CLAIMS

1. A method of reading with a reader device a marking comprising a physical unclonable function, PUF, comprising the following steps:

a stimulation step, wherein a physical challenge according to a predetermined challengeresponse authentication scheme corresponding to the PUF is created and applied to a PUF;

a detection step, wherein a response generated by the PUF in accordance with the challengeresponse authentication scheme in reaction to the challenge is detected and a digital signal representing the response is generated;

a processing step, wherein the digital signal is processed in order to generate a hash value of the response by application of a predetermined cryptographic hash function to the digital signal,

an output step, wherein data representing the generated hash value as a first reading result is output,

an acquisition step, wherein a composite security marking comprising a PUF and a corresponding first digital signature or a pointer indicating a source where such first digital signature can be accessed is read, and said first digital signature is acquired from the marking or the source indicated by the pointer, respectively;

wherein the acquisition step further comprises acquiring from the composite security marking a second digital signature or a pointer indicating a source where a particular second digital signature pertaining to the marking can be accessed; and

in the output step a representation of the acquired first digital signature, and/or

a matching output indicating whether, according to at least one predetermined matching criterion, a hash value provided and signed by the acquired first digital signature matches the hash

value generated from the response to the challenge, is output;

wherein the output step further comprises outputting a representation of the acquired second

digital signature as a second reading result.

2. The method of claim 1, wherein in the processing step the digital

signal is generated in such a way that it represents at least one PDF-specific distinctive property of the

response that is, at least substantially, invariant under variations of the environmental conditions at

which the response is detected.

3. The method of claim 1, wherein detecting the response in the detection

step comprises detecting at least one property of electromagnetic radiation emitted by the PUF as a

response in reaction to the challenge and the digital signal is generated such that it represents this

response.

4. The method of claim 3, wherein detecting the response in the detection

step comprises detecting a characteristic lifetime of a luminescence effect occurring in the response as

a property of electromagnetic radiation emitted by the PUF.

5. The method of claim 3, wherein:

detecting the response in the detection step comprises detecting a spectrum of the emitted

radiation as a property of electromagnetic radiation emitted by the PUF; and

processing the digital signal in the processing step comprises determining from the digital

signal one or more of the following:

the position of one or more characteristic features within the spectrum;

one or more statistical measures characterizing the spectrum;

one or more quantized spectral values of the spectrum;

a spectral barcode representing a continuous or a quantized range of allowed spectral values

occurring in the spectrum.

6. The method of claim 1, wherein the output step further comprises outputting at least a part of a reading result in the form of a one-dimensional or a multi-dimensional barcode.

7. The method of claim 1, further comprising an authentication step, wherein a user is authenticated before permitting him or her to further operate the reader device in case of a successful authentication.

8. The method of claim 1, further comprising a communication step, wherein a reading result is communicated over a communication link to an opposing side.

9. The method of claim 8, wherein the communication step further comprises capturing and sending security-related information to a predetermined opposing side over the communication link.

10. The method of claim 8, further comprising an information monitoring step, wherein a security event is detected in information contained in a signal received from the opposing side over the communication link.

11. The method of claim 1, further comprising an access monitoring step, wherein one or more of the following are detected by means of one or more sensors as a security event:
an attempt or actual act of physical intrusion into the reader device;
an attempt or actual act of locally or remotely accessing an internal control functionality of the reader device, wherein such access is not available to a user of the device in the course of its normal operation.

12. The method of claim 10, further comprising a security defense step,

wherein one or more of the following security measures are performed in reaction to detection of a

security event:

locking the reader device such as to limit or prevent its further use;

self-destroying at least one functional part of the reader device or destroying data stored therein in

order to prevent its further use or access by a user;

outputting an error message.

13. The method of claim 1, wherein the outputting step comprises digitally

signing data containing the generated hash value and outputting the resulting digital signature as the

first reading result.

14. The method of claim 1, further comprising a storage step, wherein a

reading result being output in the output step is stored into a block of a blockchain.

15. The method of claim 1, wherein the storage step comprises:

storing a first reading result comprising data representing the hash value generated in the

processing step into a block of a first blockchain; and

storing the second reading result obtained in the acquisition step of claim 29 into a block of

second blockchain being separate from the first blockchain.

