CLAIMS

1. An electronic pen device configured to be used with a remote secure server for registering handwritten signatures, said secure server comprising an authentication database storing authentication information in connection with pre-registered users and a signature registration database for registering handwritten signatures, the electronic pen device comprising:

   an input/output (I/O) interface ; a memory; a tip and capturing means connected thereto for capturing handwritten signatures; a network interface adapted to be connected to a data network, and a processing unit connected to said I/O interface, to said capturing means, to said memory and to said network interface;

   where said electronic pen device obtains personnel identification information originating from a user desiring to sign, automatically authenticates said user by inquiring said remote secure server using said personnel identification information, and if a successful authentication, captures said handwritten signature, associates a unique signature identifier thereto, and transmits said captured handwritten signature to said remote secure server via said data network for storage in association with said user and said unique signature identifier, and communicates said unique signature identifier to said user in order to be used as a reference during future authentication of said handwritten signature.

2. The electronic pen device as claimed in claim 1, wherein said secure server further comprises a condition subsequent database for storing conditions subsequent associated with handwritten signatures registered inside said signature registration database, and where said electronic pen device is configured to enable a user to input a condition subsequent associated with a

signature handwritten thereby, and to transmit said condition subsequent to said secure server via said data network for storage in connection with said handwritten signature inside said condition subsequent database for future inquiry.

3. The electronic pen device as claimed in any one of claims 1 to 2, where said electronic pen device is further configured to enable a user to input user identification information associated with at least one other user and to initiate a request to invite said at least one other user to sign a document, where said electronic pen device transmits said invitation request and said user identification information to said secure server for generating a unique document identifier and for transmitting an invitation to sign said document comprising said unique document identifier to said at least one other user.

4. The electronic pen device as claimed in claim 3, where said electronic pen device is further configured to receive through said data network an invitation to sign a document comprising a unique document identifier, to communicate a message about said invitation to a user in possession of said electronic pen device, to capture a signature handwritten by said user in association with said document and to transmit said handwritten signature to said secure server along with said document identifier via said data network for storage inside said signature registration database.

5. The electronic pen device as claimed in any one of claims 1 to 4, wherein said personnel identification information comprises a user name and a password which is specified by said user using said I/O interface.

6. The electronic pen device as claimed in any one of claims 1 to 5, wherein said I/O interface comprises a touch screen.

7. The electronic pen device as claimed in any one of claims 1 to 6, wherein said unique signature identifier is generated by said remote secure server and is transmitted to said electronic pen device via said data network.

8. The electronic pen device as claimed in any one of claims 1 to 7, wherein said authentication information comprises physical coordinates defining a security region within which said electronic pen device shall be located, said electronic pen device further comprising a GPS chip for tracking a physical location of said device, wherein said authenticating said user comprises inquiring said remote secure server for verifying if said tracked physical location is within said security region.

9. The electronic pen device as claimed in any one of claims 1 to 8, wherein said network interface is wireless and said data network comprises a satellite connection.

10. A system for registering handwritten signatures, the system comprising:

an authentication database comprising authentication information associated with pre-registered users;

a signature registration database for registering handwritten signatures;

a network interface adapted to be connected to a data network; and

a first processing unit adapted to be connected to said authentication database, to said signature registration database and to said network interface, where said processing unit is configured to receive a request for registering a handwritten signature comprising personnel identification information associated with a user,

to inquire said authentication database as a function of said personnel identification information, and if a successful authentication, to generate a unique signature identifier, to receive a signature handwritten by said user on a given support, to associate said unique signature identifier with said handwritten signature, to store said handwritten signature into said signature registration database in association with said user and said unique signature identifier, and to communicate said unique signature identifier to a device held by said user in order to be used as a reference during future authentication of said handwritten signature.

11. The system as claimed in claim 10, further comprising a user device configured to capture said handwritten signature, to enable said user to input said personnel identification information, to transmit said handwritten signature and said personnel identification information to said first processing unit via said data network, to receive said unique signature identifier transmitted by said first processing unit via said data network, and to enable said user to take note of said unique signature identifier.

12. The system as claimed in any one of claims 10 to 11, further comprising a condition precedent database storing conditions precedent associated with at least a part of said pre-registered users, wherein said first processing unit is configured to inquire said condition precedent database about any condition precedent in record in connection with said user, and if it is the case, to verify if said condition precedent has been fulfilled, where said first processing unit is configured to reject said request of registering a handwritten signature if a condition precedent is found in record and said condition has not been fulfilled.

