Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2285093 C 2007/05/15

(11)(21) 2 285 093

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 1997/11/07
(87) Date publication PCT/PCT Publication Date: 1999/05/20
(45) Date de délivrance/Issue Date: 2007/05/15
(85) Entrée phase nationale/National Entry: 1999/09/29
(86) N° demande PCT/PCT Application No.: CH 1997/000424
(87) N° publication PCT/PCT Publication No.: 1999/024938

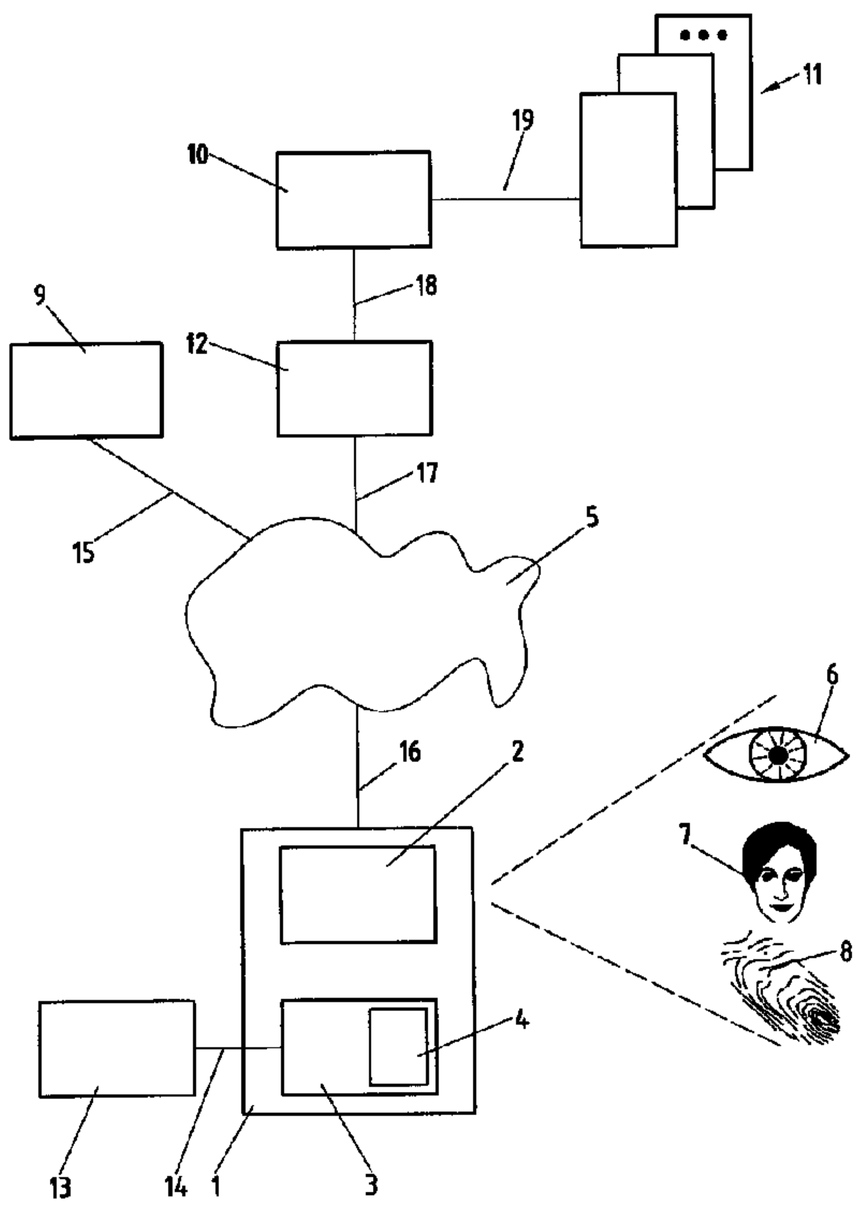
(51) Cl.Int./Int.Cl. *G07C 11/00* (2006.01), *G06F 21/00* (2006.01), *G06K 19/06* (2006.01), *G07C 9/00* (2006.01), *H04L 9/32* (2006.01)

(72) Inventeur/Inventor:
RITTER, RUDOLF, CH

(73) Propriétaire/Owner:
SWISSCOM MOBILE AG, CH

(74) Agent: MACRAE & CO.

(54) Titre : PROCEDE, SYSTEME ET DISPOSITIFS POUR L'AUTHENTIFICATION DE PERSONNES
(54) Title: METHOD, SYSTEM AND DEVICES FOR AUTHENTICATING PERSONS



(57) Abrégé/Abstract:
The invention concerns a method, system and devices for authenticating a user or group of users of a telecommunication transmitting apparatus, which consists in collecting the user's biometric codes, updated in a point of presence and stored in a biometric server as well as on personal SIM cards. The authentication is carried out by comparing current biometric codes with the biometric codes stored on the SIM cards by means of trusted third parties (TTP), the current biometric codes being retrieved from current video data transmitted by an integrated video detector to a telecommunication transmitting apparatus or an apparatus external thereto. Depending on the outcome of the authentication, the use of the telecommunication transmitting apparatus can be authorised or prohibited, or the result can be transmitted to an external protected device or still to an intermediate service supplier who, in turn, can respectively grant or deny access to the device and to the services.

