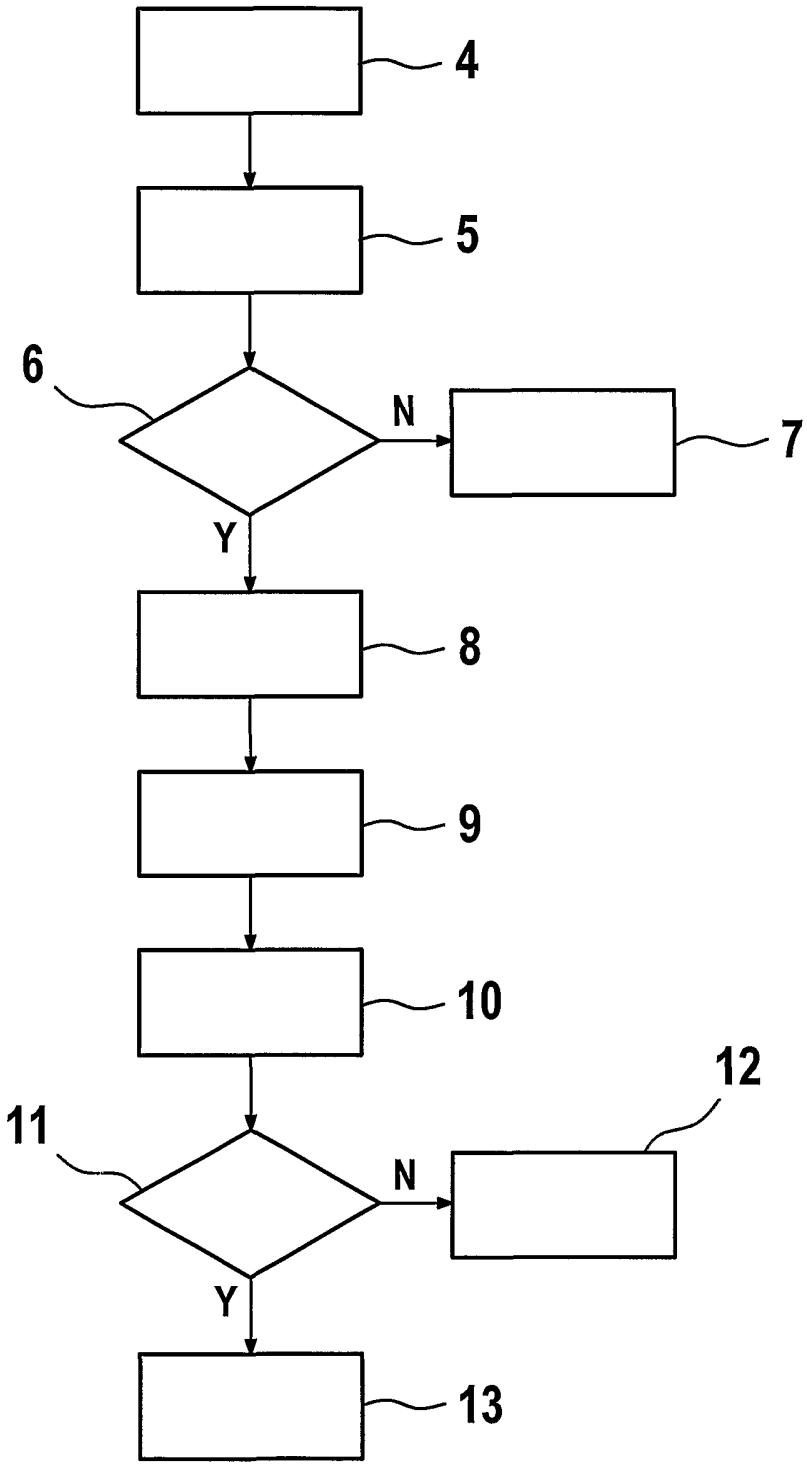


FIG. 2