C L A I M S

1. Method for creating a signal for time-stamping of documents, **c h a r a c t e r i s e d   i n** that the method comprises the following steps:

    a)   selecting a digitally stored reference document, which reference document is a digital description or sample of the current state of a certain physical reference source and/or information reference source at a certain first point in time, where the truthfulness of each reference document can be verified by consulting one or several publically available information sources concerning the historic state of said reference source;

    b)   using the reference document as one of at least one input values to a one-way function, and calculating the corresponding output value of the one-way function;

    c)   updating the signal based upon the said output value, so that the said output value is constituted by or can be determined based upon the value of the signal; and

    d)   repeating from a) using another digitally stored reference document which is a digital description or sample of the current physical state and/or information state of the same or another reference source at a subsequent point in time.

2. Method according to claim 1, **c h a r a c t e r i s e d   i n** that at least one reference source is a set of specified publically published information, the state of which is not known beforehand, such as a set of stock exchange quotes or a set of winning lottery numbers.

3. Method according to claim 1 or 2, **c h a r a c t e r i s e d   i n** that at least one reference source is a publically published physical event, the state of which is not

known beforehand, such as a specific sports event or speci-
fied news coverage.

4. Method according to any one of the preceding claims,
c h a r a c t e r i s e d   i n that the reference source is
publically available video footage, wherein the frames of the
video stream and/or a publically available audio stream are
used as reference documents.

5. Method according to any one of the preceding claims,
c h a r a c t e r i s e d   i n that the reference document
selected in step a) is associated with the output value cal-
culated in step b) or the signal value as updated in step c),
and in that the reference document is stored for future ref-
erence.

6. Method according to any one of the preceding claims,
c h a r a c t e r i s e d   i n that a collection of different
reference sources are used, and that reference documents
representing different reference sources, or different combi-
nations of such reference documents, are used as input value
in step b) in different iterations of the method.

7. Method according to any one of the preceding claims,
c h a r a c t e r i s e d   i n that for some or all iterations
of the method, a previous or current value of the signal, a
value which a previous or current value of the signal is
based upon, or a value calculated based upon such previous or
current signal value, is used as an input value in step b).

8. Method according to any one of the preceding claims,
c h a r a c t e r i s e d   i n that a certain document is
time-stamped using the current value of the signal, and in
that at least a part of a digitally stored version of the
certain time-stamped document, or the output value of a one-

way function an input value of which is the certain document, is used as an input value in step b) in an iteration of the method.

9. Method according to any one of the preceding claims, **c h a r a c t e r i s e d   i n** that the current value of the signal is continuously or periodically published or sent to a receiver.

10. Method according to claim 10, **c h a r a c t e r i s e d   i n** that the value of the signal is changed and the updated signal is published or sent at least once every minute.

11. Method for creating a digital signature of a document, where the signature is created so that it is constituted by, comprises or is calculated based upon the output value of a certain signature one-way function, where an input value to the signature one-way function is at least a part of a digitally stored version of the document in question, **c h a r - a c t e r i s e d   i n** that a signal is created according to any one of the preceding claims, and in that the current value of the signal, or a value which has been calculated based upon the current value of the signal, is also used as an input value to said signature one-way function.

12. Method according to claim 11, **c h a r a c t e r i s e d   i n** that the signature, or a value which has been calculated based upon the signature, is publically published over at least one publication channel, which channel provides the possibility for third parties to, at a later point in time, verify the publication time of the signature.

13. Method according to claim 12, **c h a r a c t e r i s e d   i n** that the publication channel is controlled by a third party.

14. Method according to claim 12 or 13, **c h a r a c t e r - i s e d i n** that signatures are calculated for a plurality of documents at different times, in that said calculated signatures are logically stored as leaves in a tree structure, in that a respective output value of a tree one-way function is calculated for each parent node in the tree structure, where the signatures and/or calculated tree one-way function output values of each respective child node for the parent node in question are used as input values for the tree one-way function, and in that it is the tree one-way function output value of a tree root, or a value which has been calculated based upon this output value, which is publically published.

15. Method according to claim 14, **c h a r a c t e r i s e d i n** that the tree one-way function output value of the tree root, or a value which has been calculated based upon this output value, is published also without being a consequence of a signature having been created for a document, and that such publication is preceded by the addition to the tree structure of a value which is not the freshly calculated signature of a document.

16. Method according to claim 15, **c h a r a c t e r i s e d i n** that the value added to the tree structure is one of the previously calculated output values of the tree one-way function.

17. Method according to any one of claims 11-16, **c h a r - a c t e r i s e d i n** that the digital version of the document used for the calculation of the signature one-way function output value is associated with the signature and stored for future reference.

18. Method according to any one of claims 11-17, **c h a r - a c t e r i s e d   i n** that a random number is also used as an input value to said signature one-way function, and in that the random number is associated with the document and/or the signature one-way function output value and stored.