ABSTRACT

The invention concerns a method, system and devices for authenticating a user or group of users of a telecommunication transmitting apparatus, which consists in collecting the user's biometric codes, updated in a point of presence and stored in a biometric server as well as on personal SIM cards. The authentication is carried out by comparing current biometric codes with the biometric codes stored on the SIM cards by means of trusted third parties (TTP), the current biometric codes being retrieved from current video data transmitted by an integrated video detector to a telecommunication transmitting apparatus or an apparatus external thereto. Depending on the outcome of the authentication, the use of the telecommunication transmitting apparatus can be authorised or prohibited, or the result can be transmitted to an external protected device or still to an intermediate service supplier who, in turn, can respectively grant or deny access to the device and to the services.

Method, System and Devices for Determining the Authenticity of Persons

The present invention relates to a method, a system and devices for determining the authenticity of a user or a group of users of a communication terminal device.

Aside from conventional methods for authenticating persons by means of photographs and personal identification papers, methods for authenticating persons by means of biometric features are also known in the prior art. In these methods, measurable and recordable body features are registered as biometric keys and, at the time of authentication, compared with the respective body features of a person to be authenticated. Known examples of such biometric features include fingerprints, eye patterns, facial contours, or voice characteristics.

It is also known that a personal computer (PC) can be equipped with means, an external video camera among others, which make it possible for the PC to record in a learning process and to reuse at a later point in time for authentication purposes the face, respectively some facial features, of a user, the PC granting the user access to the PC only if it recognizes the facial features.

The combination of video sensors with communication terminal devices is known in the context of video telephony, which is also available in a mobile version where a video camera is connected to a mobile radio telephone.

A method is described in DE 39 43 097 A1 which transfers biometrically measurable data, such as an eye pattern or a fingerprint, as search criteria over communication networks, among others by means of a mobile telephone, for retrieving stored medical data. Essentially, in this method, an individual is identified by means of biometric features in order to access his medical data. However, it is not the intention of this method to verify the authenticity of this individual nor to ensure the authenticity and the non-deniable origin of the data exchanged over the communication network in this method.

It is the object of this invention to propose a new and improved method and system for determining the authenticity of a user or of a group of users of a communication terminal device.

This object is particularly achieved through the invention in that body features are stored in a secured way as biometric keys on a personal SIM-card and in that this SIM-card is inserted into a communication device by a user, said device determining current body features from the user, determining current biometric keys therefrom, and comparing these with the biometric keys stored on the card in order to authenticate the user. This has the advantage that a personal card can authenticate the user in different communication terminal devices without the user having to use passwords, which are often forgotten or may be entered unlawfully, and that a user who acquired the SIM-card improperly, for instance through theft or accidental finding, is not authenticated. An additional advantage is the fact that the SIM-card can be prepared for a user group in that biometric keys are stored therein for all users belonging to the group.

In order to prevent improper authentication, for instance through photographic imitation of body features, body movements are included in the biometric keys.

According to the invention, authentication of the user through the communication terminal device can be used to allow or refuse a user the usage of the communication terminal device in correspondence with the result of the authentication. According to the invention, the result of the authentication can also be transmitted in a wireless manner, particularly by a mobile communication terminal device, to an external secured device which, for its part, can permit or refuse the user access to its services or buildings.

According to the invention, the first recording of biometric keys is executed in a point of presence (POP) connected to a communication network. From there, they are transmitted in a secured manner via the communication network to a biometric server where they are stored in tables, at least one biometric key in a table being assigned to a corresponding user. Additions to and updating of biometric keys

can also be executed in the POP. Moreover, with the present invention, it is possible to update biometric keys directly from the communication terminal device, provided that for the respective user there is already a plurality of biometric keys known at the biometric server.

In the present invention, for the authentication and for the transmission of biometric keys, security services are preferably used, for example Trusted Third Party (TTP) services, in order to ensure the confidentiality, authenticity, integrity and non-deniable origin of the data exchanged via a communication network as well as the authenticity of the sender of these data thereby exchanged.