13. The system as claimed in any one of claims 10 to 12, further comprising a condition subsequent database storing conditions subsequent associated with handwritten signatures stored in said signature registration database, and a

second processing unit configured to inquire said condition subsequent database about any condition subsequent in record in connection with a given handwritten signature, and if it is the case, to verify if said condition subsequent has been fulfilled.

14. The system as claimed in claim 13, further comprising a Web site connected to said condition subsequent database to allow pre-authorized persons to add and edit conditions subsequent.

15. The system as claimed in any one of claims 11 to 14, wherein said user device is further configured to enable said user to input user identification information associated with at least one other user, to enable said user to initiate a request to invite said at least one other user to sign a document, to transmit said invitation request and said user identification information to said first processing unit through said data network, where said first processing unit is configured to generate a unique document identifier and to transmit an invitation to sign said document comprising said unique document identifier to said at least one other user.

16. The system as claimed in claim 15, wherein said user device is further configured to receive through said data network an invitation from another user to sign a document comprising a unique document identifier, to communicate a message about said invitation to said user in possession of said user device, to capture a signature handwritten by said user in association with said document and to transmit said handwritten signature to said first processing unit along with said document identifier via said data network for storage inside said signature registration database.

17. The system as claimed in any one of claims 11 to 16, wherein said user device is an electronic pen device.

18. The system as claimed in claim 17, wherein said electronic pen is a ball point pen, and said sensor means comprise a movement sensor for capturing movement of said ball point.

19. The system as claimed in claim 17, wherein said user device is a scanning device comprising means for scanning said handwritten signature.

20. The system as claimed in any one of claims 10 to 19, wherein said personnel identification information comprises a user name and a password.

21. The system as claimed in any one of claims 10 to 20, wherein said authentication information comprises physical coordinates defining a security region within which said user device shall be located, said user device further comprising a GPS module for tracking a physical location thereof, wherein said authenticating said user comprises inquiring said authentication database for verifying if said tracked physical location is within said security region.

22. A method of authenticating handwritten signatures, the method comprising:

receiving, at a processing unit, a signature handwritten by a user on a given support and personnel identification information associated with said user;

automatically authenticating, by said processing unit, said user using said personnel identification information by inquiring an authentication database storing authentication information in connection with pre-registered users;

if a successful authentication, automatically generating, by said processing unit, a unique signature identifier, automatically associating said unique signature identifier to said handwritten signature, automatically storing said handwritten signature into a signature registration database in association with said user and

said unique signature identifier, and automatically communicating said unique signature identifier to said user in order to be used as a reference during future authentication of said original handwritten signature;

providing access to said signature registration database for enabling another party to authenticate said signature handwritten on said given support, where said authentication is carried out by verifying if said signature appearing on said given support is substantially identical to said electronic reproduction stored in association with said unique signature identifier.

23. The method as claimed in claim 22, wherein said given support is a paper support.

24. The method as claimed in any one of claims 22 to 23, wherein said signature has been written by said user using an electronic pen by which it has been captured and transmitted to said processing unit.

25. A method of signing a document by a plurality of contracting users, the method comprising:
receiving, from a first user, a request of signing a document by a plurality of contracting users;

receiving user identification information associated with the contracting users;

generating a unique document identifier in connection with said document to be signed;

transmitting an invitation to sign the document to each one of the contracting users along with the unique document identifier;

providing access to the document content to the contracting users before signing;

receiving handwritten signatures associated with said contracting users;

authenticating said contracting users, where said authenticating comprises verifying if said handwritten signatures originate from said contracting users; and

registering said handwritten signatures inside a signature registration database in connection with the document and with each one of the users.

26. An electronic pen device configured to be used with a remote server for archiving handwritten information, the device comprising means for capturing handwritten information, a user interface for enabling a user to specify a folder identifier associated with said remote server within which handwritten information shall be classified, a network interface adapted to be connected to a data network and a processing unit connected thereto for transmitting said captured handwritten information to said remote server in order to be classified within said identified folder.

27. The electronic pen device as claimed in claim 26, wherein said remote server is a secure remote server whereby said user shall be authenticated before accessing to content thereof, wherein said user interface receives user identification information associated with said user, and wherein said processing unit first authenticates said user by inquiring said remote secure server using said user identification information.