16. The method of claim 15, wherein the storage step further comprises:

when storing the first reading result in a block of the first blockchain, including a crossblockchain

pointer, which logically maps the block of the first blockchain to a corresponding block of

the second blockchain into the block of the first blockchain; and

when storing the second reading result in a block of the second blockchain, including a crossblockchain

pointer, which logically maps the block of the second blockchain to a corresponding block

of the first blockchain into the block of the second blockchain.

17. A reader device for reading a marking comprising a physical unclonable function, PUF, wherein the reader device is adapted to perform the method of claim 1.

18. The reader device of claim 17 comprising:
a stimulator being configured to perform the stimulation step;
a PDF-detector being configured to perform the detection step;
a processing device configured to perform the processing step; and
an output generator being configured to perform the outputting step.

19. The reader device of claim 18, further comprising one or more of the following:
an acquisition device configured to perform the acquisition step wherein a composite security
marking comprising a PUF and a corresponding first digital signature or a pointer indicating a source
where such first digital signature can be accessed is read, and said first digital signature is acquired
from the marking or the source indicated by the pointer, respectively; and
in the output step a representation of the acquired first digital signature, and/or
a matching output indicating whether, according to at least one predetermined matching
criterion, a hash value provided and signed by the acquired first digital signature matches the hash
value generated from the response to the challenge, is output;
an authentication device configured to perform the authentication step wherein a user is
authenticated before permitting him or her to further operate the reader device in case of a successful
authentication;
a communication device configured to perform the communication step further comprises
capturing and sending security-related information to a predetermined opposing side over the

communication link;

a monitoring device configured to perform the information monitoring step wherein a security

event is detected in information contained in a signal received from the opposing side over the

communication link;

a security device comprising at least one sensor and being configured to perform the access

monitoring step wherein one or more of the following are detected by means of one or more sensors as

a security event:

an attempt or actual act of physical intrusion into the reader device;

an attempt or actual act of locally or remotely accessing an internal control functionality of the

reader device, wherein such access is not available to a user of the device in the course of its normal

operation;

a security defense arrangement being configured to perform the security defense step wherein

one or more of the following security measures are performed in reaction to detection of a security

event:

locking the reader device such as to limit or prevent its further use;

self-destroying at least one functional part of the reader device or destroying data stored therein

in order to prevent its further use or access by a user;

outputting an error message;

a blockchain storing device configured to perform the storage step wherein a reading result

being output in the output step is stored into a block of a blockchain.

20. A method of reading with a reader device a marking comprising a

physical unclonable function, PUF, comprising the following steps:

a stimulation step, wherein a physical challenge according to a predetermined challengeresponse

authentication scheme corresponding to the PUF is created and applied to a PUF;

a detection step, wherein a response generated by the PUF in accordance with the challengeresponse
authentication scheme in reaction to the challenge is detected and a digital signal representing
the response is generated;
a processing step, wherein the digital signal is processed in order to generate a hash value of the
response by application of a predetermined cryptographic hash function to the digital signal,
an output step, wherein data representing the generated hash value as a first reading result is
output;
an access monitoring step, wherein one or more of the following are detected by means of one
or more sensors as a security event:
an attempt or actual act of physical intrusion into the reader device;
an attempt or actual act of locally or remotely accessing an internal control functionality
of the reader device, wherein such access is not available to a user of the device in the course of its
normal operation.

21. A reader device for reading a marking comprising a physical unclonable function, PUF, wherein the reader device is adapted to perform the method of claim 20.

22. The reader device of claim 21 comprising:
a stimulator being configured to perform the stimulation step;
a PDF-detector being configured to perform the detection step;
a processing device configured to perform the processing step; and
an output generator being configured to perform the outputting step.