In accordance with one aspect of the present invention, there is provided a method for determining the authenticity of a user or a user group of a communication terminal device, characterized in that it comprises the following steps recording and temporarily storing video information of body features of the user or the user group in a point of presence (POP); processing of said temporarily stored video information so that specific features are derived as biometric keys; storing of biometric keys in tables of a biometric server and in a SIM-card of the user or the user group, at least one biometric key being assigned in a table to a respective user; inserting the SIM-card into a communication terminal device by the user, said SIM-card containing at least one personal biometric key; recording and temporarily storing of current video information of at least one body feature of the user via a video sensor; processing of said temporarily stored current video information of the user so that at least one specific feature is derived and temporarily stored as a current biometric key; and determining the authenticity by comparing the at least one temporarily stored current biometric key of the user to the at least one stored biometric key, the authenticity being considered to be ensured if the comparison is positive and the authenticity being considered not to be ensured if the comparison is negative.

In accordance with another aspect of the present invention, there is provided a mobile device for telephoning via radio, comprising an interface for receiving a SIM-card, and a video sensor for recording of video information, characterized in that it is provided with storage means for storing biometric keys, in that it comprises processing means for deriving specific features from the video information, and in that it

comprises comparison means for comparing these specific features to the stored biometric keys.

In accordance with yet another aspect of the present invention, there is provided a subscriber identity module (SIM) card for a communication terminal device, characterized in that at least one biometric key for determining the authenticity of a person or a group of persons is stored in the memory of the SIM-card.

In the following one embodiment of the present invention is described by way of example. The embodiment example is illustrated by means of the following appended figure:

Figure 1 shows a block diagram comprising a communication network and, connected to it, a mobile communication terminal device with a SIM-card and a video sensor, a biometric server with connected tables and SIM-server, and a point of presence, as well as a secured device.

The reference numeral 9 refers to a point of presence (POP), for instance connected to a point of sale of a network operator or of a service provider company. The point of presence 9 is provided with at least one computer which, for instance, also serves as communication terminal device, preferably a personal computer or a work station connected to a communication network 5, for instance a fixed network 15. In addition, the point of presence 9 is provided with peripherals for recording body features, which peripherals are connected to the computer and are not illustrated, for instance a video camera connected to the computer via a video cable and a video

interface card. The computer is provided with a program which can access and control the peripheral devices and particularly read, temporarily store and process data recorded by the peripheral devices. The program is also provided with a user interface by means of which it can be used, for example by an operator who is an employee of the POP 9. The user interface helps the operator to record the body features of a client, for example his facial features 7, eye patterns, or fingerprints 8, by providing modules known to one skilled in the art, for example modules to adjust the video camera, to adjust the contrast, to appropriately display picture segments, and also to indicate to the operator when the biometric keys derived by the program are completed, after the program has checked them on site for authentication purposes with the assistance of the client.

Particularly for recording body movements, it is necessary that the program provides the client and the operator via the user interface with instructions, for example to execute certain specific movements, such as mouth or eye movements, for example. At this point, it is important to mention that in an embodiment variant the user interface can be fully automated for recording biometric keys, without the need for an operator, but by giving instructions directly to the client. In such an embodiment variant, the computer and its screen and the camera may be arranged in a manner similar to the one known from automatic passport photo machines or automatic teller machines.

Aside from visual biometric keys, voice features can be recorded correspondingly, by means of peripheral devices, such as microphones and audio interface cards, and can be stored as biometric keys.

The recorded and derived biometric keys of a client can be stored in a corresponding personal user profile; they can also be assigned to a user group. The program and its user interface are provided with the respective components, which can be implemented easily by one skilled in the art, for recording related personal data and for storing this data in respective user or user group profiles. Moreover, additional security information, such as security levels, for example, can also be recorded. Security levels can be used, for instance, to divide secured devices 13 into different levels of access rights to

different services, for example, the access rights of a user may be limited to conduct conversations via the mobile radio telephone 1, whereas another user may execute in addition also other functions, such as selecting and executing special services via the mobile radio telephone 1. Other examples for additional security information, which can be entered and stored, include information relating to the duration of validity, for example in order to limit the validity of certain rights to a specific duration of time or point in time, location information, for example in order to limit access rights to devices or services to specific geographic areas, or personal passwords.

In order to prevent improper assignments, it is important that the assignment of the biometric keys to a user profile or to a user group profile is handled in a controlled manner, for instance exclusively by an operator, under strict authentication conditions, for example by means of multiple identification papers with photographs and possibly with confirming testimony from a present third party.

