

preferred embodiment of the present invention. Method **700** as shown in FIG. **7** is a method of generating the prestored user profiles previously described. When a user or a plurality of users are to be registered as valid users of a subscriber unit, method **700** is utilized in conjunction with the test set of FIG. **4** to generate valid user profiles to be stored in the home location register.

Method **700** begins with step **710** when biometric information is obtained describing a user. In step **720**, a signal characteristic of a subscriber unit is measured to obtain an RF signature. The signal of **720** may be the signal which transmitted the biometric information of step **710**, but this is not a limitation of the present invention. For example, a separate signal may be transmitted from a subscriber unit for the purposes of measuring the RF signature. In step **730**, the biometric information and the RF signature are formatted into a user profile. The user profile of step **730** includes information which describes a valid user in conjunction with a valid subscriber unit. In step **740**, the user profile is sent to a home location register. If, in step **750**, there are more users to be registered, then processing proceeds with step **760** where the next user is substituted for the present user. After step **760**, steps **710** through **740** of method of **700** are repeated for the next user. When there are no more users to be registered, processing ends after step **750**.

Although method **700** describes a preferred embodiment where each separate user profile is sent to a home location register separately in step **740**, other embodiments exist where the user profiles are not sent to the home location register until all user profiles for all valid users have been generated.

Method **700** is typically performed when a new subscriber unit is issued to a user or a number of users, or after a subscriber unit undergoes service which may cause the RF signature to change. Method **700** can also be performed periodically to take into account any changes occurring over time which affect either biometric information or RF signatures.

In summary, the method and apparatus of the present invention provides an advantageous means for authenticating subscriber units and users in a communications system. While we have shown and described specific embodiments of the present invention, further modifications and improvements will occur to those skilled in the art. For example, the specific embodiments described pertain mainly to telephony systems, but the method and apparatus of the present invention also apply to wideband systems, paging systems, and other data delivery services. We desire it to be understood, therefore, that this invention is not limited to the particular forms shown and we intend in the appended claims to cover all modifications that do not depart from the spirit and scope of this invention.

What is claimed is:

1. A communications system comprising:

at least one subscriber unit associated with a biometric sensor for measuring biometric information of a user
 a transmitter capable of transmitting a signal with a unique signature of said at least one subscriber unit;
 a register which has a pre-stored user profile including a valid signature and valid biometric information;
 a communications node which receives said biometric information and said signal from the at least one subscriber unit and receives said pre-stored user profile from said register, said communication node evaluating a probability that said biometric information and said unique signature substantially match said pre-stored user profile and providing access to said user if said probability is greater than a threshold and denying access to said user if said probability is less than a threshold.

2. A user authentication apparatus in a communications system, said user authentication apparatus comprising:

a subscriber unit having:

a biometric sensor for measuring biometric information of a user;
 a processor in communication with said biometric sensor, said processor formatting said biometric information and producing formatted biometric information; and
 a transmitter in communication with processor, said transmitter receiving said formatted biometric information and preparing said formatted biometric information for transmission as a signal having said biometric information;

a communication node receiving said signal and a pre-stored user profile and said signal, said communication node evaluating a probability that said signal having said biometric information substantially matches said pre-stored user profile and authenticating access of said user if said probability is greater than a threshold and failing to authenticate access of said user if said probability is less than a threshold.

3. The user authentication apparatus of claim **2** wherein said biometric sensor is a fingerprint measuring device.

4. The user authentication apparatus of claim **3**, wherein said fingerprint measuring device is integrated into at least one button of a keypad.

5. The user authentication apparatus of claim **2** wherein said biometric sensor is a retinal eye scanner.

6. The user authentication apparatus of claim **2** wherein said biometric sensor is a vocoder.

7. The user authentication apparatus of claim **2** wherein said signal includes a unique RF signature.

8. The user authentication apparatus of claim **2** further comprising a receiver for receiving an authentication message generated in response to said communication node evaluating a probability that said signal having said biometric information substantially matches said pre-stored user profile.

9. The user authentication apparatus of claim **2** wherein said biometric sensor is a facial thermographer.

10. A method of authenticating access for a user of a subscriber unit in a communications system, said method comprising the steps of:

obtaining biometric information of said user;
 measuring a signal characteristic of said subscriber unit to obtain a signature;
 comparing said biometric information and said signature against a pre-stored user profile;
 evaluating a probability that said biometric information and said signature substantially match said pre-stored user profile;
 providing access to said communications system if said probability is above a threshold; and
 denying access to said communications system if said probability is below said threshold.

11. The method of claim **10** wherein said biometric information includes voice print data.

12. The method of claim **11** wherein said voice print data includes vocoder coefficients.

13. The method of claim **10** wherein said biometric information includes fingerprint data.

14. The method of claim **10** wherein said biometric information includes retinal eye scan data.