28. The electronic pen device as claimed in any one of claims 26 to 27, wherein said processing unit inquires said remote server about existence of said identified folder and transmits said captured handwritten information to said remote server only if said folder identifier exists.

29. The electronic pen device as claimed in any one of claims 26 to 28, wherein, if said folder identifier does not exist, said processing unit instructs said remote server to open a new folder having said specified identifier and to classify said captured handwritten information within said new created folder.

30. The electronic pen device as claimed in any one of claims 26 to 29, further comprising a memory wherein said captured handwritten information is stored for a later time before classifying it into said remote server.

CLAIMS

1. An electronic pen device (10) configured to be used with a remote secure server (80) for registering handwritten signatures, said secure server comprising an authentication database (110) storing authentication information in connection with pre- registered users and a signature registration database (112) for registering handwritten signatures, the electronic pen device (10) comprising:

an input/output (I/O) interface (22); a memory (18); a tip (14) and capturing means (12) connected thereto for capturing handwritten signatures; a network interface (24) adapted to be connected to a data network (50), and a processing unit (16) connected to said I/O interface, to said capturing means, to said memory and to said network interface;

where said electronic pen device (10) is configured to:

obtain personnel identification information originating from a user desiring to sign and automatically authenticate said user by inquiring said remote secure server (80) using said personnel identification information, wherein said authentication includes synchronizing the pen clock (36) with the server clock (96) via the network interface (24);

receive an encryption code, generated by the secure server (80), unique to the given user and an indication of a successful authentication, wherein the pen (10) is configured to communicate with the secure server using said encryption code for all subsequent messages transmitted;

capture a handwritten signature after a successful authentication, encrypt and transmit said captured handwritten signature to said remote secure server (80) via said data network (50) for storage in association with said user; and receive via said data network a unique signature identifier thereto, generated by said secure server and communicate said unique signature identifier to said user in order to be used as a reference during future authentication of said handwritten signature.

2. The electronic pen device (10) as claimed in claim 1 , wherein said secure server further comprises a condition subsequent database (116) for storing conditions subsequent associated with handwritten signatures registered inside said signature registration database, and where said electronic pen device (10) is configured to enable a user to input a condition subsequent associated with a signature handwritten thereby, and to transmit said condition subsequent to said secure server via said data network for storage in connection with said handwritten signature inside said condition subsequent database (116) for future inquiry.

3. The electronic pen device (10) as claimed in any one of claims 1 to 2, where said electronic pen device is further configured to enable a user to input user identification information associated with at least one other user and to initiate a request to invite said at least one other user to sign a document, where said electronic pen device transmits said invitation request and said user identification information to said secure server for generating a unique document identifier and for transmitting an invitation to sign said document comprising said unique document identifier to said at least one other user.

4. The electronic pen device (10) as claimed in claim 3, where said electronic pen device is further configured to receive through said data network (50) an

invitation to sign a document comprising a unique document identifier, to communicate a message about said invitation to a user in possession of said electronic pen device, to capture a signature handwritten by said user in association with said document and to transmit said handwritten signature to said secure server along with said document identifier via said data network for storage inside said signature registration database.

5. The electronic pen device (10) as claimed in any one of claims 1 to 4, wherein said personnel identification information comprises a user name and a password which is specified by said user using said I/O interface.

6. The electronic pen device (10) as claimed in any one of claims 1 to 5, wherein said authentication information comprises physical coordinates defining a security region within which said electronic pen device shall be located, said electronic pen device further comprising a GPS chip for tracking a physical location of said device, wherein said authenticating said user comprises inquiring said remote secure server for verifying if said tracked physical location is within said security region.

7. The electronic pen device (10) as claimed in any one of claims 1 to 6, wherein said network interface is wireless and said data network comprises a satellite connection.

8. A secure server (80) for registering handwritten signatures received from an electronic pen device (10), said secure server comprising:

an authentication database (110) comprising authentication information associated with pre-registered users, and a signature registration database (112) for registering handwritten signatures;

a network interface (84) adapted to be connected to a data network (50);

and a first processing unit (86) adapted to be connected to said authentication database, to said signature registration database and to said network interface, wherein said processing unit is configured to:

receive a request for registering a handwritten signature comprising personnel identification information associated with a user;

inquire said authentication database as a function of said personnel identification information, synchronize the first processing unit clock with the electronic pen device (10), and if a successful authentication, to generate a unique signature identifier and send a unique encryption code to the given user, wherein the first processing unit (86) is configured to communicate with the electronic pen device (10) using said encryption code for all subsequent messages transmitted;

receive a handwritten signature by said user on a given support via said data network for storage in association with said user; and

generate a unique signature identifier and communicate said unique signature identifier to said user via the electronic pen device in order to be used as a reference during future authentication of said handwritten signature;

wherein the server is configured to store said handwritten signature into said signature registration database in association with said user and said unique signature identifier.