For completing the recording of the biometric keys, the user profiles or user group profiles with the biometric keys and the security information are transmitted by the program of the computer in a secured manner via a communication network 5 to a server for maintaining the biometric keys, in the following paragraphs referred to as biometric server 10, where they are stored for the respective user or user group in tables 11, connected 19 to the biometric server 10. For one skilled in the art it is clear that there are different possibilities for implementing the biometric server 10 with the tables 11. For example, the tables 11 can be located in a database server which is located on a computer together with the biometric server or which is located on another computer connected to the computer of the biometric server 10 via a communication network. For one skilled in the art, there are also different variants for storing the information in the tables 11, which will not be gone into in more detail here. The same information is likewise stored on the personal SIM card 3 of the user, preferably a GSM card, or on possibly several SIM cards 3 of a user group in corresponding tables 4, in that it is transmitted by the POP 9 to a SIM-server 12, and from there, according to the SICAP method described in EP 0 689 368 B1, by means of special short messages via a

mobile radio network, for instance according to the GSM standard, to the SIM card, and is stored there. In another variant, the SIM-cards 3 are inserted in a special interface (which is not illustrated) of the respective computer in the POP 9 and the program stores the information in a secured manner in the table 4. Thereafter, the SIM-cards, which are thus personalized, can be passed to its user or its user group.

For a secured transmission and storage of biometric keys, security services, for instance trusted third party (TTP) services, are preferably used to ensure the confidentiality, the authenticity, the integrity and the non-deniable origin of this transmitted data. It is also thoroughly possible to execute the encryption by means of a point-to-point method.

Moreover, it is also possible to offer further services in the POP 9, particularly services for updating biometric keys, for instance because of changes due to aging, or services for completing or adding additional biometric keys or other security information, which further services can be implemented by one skilled in the art according to the above descriptions.

The user can insert his personal SIM-card 3 in a communication terminal device 1 and turn on the device. In this example, the communication terminal device 1 is a mobile radio telephone, which is equipped with a video sensor 2 for recording body features, such as eye patterns 6, facial features 7, or fingerprints 8, for example. The video sensor 2 can be directly built into the mobile radio telephone 1 or it can be inserted into the SIM-card 3 interface of the mobile radio telephone 1 by means of an adapter, which itself may comprise an interface for receiving a SIM-card 3. After turning on the mobile radio telephone 1, an authentication program is started, which may be located in the SIM-card 3, for instance, and the user is requested, for example by means of the display (not illustrated) of the mobile radio telephone 1, to look into the video sensor 2, to put a specific finger onto the video sensor 2 and/or to talk into the mobile radio telephone 1. The data recorded by means of the video sensor 2 and, if applicable, by means of the microphone (not illustrated) of the mobile radio telephone 1, is temporarily stored by the authentication program. From this data, current biometric keys are derived which are

temporarily stored and compared to the stored biometric keys 4. In addition to this direct comparison, the authenticity and the integrity of the stored biometric keys 4 can be confirmed by means of TTP services by the biometric server 10, for example. If the comparison of the current biometric key to the biometric key 4 stored in the SIM-card 3 turns out to be positive and if the stored biometric keys 4 are authenticated positively by the biometric server 10, further usage of the mobile radio telephone 1 may be permitted, for example. Otherwise, further usage of the mobile radio telephone 1 by this user may be prevented and the mobile radio telephone 1 may be turned off, for example. Permission may be sustained until the mobile radio telephone 1 is turned off again or it may be time limited, in that the user has to be authenticated again after a predefined period, this may be executed automatically during usage of the mobile radio telephone 1, for example.

Preferably, the SIM-card 3 communicates with the biometric server 10 by means of special short messages which are transmitted via a mobile radio network 16, for instance according to the GSM-standard, within the communication network 5, to a SIM-server 12. Said SIM-server 12 is connected to the communication network 5 via the connection 17 and forwards these special short messages, according to the SICAP method described in EP 0689 368 B1, for further processing to the biometric server 10 via the connection 18.

In the case where a plurality of biometric keys 11 of the user are known at the biometric server 10, it is possible to update biometric keys 11, which have changed, for instance, due to aging, directly from the mobile radio telephone 1. This can take place on condition that the user was authenticated through at least a second biometric key which does not need to be changed and that the quality of the video information to be used for updating a first biometric key meets predefined minimum requirements. For example, these requirements may be requirements on minimum light conditions or image contrast or requirements on the maximum deviation of the new biometric keys from the old biometric keys.

In a variant, the authentication is not primarily used to control usage of the mobile radio telephone 1, but the result of the authentication according to

the description above is transmitted in a wireless and secured manner to an external secured device13, which on its part permits or refuses the access to the device 13 accordingly. Together with the result of the authentication, personal data of the authenticated user may also be transmitted to the secured device 13 so that the secured device 13 may permit or refuse access on the basis of this personal data. In another variant, additional security information of the user, such as security levels, location information, and information about the duration of the validity, for example, is transmitted to the secured device 13 together with the result of the authentication. Based on this security information, the secured device 13 may make the decision about permitting or refusing access. In another variant, the secured device 13 transmits, on request, information about its identity to the mobile radio telephone 1. With this information and by means of additional security information of the user, such as security levels, location information, and information about the duration of the validity, for example, the mobile radio telephone 1 may also make decisions during the authentication process about the user's access to the respective secured device 13 and transmit the result to the secured device 13. For example, the external secured device 13 is an apparatus, for instance an automatic teller machine or a video terminal for information inquiries, an entrance to a secured building, such as a secret industrial manufacturing installation, a police headquarter, or a nuclear power plant, for instance, or the entrance to a restricted area, such as an army base, an airport or a factory, for example. The wireless transmission can be performed, for example, in a contactless manner via an inductive interface 14 by means of an electromagnetic coil located in the SIM-card 3. The mobile radio telephone 1 can also perform the transmission to the secured device 13 by means of a contactless infrared interface (not illustrated) or by means of short messages. The respective transmission takes place in a secured manner, for example by using TTP services or by means of a point to point method.