19. Method for time-stamping a document, **c h a r a c t e r - i s e d   i n** that a signal is created according to any one of claims 1-10, and that the current value at the time of time-stamping of the document is embedded into the document or associated and stored together on a central server togeth- er with the document.

20. Method according to claim 19, **c h a r a c t e r i s e d   i n** that the signal is embedded into the document in the form of a piece of information from which the value of the signal can be deduced,

by introducing a graphical element, such as a string of alphanumeric characters, a QR code or a barcode, into a visu- al representation of the document, which graphical element carries said piece of information;

by adding said piece of information to a digitally stored version of the document as metadata; and/or

by adding said piece of information in the form of a dig- itally coded watermark to a digitally stored version of the document.

21. Method according to claim 19 or 20, **c h a r a c t e r - i s e d   i n** that the document comprises information cap- tured using a piece of sampling equipment for sampling a physical phenomenon, such as a camera or an audio recorder, which sampled physical phenomenon constitutes the document, in that the sampling equipment is provided access to a commu- nication channel over which the current value of the signal

is communicated to the sampling equipment, and in that the sampling equipment embeds the current signal value into the document in connection to performing the sampling.

22. Method according to claim 20 or 21, **c h a r a c t e r - i s e d   i n** that the document comprises at least one still image, or one frame in a moving image, captured using an image capturing device such as a camera, and that the current signal value at the time of capturing the image or frame is embedded into the image or frame by positioning a graphics-presenting device, arranged to show a graphical element carrying said piece of information, in the image or frame view so that the graphical element is captured as a part of the captured image or frame.

23. Method according to claim 22, **c h a r a c t e r i s e d   i n** that the graphics-presenting device is a part of the same general device as the image-capturing device, and in that the graphics-presenting device is arranged to present said graphical element at the same time as the image-capturing device captures an image depicting, via a mirror, an image covering the graphics-presenting device.

24. Method according to claim 20 or 21, **c h a r a c t e r - i s e d   i n** that the document comprises at least one still image, or one frame in a moving image, captured using an image capturing device such as a camera, and that the current signal value at the time of capturing the image or frame is embedded into the image or frame by feeding the signal to the image capturing device and causing the image capturing device to embed the said piece of information digitally into the image or frame.

25. Method according to any one of claims 20-24, **c h a r - a c t e r i s e d   i n** that the document is a frame in a video footage, and that the signal is embedded into the video footage by individual frames of the video being caused to contain the respective current value of the signal at the time of capturing the frame in question.

26. Method according to claim 25, **c h a r a c t e r i s e d   i n** that a number of consecutive frames comprise footage of a natural phenomenon the development of which is deterministic by nature.

27. Method according to claim 25 or 26, **c h a r a c t e r - i s e d   i n** the video footage is captured by a video conference system.

28. Method according to claim 25 or 26, **c h a r a c t e r - i s e d   i n** that the video footage is captured by a video surveillance system.

29. Method according to any one of claims 19-28, **c h a r - a c t e r i s e d   i n** that a digital signature of the time-stamped document is created according to any one of claims 11-18, associated with the document and stored in the central server.

30. Method according to claim 29, **c h a r a c t e r i s e d   i n** that the document is captured using a piece of sampling equipment for sampling a physical phenomenon, such as a camera or an audio recorder, which sampling equipment is caused to calculate the said digital signature in connection to performing the sampling, which sampled physical phenomenon constitutes the document, and in that the sampling equipment is provided access to a communication channel over which the signature is communicated to the central server.

31. Method according to claim 30, **c h a r a c t e r i s e d i n** that the sampling equipment is caused to sample the physical phenomenon repeatedly over some period of time so that several reference documents are produced, in that at least a part of a digitally stored version of at least one time-stamped document is used, by the central server, as an input value in step b) in the method according to claim 1 for creating the signal, and in that the signal value after being updated using the time-stamped reference document is embedded into a reference document produced later than the said at least one time-stamped document.

32. Method according to claim 29, **c h a r a c t e r i s e d i n** that the document is a web page.

33. Method according to claim 32, **c h a r a c t e r i s e d i n** that the web page comprises programming code arranged to initiate a time-stamping according to claim 19 as a conse-quence of the web page being viewed.

34. Method of providing a way to verify the integrity of a document, **c h a r a c t e r i s e d i n** that the method com-prises the following steps:

e) time-stamping the document according to any one of claims 29-31;

f) publishing the document with a visibly embedded piece of information according to claim 22;

g) providing a communication channel over which a third party can send a depiction of the published document;

h) accepting said depiction of the published document and deducing the value of the signal from the piece of information visible in the depiction;

i) finding, in the central server and based upon the signal value, the document previously time-stamped using the said signal value, if any; and

j) if a document is found in the central server, communicating to the third party that document itself and/or information pertinent to that document.

