

cessor **320** and transmitted by transceiver **310**. Vocoder **330** is also coupled to speaker **340** so that the user can receive audible information received by transceiver **310**. Subscriber unit **30**, as shown in FIG. 3, includes three of the many different possible biometric sensors: fingerprint sensor **375**, retinal scanner **360**, and vocoder **330**. The number of biometric sensors is not a limitation of the present invention. For example, fingerprint sensor **375** can be included, where retinal scanner **360** is not. Likewise, subscriber unit **30** may include retinal scanner **360** and not fingerprint sensor **375**. In an alternate embodiment, subscriber unit **30** includes neither fingerprint sensor **375** nor retinal scanner **360**, but instead includes a palm pressure print sensor or a facial thermographer. One skilled in the art will appreciate that still other types of biometric sensors may be included while still practicing the present invention.

Processor **320** receives biometric information from other subsystems included within subscriber unit **30**, and formats them for transmission by transceiver **310**. Transceiver **310** receives the formatted biometric information from processor **320** and prepares it for transmission at RF frequencies. The functions of transceiver **310** can include, but are not limited to, modulation, frequency conversion, and amplification. As a result, transceiver **310** transmits a signal which has distinguishable characteristics.

Subscriber unit **30** has many advantages. By measuring biometric information describing the current user, subscriber unit **30** provides communications system **10** (FIG. 1) with the ability to robustly authenticate the user. In addition, subscriber unit **30** transmits an RF signature to communications system **10** (FIG. 1) which allows the system to authenticate subscriber unit **30**. After subscriber unit **30** transmits biometric information describing the user, and an RF signature describing the subscriber unit, communication system **10** (FIG. 1) transmits information back to subscriber unit **30** granting access. If, however, a pirate is using subscriber unit **30**, the biometric information measured by subscriber unit **30** will not match the valid biometric information, and communications system **10** (FIG. 1) will transmit information back to subscriber unit **30** denying access.

FIG. 4 shows a diagram of a test set in accordance with a preferred embodiment of the present invention. Test set **400** is used to generate the valid user profiles which are stored in the home location register. When a new user registers with communications system **10** (FIG. 1), his biometric information is measured along with the RF signature of his subscriber unit, and the result is stored in the home location register.

Test set **400** includes receiver **420**, signal characteristic analyzer **425**, processor **430**, and HLR interface **435**. The functional blocks described with reference to test set **400** operate analogously to the corresponding functional blocks of node **200** (FIG. 2), with the exception that rather than authenticating access, test set **400** generates the known valid user profile.

In operation, user **25** operates subscriber unit **30**, and the resulting signal **410** includes the measured biometric information and the RF signature of subscriber unit **30**. Receiver **420** receives signal **410** and routes it to signal characteristic analyzer **425**. Signal characteristic analyzer **425** measures the RF signature of signal **410** and provides a datagram describing the RF signature to processor **430**. Likewise, receiver **420** provides the biometric information to processor **430**. Processor **430** formats the RF signature and the biometric information into a valid user profile that is sent to

HLR interface **435**. HLR interface **435** stores the valid user profile in the HLR for retrieval later when user **25** and subscriber unit **30** need to be authenticated.

FIG. 4 shows a single user **25** with a single subscriber unit **30** being registered. In a preferred embodiment, multiple users **25** can be registered for use with a single subscriber unit **30**. This allows a number of people to be registered for use of a single subscriber unit. When multiple users **25** are registered for use of subscriber unit **30**, test set **400** runs the test at least once for each user **25**.

FIG. 5 shows a flow chart of a method of authenticating a user and a subscriber unit in a communications system in accordance with a preferred embodiment of the present invention. Method **500** begins with step **510** when biometric information is obtained describing a user. The biometric information of step **510** can be fingerprint information, retinal eyescan information, voiceprint information, or any other information describing the user. In step **520**, a signal characteristic of a subscriber unit is measured to obtain an RF signature. The RF signature obtained in step **520** identifies, to the greatest extent possible, the subscriber unit being used by the user.

In step **530**, a probability is evaluated that the biometric information and the RF signature match a prestored user profile. The pre-stored user profile of step **530** preferably includes a threshold, above which the probability will signify a match, and below which the probability will indicate a non-match. In step **540**, the probability is compared against the threshold. If the probability is above the threshold, processing proceeds with step **560** where access is granted. On the other hand, if the probability is below the threshold, processing proceeds with step **550** where access is denied. After either step **550** or **560**, the authentication process is complete and method **500** ends.

The steps of method **500** as just described, can be performed in a single node of a communications system, or can be performed in a distributed fashion among multiple nodes of a communications system. For example, a portion of method **500** can be performed in a satellite, such as steps **510** and **520**, with the remaining steps performed in a gateway. In another example embodiment, all of the steps in method **500** are performed in a base station, such as base station **35** in communications system **10** (FIG. 1).

FIG. 6 shows a flowchart of a method of operating a subscriber unit in a communications system in accordance with a preferred embodiment of the present invention. Method **600** begins with step **610** when biometric information is measured which describes a user. After the biometric information is measured in step **610**, the biometric information is formatted and sent to a communications system for authentication in step **620**. In step **630**, a signal with a unique RF signature is sent to the communications system for authentication. The signal with a unique RF signature of step **630** can be the signal which includes the biometric information of step **620**, or can be a separate signal. Then, in step **640**, an acknowledgment signal is received from the communications system. After receiving the acknowledgment signal in step **640**, processing proceeds with step **650**. If, in step **650**, access has been granted because the biometric information and the RF signature matched a pre-stored user profile, then processing proceeds with step **670** where communications are commenced. Otherwise, processing proceeds with step **660** where communications are not commenced. At the completion of either step **660** or step **670**, method **600** is complete, and processing ends.

FIG. 7 shows a flowchart of a method of operating a test set in a communications system in accordance with a