In a further variant, the video sensor is located outside the mobile radio telephone 1, for example in the external secured device 13. In this variant, the video information is recorded by the external video camera and transmitted to the mobile radio telephone for evaluation. The wireless transmission may be performed, for example, in a contactless manner via an

inductive interface 14 by means of an electromagnetic coil located in the SIM-card 3. The secured device 13 may also perform the transmission to the mobile radio telephone 1 by means of a contactless infrared interface (not illustrated) or by means of short messages. The respective transmission takes place in a secured manner, for example by using TTP services or by means of a point to point method.

Here too, it must be mentioned that, aside from mobile radio telephones 1, other communication terminal devices, such as personal computers, laptop computers, or palmtop computers, for example, may execute this authentication method, if they are equipped with a SIM-card 3 and with peripheral devices for recording body features. Moreover, the application of the authentication does not need to be restricted to access control for communication terminal devices or external secured devices 13, but may also be perfectly well applied to controlling access to services, particularly to services available via the communication network 5, which may comprise the Internet. In these cases, the result of the authentication is transmitted to the respective service provider, for instance an automated Internet site, which can permit or refuse services accordingly. Possibly, the result of the authentication is transmitted to the service provider together with information about the user's access rights to the respective services or with personal data of the user, as was described above in connection with secured devices 13.

It is thoroughly possible that this method and system may be offered by a service provider as a payable service to third parties, who may be interested, for example, in protecting their devices, buildings, areas, or services.

CLAIMS

1. Method for determining the authenticity of a user or a user group of a communication terminal device, characterized in that it comprises the following steps:

- recording and temporarily storing video information of body features of the user or the user group in a point of presence (POP);

- processing of said temporarily stored video information so that specific features are derived as biometric keys;

- storing of biometric keys in tables of a biometric server and in a SIM-card of the user or the user group, at least one biometric key being assigned in a table to a respective user;

- inserting the SIM-card into a communication terminal device by the user, said SIM-card containing at least one personal biometric key;

- recording and temporarily storing of current video information of at least one body feature of the user via a video sensor;

- processing of said temporarily stored current video information of the user so that at least one specific feature is derived and temporarily stored as a current biometric key; and

- determining the authenticity by comparing the at least one temporarily stored current biometric key of the user to the at least one stored biometric key, the authenticity being considered to be ensured if the comparison is positive and the authenticity being considered not to be ensured if the comparison is negative.

2. Method according to claim 1, characterized in that with the recording and temporarily storing of current video information, the video sensor particularly also register movement, and in that this is included in the determination of the authenticity.

3. Method according to claim 1 or claim 2, characterized in that the temporary storage of current video information, their processing and renewed temporary storage, and the determination of the authenticity by comparison to the stored biometric keys are executed by the SIM-card.

4. Method according to any one of claims 1 to 3, characterized in that for the transmission of at least certain messages, security services of TTP (TTP services) are

used in order to ensure the confidentiality, authenticity, integrity and non-deniable origin of the data exchanged via a communication network as well as the authenticity of the sender of the data thereby exchanged.

5. Method according to any one of claims 1 to 4, characterized in that in addition to the biometric keys, using TTP services, security information is recorded in the POP and stored in tables of the biometric server and in the SIM-card, said security information being assigned to the respective users or user groups in tables, and in that said security information is included in the determination of the authenticity.

6. Method according to claim 5, characterized in that the additional security information comprises security levels.

7. Method according to claim 5 or claim 6, characterized in that the additional security information comprises information about the duration of validity.

8. Method according to any one of claims 5 to 7, characterized in that the additional security information comprises location information.

9. Method according to any one of claims 5 to 8, characterized in that the additional security information comprises passwords.

10. Method according to any one of claims 1 to 9, characterized in that existing information for respective users or user groups can be updated and supplemented in the POP using TTP services.

11. Method according to any one of claims 1 to 10, characterized in that biometric keys stored in the tables of the biometric server and in the SIM-card of a communication terminal device can be updated directly from the communication terminal device using TTP services.

12. Method according to any one of claims 1 to 11, characterized in that particularly facial features are derived as biometric keys.

13. Method according to any one of claims 1 to 12, characterized in that particularly eye patterns are derived as biometric keys.

