

in the art that various changes in form and detail may be made without departing from the spirit and scope of the invention which receives definition in the following claims.

What is claimed is:

1. A machine-implemented method for time-stamping and signing a digital message to establish the date and time when said message was received by a first machine, comprising the machine implemented steps of:

providing for the inputting of said message into said first machine;

providing for the coordination of the time of said first machine with Universal Coordinated Time (UTC);

providing for the addition of a time-stamp to said message, said time stamp being the Universal Coordinated Time (UTC) at which said first machine receives said message;

providing a procedure for checking the time accuracy of said first machine to verify the accuracy of the time-stamp;

providing for the computation of a hash code for the time-stamped message with a specific hashing procedure;

providing for the computation of a digital signature for the hashed time-stamped message utilizing a private key; and

providing for outputting the signed hashed time-stamped message.

2. The method of claim 1 wherein said first machine is connected into an electronic network and further including the machine-implemented steps of:

providing for the acceptance of requests for the time of said first machine;

providing for the return of the time of said first machine to the requestor over the network wherein the accuracy of the time of said first machine can be checked by anyone connected into the network in a manner independent of the time-stamp operation.

3. The method of claim 2 wherein the steps of computing a hash code and computing a digital signature are performed on a second machine not connected to said electronic network, said method further comprising the step of:

providing for the transmittal of the time-stamped message from said first machine to said second machine.

4. The method of claim 3 further comprising the steps of:

providing for outputting the signed hashed time-stamped message from said second machine to said first machine; and

providing for sending the signed hashed time-stamped message over said electronic network to recipients as directed by the originator of said message.

5. The method of claim 4 wherein said first machine and said second machine are owned and operated by an authenticating agency and wherein said agency publishes a public key to decipher said signature produced with said private key.

6. The method of claim 1 wherein the genuiness and authenticity of the signed hashed time-stamped message is verified through machine-implemented steps comprising:

reading the original message and computing the hash code of the message using said specific hashing procedure; and

reading a public key and testing said signature using said public key.

7. A system for time-stamping and signing a digital message to establish the date and time when said message was received by a first machine, said system comprising:

a first machine including means for receiving a digital message and means for time-stamping said digital message upon reception with Universal Coordinated Time (UTC);

means for coordinating the time of said first machine with Universal Coordinated Time (UTC);

means for checking the time accuracy of said first machine to verify the time accuracy of the time-stamp;

means for computing a hash code for the time-stamped message utilizing a specific hashing procedure; and

means for computing a digital signature for the hashed time-stamped message utilizing a private key.

8. The system of claim 7 wherein said first machine is connected into an electronic network, said system further including:

means adapted for accepting requests from said network for the time of said first machine in a manner independent of the time-stamp operation and returning said time of said first machine to the requestor wherein the time accuracy of the time of said first machine can be checked by any interested party on said network.

9. The system of claim 8 further including:

a second machine not connected to any electronic network;

means for enabling said second machine to receive a time-stamped digital message from said first machine; and

said second machine including said means for computing a digital signature for the time-stamped message utilizing a private key.

10. The system of claim 9 wherein said second machine includes said means for computing a hash code for the time-stamped message.

11. The system of claim 10 further including:

means at said first machine for receiving the signed hashed time-stamped message from said second machine; and

means at said first machine adapted for transmitting said signed hashed time-stamped message over said network.

12. The system of claim 11 further including:

a plurality of first machines each connected in parallel with said first machine, each capable of receiving messages and time-stamping the received message; and

a plurality of second machines each connected in parallel with said second machine, each capable of receiving a time-stamped digital message and including means for computing a digital signature using a private key.