9. A system for registering handwritten signatures, the system comprising a secure server (80) according to claim 8 and an electronic pen device (10) according to claim 1.

10. The system as claimed in claim 9, or the server of claim 8, further comprising a condition precedent database (114) storing conditions precedent associated with at least a part of said pre-registered users, wherein said first processing unit (86) is configured to inquire said condition precedent database about any condition precedent in record in connection with said user, and if it is the case, to verify if said condition precedent has been fulfilled, where said first processing unit is configured to reject said request of registering a handwritten signature if a condition precedent is found in record and said condition has not been fulfilled.

11. The system as claimed in any one of claims 9 or 10, or the server of claim 8, further comprising a condition subsequent database (116) storing conditions subsequent associated with handwritten signatures stored in said signature registration database, and a second processing unit configured to inquire said condition subsequent database about any condition subsequent in record in connection with a given handwritten signature, and if it is the case, to verify if said condition subsequent has been fulfilled.

12. The system as claimed in claim 11 further comprising a Web site connected to said condition subsequent database to allow pre-authorized persons to add and edit conditions subsequent.

13. The system as claimed in any one of claims 9 to 12, wherein said user device is further configured to enable said user to input user identification information associated with at least one other user, to enable said user to

initiate a request to invite said at least one other user to sign a document, to transmit said invitation request and said user identification information to said first processing unit through said data network, where said first processing unit is configured to generate a unique document identifier and to transmit an invitation to sign said document comprising said unique document identifier to said at least one other user.

14. The system as claimed in claim 13, wherein said user device is further configured to receive through said data network an invitation from another user to sign a document comprising a unique document identifier, to communicate a message about said invitation to said user in possession of said user device, to capture a signature handwritten by said user in association with said document and to transmit said handwritten signature to said first processing unit along with said document identifier via said data network for storage inside said signature registration database.

15. The system as claimed in claim 14, wherein said electronic pen is a ball point pen, and said sensor means comprise a movement sensor for capturing movement of said ball point.

16. The system as claimed in claim 14, wherein said user device is a scanning device comprising means for scanning said handwritten signature.

17. The system as claimed in any one of claims 9 to 16, wherein said personnel identification information comprises a user name and a password.

18. The system as claimed in any one of claims 9 to 17, wherein said authentication information comprises physical coordinates defining a security region within which said user device shall be located, said user device further

comprising a GPS module for tracking a physical location thereof, wherein said authenticating said user comprises inquiring said authentication database for verifying if said tracked physical location is within said security region.

19. A method of authenticating handwritten signatures, the method comprising:

receiving, at a first processing unit (16), a request for registering a handwritten signature comprising personnel identification information associated with a user;

communicating with a secure server (80) over a network interface (24) connected to a data network (50), said secure server having:

an authentication database (110) comprising authentication information associated with pre-registered users; and a signature registration database (112) for registering handwritten signatures;

inquiring with said authentication database as a function of said personnel identification information, wherein said inquiry and authentication includes synchronizing a first processing unit clock with the server;

issuing an encryption code, generated by the secure server, unique to the given user and an indication of a successful authentication, wherein the first processing unit is configured to communicate with the user using said encryption code for all subsequent messages transmitted;

after a successful authentication, capturing a handwritten signature by said user on a given support, encrypting and transmitting said captured handwritten

signature to said remote secure server via said data network for storage in association with said user;

assigning a unique signature identifier thereto, generated by said secure server (80) and communicating said unique signature identifier to said user in order to be used as a reference during future authentication of said handwritten signature; and

storing said handwritten signature into said signature registration database (112) in association with said user and said unique signature identifier, which provides a reference during future authentication of said handwritten signature using said unique signature identifier.

20. A method according to claim 19, wherein the signature is handwritten by a user on a given support and personnel identification information associated with said user.

21. The method as claimed in claim 20, wherein said given support is a paper support.

22. The method as claimed in any one of claims 19 to 21, wherein said signature has been written by said user using an electronic pen by which it has been captured and transmitted to said processing unit.