14. Method according to any one of claims 1 to 13, characterized in that particularly fingerprints are derived as biometric keys.

15. Method according to any one of claims 1 to 14, characterized in that aside from visual features, particularly voice features are also recorded as biometric keys.

16. Method according to any one of claims 1 to 15, characterized in that the recording of current video information is executed by a video sensor located in the communication device.

17. Method according to any one of claims 1 to 16, characterized in that the recording of current video information is executed by a video sensor located outside the communication device, the video information being transmitted to the communication device for temporary storage and further processing.

18. Method according to claim 17, characterized in that the transmission of the current video information to the communication device is executed by induction via a coil in a SIM-card.

19. Method according to claim 17, characterized in that the transmission of the current video information to the communication device is executed by means of infrared.

20. Method according to claim 17, characterized in that the transmission of the current video information to the communication device is executed by means of short messages.

21. Method according to any one of claims 17 to 20, characterized in that the video information is transmitted to the communication device using TTP services.

22. Method according to any one of claims 1 to 21, characterized in that the

communication between the SIM-card in the communication terminal device and the biometric server is executed by means of special messages via a SIM-server.

23. Method according to any one of claims 1 to 22, characterized in that for the case where the authenticity of the user is ensured, usage of the communication terminal device can be permitted, whereas for the case where the authenticity of the user is not ensured, usage of the communication terminal device is not permitted.

24. Mobile device for telephoning via radio, comprising an interface for receiving a SIM-card, and a video sensor for recording of video information, characterized in that it is provided with storage means for storing biometric keys, in that it comprises processing means for deriving specific features from the video information, and in that it comprises comparison means for comparing these specific features to the stored biometric keys.

25. Device according to claim 24, characterized in that it comprises a mobile radio telephone into which the video-sensor is directly built in.

26. Device according to claim 24, characterized in that it comprises an adapter into which the video-sensor is built in.

27. Device according to any one of claims 24 to 26, characterized in that it comprises a SIM-card, which is located in said interface for receiving the SIM-card and in which said biometric keys are stored.

28. Device according to claim 27, characterized in that said storage means, processing means, and comparison means are implemented in the SIM-card.

29. Device according to any one of claims 24 to 28, characterized in that the processing means are especially prepared for determining body features from the video information.

30. Device according to claim 29, characterized in that the body features, for which the processing means are especially prepared, comprise facial features.

31. Device according to claim 29 or claim 30, characterized in that the body features, for which the processing means are especially prepared, comprise eye patterns.

32. Device according to any one of claims 29 to 31, characterized in that the body features, for which the processing means are especially prepared, comprise fingerprints.

33. Device according to any one of claims 24 to 32, characterized in that the biometric key also comprises body movements.

34. Subscriber identity module (SIM) card for a communication terminal device, characterized in that at least one biometric key for determining the authenticity of a person or a group of persons is stored in the memory of the SIM-card.

35. SIM-card according to claim 34, characterized in that the stored biometric key comprises facial features.

36. SIM-card according to claim 34 or claim 35, characterized in that the stored biometric key comprises eye patterns.

37. SIM-card according to any one of claims 34 to 36, characterized in that the stored biometric key comprises fingerprints.

38. SIM-card according to any one of claims 34 to 37, characterized in that the stored biometric keys also comprise voice features aside from visual features.

39. SIM-card according to any one of claims 34 to 38, characterized in that other security information comprising at least one of the group consisting of security levels, information about the duration of validity location information, and passwords is stored in the SIM-card.

40. SIM-card according to claim 39, characterized in that the stored security information comprises security levels.

41. SIM-card according to claim 39 or claim 40, characterized in that the stored security information comprises duration of validity information.

42. SIM-card according to any one of claims 39 to 41, characterized in that the stored security information comprises location information.

43. SIM-card according to any one of claims 39 to 42, characterized in that the stored security information comprises passwords.

44. SIM-card according to any one of claims 34 to 43, characterized in that it is provided with means for temporarily storing video information, for deriving specific features from the temporarily stored video information and for temporarily storing these specific features, for comparing said temporarily stored features to the said stored biometric keys, and for executing different further steps depending on the result of this comparison.

45. SIM-card according to any one of claims 34 to 44, characterized in that it is provided with means for composing and deciphering digitally signed and encrypted messages, particularly using trusted third party (TTP) services in order to ensure the confidentiality, authenticity, integrity and non-deniable origin of these messages as well as the authenticity of the sender of these messages, and for transmitting these messages to a biometric server.

46. SIM-card according to any one of claims 34 to 45, characterized in that it is provided with means for composing and deciphering messages, particularly according to a point-to-point method.

47. SIM-card according to any one of claims 34 to 46, characterized in that it comprises an electromagnetic coil via which it can exchange by inductance data with an external secured device, which data is related to the security of these external devices.