35. Method of providing a way to verify the integrity of a digitally stored document which is published on the Internet and viewed using a web browser, **c h a r a c t e r i s e d   i n** that the method comprises the following steps:

e) time-stamping the document according to any one of claims 29-31;

f) publishing the document on the Internet with associated programming code arranged to react upon a selection of or clicking on the document, or the activation of a user control;

g) upon a detection of a selection of or clicking on the document, or an activation of said user control, by a third party viewing the document, sending the document to the central server;

h) upon receipt of the document therein, causing the central server to lookup if the document has been time-stamped by calculating the corresponding digital signature and checking if a document with the same digital signature has previously been time-stamped; and

i) if such a document is found, communicating to the third party information pertinent to the document.

36. Method according to claim 35, **c h a r a c t e r i s e d   i n** that, in step i), the said pertinent information is communicated in the form of the document itself with the said pertinent information visually embedded in the document.

37. Method according to claim 35 or 36, **c h a r a c t e r - i s e d   i n** that the document is a still or moving image, in that, upon a first selection of or click on the document, or activation of the user control, the said pertinent information is published in connection to the image without the web browser leaving the current web page.

38. Method according claim 37, **c h a r a c t e r i s e d   i n** that, upon a second selection of or click on the document, or activation of the user control, the web browser is redirected to another page, where the document together with pertinent information is presented.

39. Method according to any one of claims 34-38, **c h a r - a c t e r i s e d   i n** that said pertinent information comprises the time of the document time-stamp.

40. Method of verifying the integrity of a digitally stored document, **c h a r a c t e r i s e d   i n** that the method comprises, at a first point in time, creating a digital proof signature of the document according to any one of claims 11-18 and storing the digital proof signature, and, at a later second point in time, verifying the integrity of the document in question by receiving a digital copy of the document, creating a corresponding digital verification signature of the document according to any one of claims 11-18 and using the same value of the signal used for the creation of the digital proof signature, and confirming the integrity of the document only in case the digital proof signature is equal to the digital verification signature.

41. Method of verifying the integrity of a certain metadata information pertinent to a digitally stored document, **c h a r a c t e r i s e d   i n** that the method comprises, at a first point in time, creating a digital proof signature of

the document according to any one of claims 11-18, wherein the signature one-way function is calculated based upon both at least a part of a digitally stored version of the document itself and upon said metadata information, and storing the digital proof signature, and, at a later second point in time, verifying the integrity of the metadata in question by receiving the metadata information, creating a corresponding digital verification signature of the document according to any one of claims 11-18 and using the same value of the signal used for the creation of the digital proof signature, and confirming the integrity of the metadata information only in case the digital proof signature is equal to the digital verification signature pertinent to the document.

42. Method according to claim 41, **c h a r a c t e r i s e d i n** that there are several pieces of metadata pertinent to the digitally stored document, in that, at the said first point in time, a separate digital metadata signature is created according to any one of claims 11-18 for each such piece of metadata and stored, and that the digital proof signature is created so that the signature one-way function is calculated based upon also each digital metadata signature, in that, at the said second point in time, a subset of the several pieces of metadata is received, corresponding digital verification signatures are created both of the received pieces of metadata and of the document according to any one of claims 11-18 and using the same value of the signal used for the creation of the digital metadata signatures and the digital proof signature, wherein the stored digital metadata signatures are used for pieces of metadata not received at the second point in time, and confirming the integrity of the subset of the pieces of metadata only in case the digital proof signature is equal to the digital verification signature pertinent to the document.

43. Method of providing a way to verify that a certain document is published in realtime or near realtime, **c h a r a c - t e r i s e d   i n** that the method comprises the following steps:

e) continuously time-stamping the document according to any one of claims 29-31; and

f) providing access for a third party to a means for comparing a continuously updated piece of information which is embedded into the document with a corresponding current signal value stored in the central server.

44. Method according claim 43, **c h a r a c t e r i s e d   i n** that the document is published on the Internet, and that the said means for comparing the continuously updated piece of information is in the form of program code which is associated with the document and arranged to automatically perform such a comparison and to signal to the third party whether a signal value deduced from the piece of information corresponds to the current value of the signal.

45. Method for verifying the integrity of data in a database, **c h a r a c t e r i s e d   i n** that at least one digital proof signature is created of said data according to any one of claims 11-18 and stored, in that the integrity of the said data is repeatedly checked by comparing the stored digital proof signature with a corresponding but later created digital verification signature which is based upon the current value of the data to be verified and the same signal value used for creation of the digital proof signature, and in that a report is sent in case of any discrepancy between the digital verification signature and the digital proof signature.

46. Method according to claim 45, **c h a r a c t e r i s e d i n** that the value of the stored digital proof signature is updated repeatedly, by creating a new digital proof signature according to any of claims 11-18.

47. Method according to claim 46, **c h a r a c t e r i s e d i n** that the updating of the value of the stored digital proof signature is triggered by access events to the database.