

SYSTEM AND METHOD OF USER AND DATA VERIFICATION

RELATED APPLICATION

[0001] This application claims the benefit of and incorporates by reference, in its entirety, U.S. Provisional Application No. 60/274,518, filed Mar. 9, 2001.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The invention relates to the conversion of physical or biological signatures into digital signatures. More particularly, the invention relates to generating digital signatures using biometric identification.

[0004] 2. Description of the Related Technology

[0005] Physical signatures are becoming an anachronism in the electronic world and the process of verifying pen-and-ink signatures, photographs or fingerprints on paper or other materials are costly and error-prone. At least with physical documents, however, the signer retains the basic "contextual controls" of document preparation and physical delivery. On a digitally signed electronic document, on the other hand, a signer controls only the encoded signature. All time, place and manner controls are absent, and nothing distinguishes a valid user signature from one fraudulently produced by another user who somehow obtained the first user's data, algorithms and keys.

[0006] Public-key cryptography is a computer security technology that can support the creation of electronic document systems, providing that the user's digital signature on an electronic document, i.e., the user's electronic authentication and verification of the electronic document, can be given sufficient practical and legal meaning.

[0007] These systems have enormous commercial significance because, in many cases, large cost reductions can be realized over current paper transaction procedures. This improvement is sufficiently dramatic that many organizations are, for economic and competitive reasons, compelled to use them once their practicality has been demonstrated.

[0008] Disadvantageously, known systems do not allow for authentication of messages using biometric information. Biometrics is the measure of an individual's body or behavior in order to identify or verify the individual's identity. Biometrics provides for new ways to identify a user with his fingerprint, voiceprint, iris scan, facial picture, hand geometry or various other unique features of his body or behavior. Biometric measurement data, albeit subject to statistical variations, is nevertheless conventionally used to verify the identity of individuals. Typical methods used are based on statistical hypothesis testing where an individual's biometric measurements are stored at the time of "enrollment". Then, during "verification", biometric measurements are taken again and compared to the stored measurements. Various algorithms can be used to convert the measurements into mathematical representations and accept a range of biometric data. This conversion and statistical analysis is useful because sequential biometric measurements have a range for any one individual, especially when taken at different times and places using even slightly different equipment.

[0009] There is a need for new and improved systems for authenticating messages. The system should analyze biometric information as provided by the user as part of the authentication process. The system should also include features to safeguard the keys that are used in the authentication process.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is a block diagram illustrating certain components of a smart card embodiment of a portable encryption device.

[0011] FIG. 2 is a block diagram illustrating the functional modules and data involved in an enrollment process that is performed by the smart card of FIG. 1.

[0012] FIG. 3 is a block diagram illustrating the functional modules and data involved in a signing process that is performed by the smart card of FIG. 1.

[0013] FIG. 4 is a flowchart illustrating an exemplary process of registering biometric information with the portable encryption device of FIG. 1.

[0014] FIG. 5 is a flowchart illustrating an exemplary process of generating and authenticating a message using the portable encryption device of FIG. 1.

SUMMARY OF THE CERTAIN INVENTIVE ASPECTS

[0015] One aspect of the invention comprises a method of generating digital signature, the method comprising: generating public and private keys on a secure device, storing biometric information indicative of a user on the secure device, receiving biometric information indicative of the user, and comparing the stored biometric information with the received biometric information on the secure device, and if the comparison is successful, generating a digital signature for a message. In one embodiment, the secure device is portable. Furthermore, in one embodiment of the invention, the secure device is a smart card.

[0016] Another aspect of the invention comprises a method of generating a digital signature, the method comprising registering biometric information in a secure device and generating public and private keys on the secure device in conjunction with the biometric information. The digital device may include a unique device identifier which is used for key generation.

[0017] Yet another aspect of the invention comprises a secure device for generating a digital signature, the device comprising: a module for generating public and private keys on a secure device, a module for storing biometric information indicative of a user on the secure device, a module for receiving biometric information indicative of the user, and a module for comparing the stored biometric information with the received biometric information on the secure device, and if the comparison is successful, generating a digital signature for a message.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0018] The following detailed description is directed to certain specific embodiments of the invention. However, the