48. System for executing a method according to any one of claims 1 to 23 by means of mobile devices according to any one of claims 24 to 33, which devices comprise SIM-cards according to any one of claims 34 to 47 and which devices are

connected to each other as communication terminal devices via a communication network.

49. System according to claim 48, characterized in that the communication network comprises a mobile radio network.

50. System according to claim 49, characterized in that the mobile radio network is a mobile radio network according to the GSM standard.

51. System according to any one of claims 48 to 50, characterized in that the communication network comprises a fixed network.

52. System according to any one of claims 48 to 51, characterized in that the communication network comprises the Internet.

53. System according to any one of claims 48 to 52, characterized in that it comprises additional communication terminal devices, particularly personal computers, laptop and palmtop computers, of which at least certain ones are equipped with a video sensor and which are connected to each other via the communication network.

54. System according to any one of claims 48 to 53, characterized in that it comprises in addition external secured devices, which can communicate with communication terminal devices in a wireless manner and by using TTP services.

55. System according to claim 54, characterized in that the secured device communicates with the SIM-card in the communication terminal device by means of inductance.

56. System according to claim 54, characterized in that the secured device communicates with the communication terminal device by means of infrared.

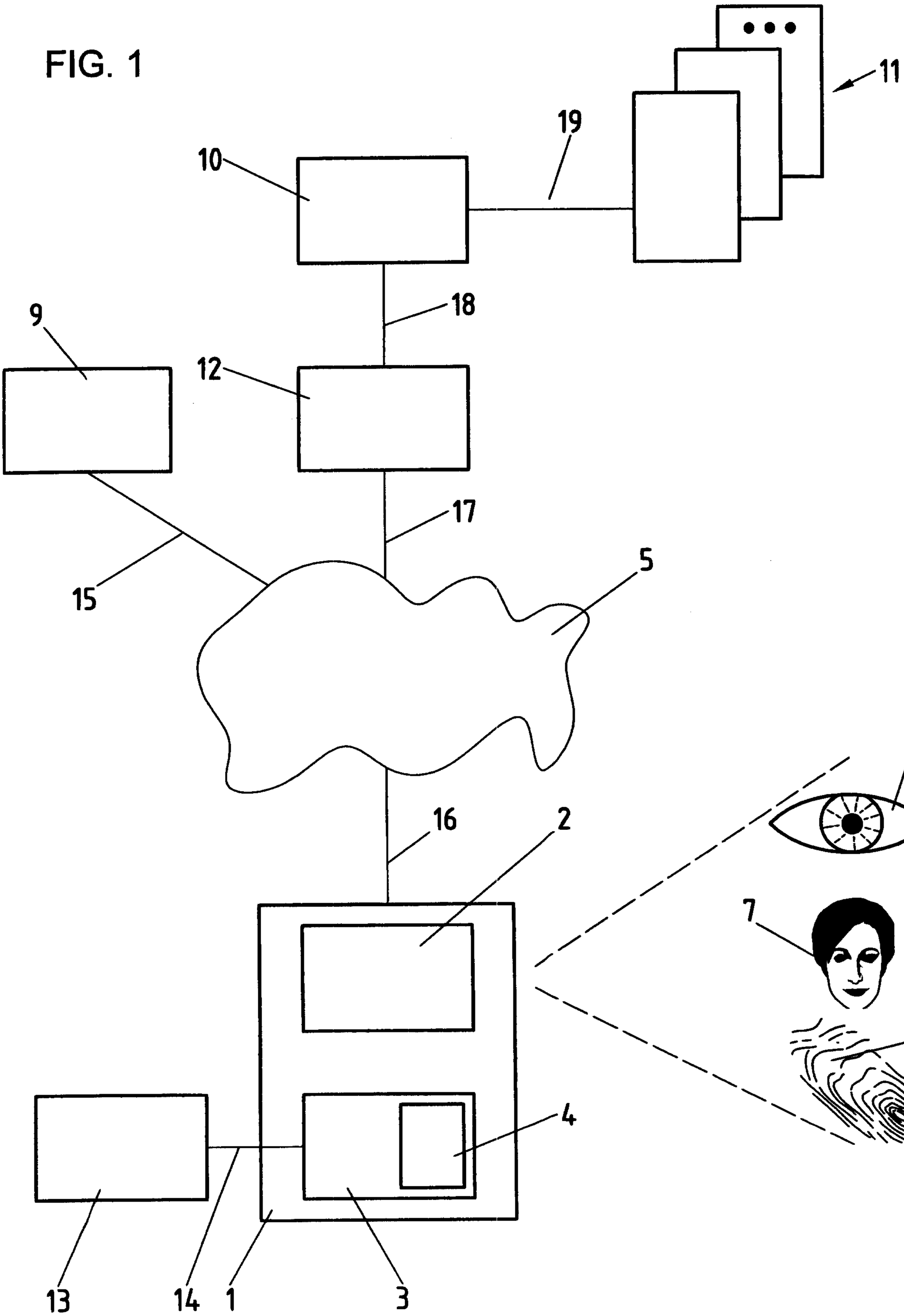
57. System according to claim 54, characterized in that the secured device communicates with the communication terminal device by means of short messages.

