CLAIMS:

1. A validation and authentication system for authenticating and validating messages, the system comprising:

a data store storing one or more digital fingerprints associated with user imaging devices;

a communication module configured to:

receive a message M;

receive a request for validation and authentication of at least one of the message M and a user and

receive an image P_M of the message M captured using a user imaging device associated with said user; and

an image validation module for analysing the received image P_M to determine if the image is valid by determining whether the received image P_M comprises a digital fingerprint matching one of the one or more digital fingerprints stored in the data store and to determine if the received image P_M is authentic by extracting data from the received image P_M and comparing the extracted data with the message M; and

wherein, if the received image P_M is determined to be authentic and valid, the image validation module generates a response to the request.

2. The validation and authentication system as claimed in claim 1, wherein the request is a request for validation and authentication of the message M and wherein, if the received image P_M is determined to be authentic and valid, the image validation module generates a response to the request which confirms that the message M is authentic and valid.

3. The validation and authentication system as claimed in claim 1, wherein the request is a request for validation and authentication of a user using the user imaging device and wherein, if the received image P_M is determined to be authentic and valid, the image validation module generates a response to the request which confirms that the user is authentic and valid.

4. The validation and authentication system as claimed in any one of the preceding claims wherein the image validation module comprises a ballistics sub-module

configured to determine that the received image P_M comprises a digital fingerprint matching one of the digital fingerprints stored in the data store.

5. The validation and authentication system as claimed in any one of the preceding claims wherein the image validation module comprises a forensics sub-module configured to determine that the received image P_M has not been altered during transit to the validation and authentication system.

6. The validation and authentication system as claimed in any one of the preceding claims wherein the image validation module comprises an optical character recognition sub-module configured to extract the data from the received image P_M, compare the extracted data with the received message M; and determine that the image is authentic if the extracted data matches the received message M.

7. The validation and authentication system as claimed in any preceding claim wherein the communication module is configured to receive at least one of:

the message M from a third party system;

the request for validation and authentication from the user or a third party system; and

the image P_M of the message M from the user.

8. The validation and authentication system as claimed in any preceding claim which is a central validation and authentication system which is remote from the user imaging device.

9. A validating and authenticating method comprising:

receiving a message M;

receiving a request for validation and authentication of at least one of the message M or a user;

receiving an image P_M of the message M captured using a user imaging device associated with said user;

analysing the received image P_M to determine if the image is valid by determining whether the received image P_M comprises a digital fingerprint matching one of one or more digital fingerprints stored in a data store wherein said one or more digital fingerprints are associated with user imaging devices and to determine if the image is

authentic by extracting data from the received image P_M and comparing the extracted data with the message M; and

generating, if the image is valid and authentic, a response to the request.

10. The method as claimed in claim 9, wherein receiving the request comprises:

receiving a request for validation and authentication of the message M and generating the response comprises generating a response which confirms or denies that the message M is authentic and valid; or

receiving the request comprises receiving a request for validation and authentication of a user using the user imaging device and generating the response comprises generating a response which confirms or denies that the user is authentic and valid.

11. The method as claimed in any one of claims 9 to 10 wherein analysing the received image P_M comprises using a ballistics image processing algorithm to extract the digital fingerprint from the received image P_M; and

wherein optionally analysing the received image P_M further comprises comparing the extracted digital fingerprint with the one of the one or more digital fingerprints stored in the data store, and determining if the extracted digital fingerprint corresponds to a stored digital fingerprint.

12. The method as claimed in any one of claims 9 to 11 wherein analysing the received image P_M further comprises using a forensics image processing algorithm to determine that the received image P_M has not been altered during transit.

13. The method as claimed in any one of claims 9 to 12 wherein analysing the received image P_M further comprises using an optical character recognition algorithm to extract the data from the received image P_M and compare the extracted data with the received message M.

14. The method as claimed in any one of claims 9 to 13 wherein receiving a message M comprises receiving the message M from a third party system; and

wherein optionally receiving an image P_M of the message M comprises capturing an image P_M of the message M using a user imaging device and receiving the image from the user imaging device.

15. The method as claimed in any one of claims 9 to 14 wherein receiving a request for validation and authentication comprises receiving a request from a user imaging device or a third party system.

16. A method of generating a digital signature, the method comprising:

receiving a request to create a signature for an electronic message M_F;

generating a validation challenge comprising the electronic message M which is based on message M_F;

receiving the electronic message M;

receiving a request for validation and authentication of at least one of the message M or a user;

validating and authenticating by:

receiving an image P_M of the electronic message M from a user;

analysing the received image P_M using to determine if the image is valid by determining whether the received image P_M comprises a digital fingerprint matching one of one or more digital fingerprints stored in a data store wherein said one or more digital fingerprints are associated with user imaging devices and to determine if the image is authentic by extracting data from the received image P_M and comparing the extracted data with the message M;

generating a validation response confirming that the received image P_M is valid and authentic; and

generating the signature for the electronic message M_F.

17. The method of claim 16, comprising

generating the signature for the electronic message M_F using a signature creation device which is local to the user imaging device.

18. The method of claim 17, comprising

authenticating and validating at an authentication and validation system which is part of at least one of:

the signature creation device;

the user imaging device; and

a user transaction device.

19. The method of claim 16, comprising

authenticating and validating at an authentication and validation system which is remote from the user imaging device; and

generating the signature for the electronic message M_F using a signature creation device which is remote from the user imaging device.

20. A non-transitory data carrier carrying processor control code which when running on a processor, causes the processor to implement the method of any one of claims 9 to 19.

21. A system for generating a digital signature on behalf of a user, the system comprising:

a signature server;

a data store storing one or more digital fingerprints associated with user imaging devices;

a communication module configured to:

receive a request to create a signature for an electronic message M_F;

receive an electronic message M, which is based on message M_F;

receive a request for validation and authentication of at least one of the message M and a user; and

receive an image P_M of the electronic message M from a user; and

an image validation module for analysing the received image P_M to determine if the image is valid by determining whether the received image P_M comprises a digital fingerprint matching one of the one or more digital fingerprints stored in the data store and to determine if the received image P_M is authentic by extracting data from the received image P_M and comparing the extracted data with the message M; and,

wherein, if the received image P_M is determined to be authentic and valid, the signature server generates a digital signature for electronic message M_F.