

smart card **100**, even with the knowledge of the user's biometric data does not allow the generation of the same private key and the same signature. Only the combination of the unique smart card and its corresponding specific accurate biometric data allows the generation of the digital signature.

[0050] The device provides for a novel way to generate a digital signature, which is unique, cannot be duplicated, even by the user or the manufacturer, and requires the user's specific biometric data in all cases. By requiring the physical presence of the individual and the device to generate the digital signature it provides for a contextual control of the signature, which is equivalent or even superior in many ways to controls currently applied on physical or biological signatures and used in today's legal and administrative world.

[0051] A device according to the present invention utilizes a biometrics authentication procedure to generate a digital signature. In the disclosed embodiment of the invention, the token or smart card is used in two different ways, i.e., in an enrollment mode or in a signing mode. FIG. 4 is a flowchart illustrating an exemplary process of registering biometric information received from a user in the enrollment mode. FIG. 5 is a flowchart illustrating an exemplary process of authenticating a messaging in the signing mode. It is to be appreciated that depending on the embodiment, additional states may be added, others removed, and the ordering of the states may be rearranged.

[0052] Referring to FIG. 4, at a state **400**, in the "enrollment" or "registration" mode the smart card **100** uses the biometrics data analyzer **200** to register biometrics templates coming through the biometrics interface **110**. Next, at a state **404**, after completion of the biometrics registration procedure, the smart card **100** generates, via the random key generation module **204**, the private key **224**. Moving to a state **408**, the smart card **100** generates the public key **220**. The private key **224** is stored in the card non-volatile memory, such as EEPROM **134**, and remains unknown to the user, whereas the public key **220** is communicated to the user and his correspondents through the card reader interface **130** and any subsequent communication channel.

[0053] Continuing to a state **412**, the public key **220** can be provided to the correspondents by a certification authority along with a digital certificate. The certification authority assigns to the smart card **100** a specific serial number that is specific to an individual and certifies the corresponding public key **220** after successful enrollment by the individual.

[0054] Referring now to FIG. 5, at a state **504**, in the "signing" mode a message **230** is downloaded from a computer into the smart card **100** through the card interface **130** and processed with the one-way hash function **212** to generate a message digest  $D=H(M)$ . Next, at a state **506**, biometric measurements are taken again from the biometrics interface **110** and verified by the biometric data analyzer **200**. It is to be appreciated that the biometric information may optionally be received concurrently with or before the receipt of the message.

[0055] Continuing to a decision state **508**, if the biometric data **216** is identified (and the identity of the user is authenticated), the process proceeds to a state **512**, wherein a message digest for the message is created. Otherwise, if the biometric data **216** is not identified, the process ends.

[0056] From state **512**, the process proceeds to a state **516** wherein the message digest is encrypted by the encryption module **208** on the card **100** using the private key **224**. The result is an encrypted message digest that is the digital signature **234** for the message **230**. This digital signature **234** is added to the message **230**. Proceeding to a state **520**, the message is sent back to a computer for further processing and communication.

[0057] In order for the process to be secure it is recommended that the biometric data analyzer **200**, the random number generator **204**, the private key **224** and the encryption module **208** be embedded into the card in a tamperproof way. The fact that the private key **224** is inaccessible provides security to the system. The one-way hash function **212** and the public key **220** are shared with the recipients of the message in order to decrypt the signature and to compare the message digest with the decrypted signature, accordingly it is not necessary to have the one-way hash function **212** nor the message digest **232** be embedded into the smart card **100**. However, depending on the application considered, it might be preferable to generate the message digest on the smart card **100**. For example, the smart card **100** could also be used to verify other user's signatures, in which case it will be convenient to store the one way hash function **212** in the smart card **100** to be able to verify and create message digests. Incorporating the biometric data analyzer **200** into the smart card **100** is advantageous because it provides for an additional level of security. Any attempt to simulate the biometric data is extremely difficult because the details of the biometric data and the analysis algorithms are embedded into the smart card **100** and are unknown to a fraudulent user.

[0058] The digital signature can be added to any message or any electronic document. The use of the smart card **100** opens a vast area of applications ranging from electronic signatures on bilateral and multilateral transactions, electronic notary services, electronic authorizations for financial transactions in banking and trading, payments for electronic commerce, payments for electronic auctions, payments for access to electronic services, and more generally all activities requiring the identification of a user requesting or performing an electronic transaction.

[0059] By using the random key generator **204** and the encryption module **208**, the private key **224** does not need to be stored in a host computer. Further, the user biometrics verification process is advantageous due to the fact that if the smart card **100** is stolen, it is of little value. The user and the device are required to generate the digital signature.

[0060] While the above detailed description has shown, described, and pointed out novel features of the invention as applied to various embodiments, it will be understood that various omissions, substitutions, and changes in the form and details of the device or process illustrated may be made by those skilled in the art without departing from the scope of the invention. The scope of the invention is indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.