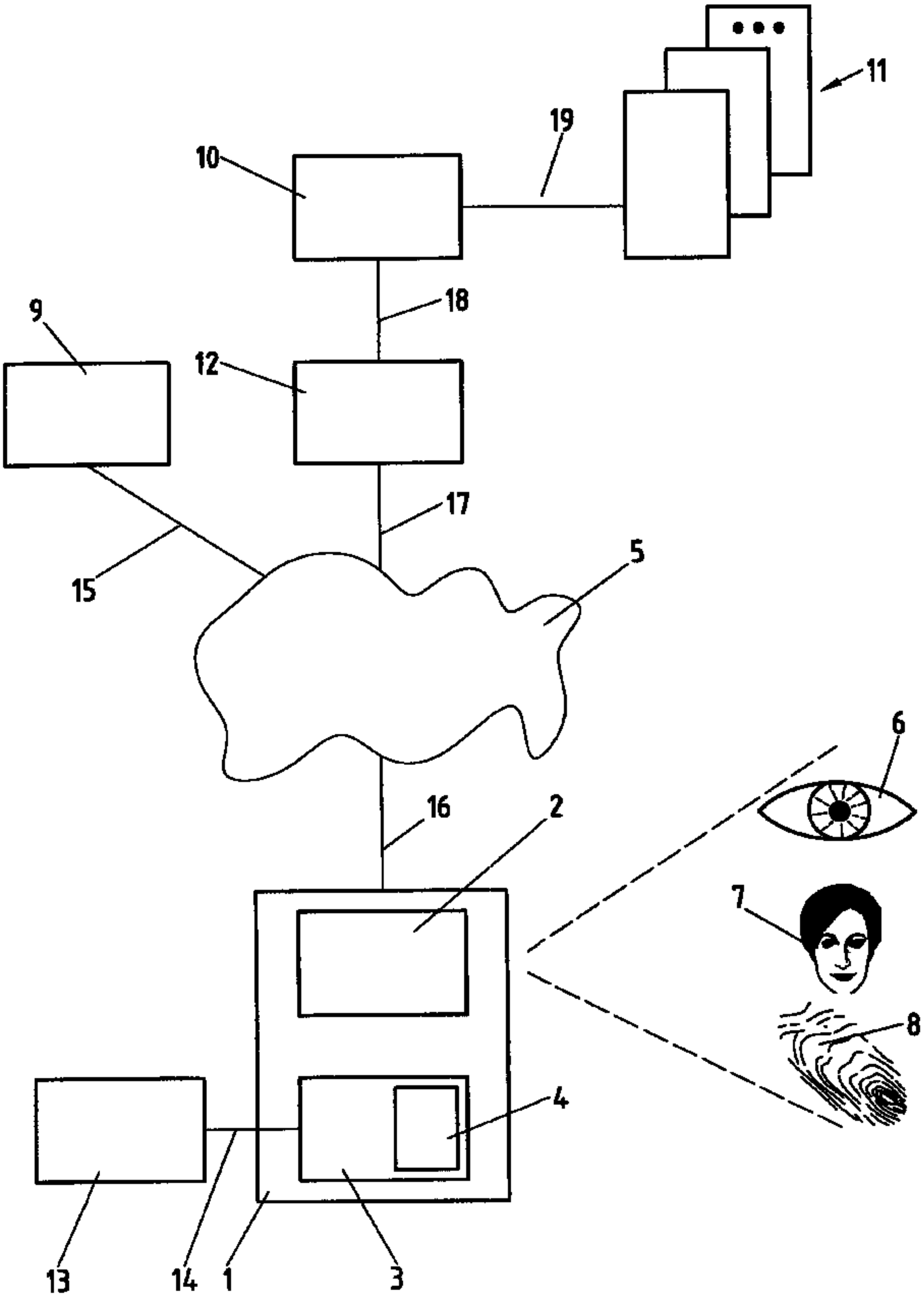
58. System according to any one of claims 48 to 57, characterized in that it comprises secured devices which are equipped with video cameras.

59. System according to any one of claims 48 to 58, characterized in that it comprises SIM-servers via which the SIM-cards in the communication terminal devices communicate with a biometric server by means of special messages.

60. System according to any one of claims 48 to 59, characterized in that it comprises biometric servers which are connected to tables in which biometric keys are stored, at least one biometric key being assigned to a respective user in a table.

FIG. 1




11
19
10
18
9
12
17
15
5
16
2
6
7
8
4
13
14
1
3