23. The reader device of claim 21, further comprising one or more of the following:
an acquisition device configured to perform the acquisition step wherein a composite security

marking comprising a PUF and a corresponding first digital signature or a pointer indicating a source

where such first digital signature can be accessed is read, and said first digital signature is acquired

from the marking or the source indicated by the pointer, respectively; and

in the output step a representation of the acquired first digital signature, and/or

a matching output indicating whether, according to at least one predetermined matching

criterion, a hash value provided and signed by the acquired first digital signature matches the hash

value generated from the response to the challenge, is output;

an authentication device configured to perform the authentication step wherein a user is

authenticated before permitting him or her to further operate the reader device in case of a successful

authentication;

a communication device configured to perform the communication step further comprises

capturing and sending security-related information to a predetermined opposing side over the

communication link;

a monitoring device configured to perform the information monitoring step wherein a security

event is detected in information contained in a signal received from the opposing side over the

communication link;

a security device comprising at least one sensor and being configured to perform the access

monitoring step wherein one or more of the following are detected by means of one or more sensors as

a security event:

an attempt or actual act of physical intrusion into the reader device;

an attempt or actual act of locally or remotely accessing an internal control functionality of the

reader device, wherein such access is not available to a user of the device in the course of its normal

operation;

a security defense arrangement being configured to perform the security defense step wherein

one or more of the following security measures are performed in reaction to detection of a security

event:

locking the reader device such as to limit or prevent its further use;

self-destroying at least one functional part of the reader device or destroying data stored therein

in order to prevent its further use or access by a user;

outputting an error message;

a blockchain storing device configured to perform the storage step wherein a reading result

being output in the output step is stored into a block of a blockchain.

24. The method of claim 20, wherein in the processing step the digital

signal is generated in such a way that it represents at least one PUP-specific distinctive property of the

response that is, at least substantially, invariant under variations of the environmental conditions at

which the response is detected.

25. The method of claim 20, wherein detecting the response in the detection

step comprises detecting at least one property of electromagnetic radiation emitted by the PUF as a

response in reaction to the challenge and the digital signal is generated such that it represents this

response.

26. The method of claim 25, wherein detecting the response in the detection

step comprises detecting a characteristic lifetime of a luminescence effect occurring in the response as

a property of electromagnetic radiation emitted by the PUF.

27. The method of claim 25, wherein:

detecting the response in the detection step comprises detecting a spectrum of the emitted
radiation as a property of electromagnetic radiation emitted by the PUF; and
processing the digital signal in the processing step comprises determining from the digital
signal one or more of the following:
the position of one or more characteristic features within the spectrum;
one or more statistical measures characterizing the spectrum;
one or more quantized spectral values of the spectrum;
a spectral barcode representing a continuous or a quantized range of allowed spectral values
occurring in the spectrum.

28. The method of claim 20, further comprising:
an acquisition step, wherein a composite security marking comprising a PUF and a
corresponding first digital signature or a pointer indicating a source where such first digital signature
can be accessed is read, and said first digital signature is acquired from the marking or the source
indicated by the pointer, respectively; and
in the output step, a representation of the acquired first digital signature, and/or a matching
output indicating whether, according to at least one predetermined matching criterion, a hash value
provided and signed by the acquired first digital signature matches the hash value generated from the
response to the challenge, is output.

29. The method of claim 28, wherein the acquisition step further comprises
acquiring from the composite security marking a second digital signature or a pointer indicating a
source where a particular second digital signal pertaining to the marking can be accessed; and
The output step further comprises outputting a representation of the acquired second digital
signature as a second reading result.

30. The method of claim 20, wherein the output step further comprises outputting at least a part of a reading result in the form of a one-dimensional or a multi-dimensional barcode.

31. The method of claim 20, further comprising an authentication step, wherein a user is authenticated before permitting him or her to further operate the reader device in case of a successful authentication.

32. The method of claim 20, further comprising a communication step, wherein a reading result is communicated over a communication link to an opposing side.

33. The method of claim 32, wherein the communication step further comprises capturing and sending security-related information to a predetermined opposing side over the communication link.

34. The method of claim 32, further comprising an information monitoring step, wherein a security event is detected in information contained in a signal received from the opposing side over the communication link.

35. The method of claim 34, further comprising a security defense step, wherein one or more of the following security measures are performed in reaction to detection of a security event:
locking the reader device such as to limit or prevent its further use;
self-destroying at least one functional part of the reader device or destroying data stored therein in order to prevent its further use or access by a user;
outputting an error message.

36. The method of claim 20, wherein the outputting step comprises digitally

signing data containing the generated hash value and outputting the resulting digital signature as the
first reading result.

37. The method of claim 20, further comprising a storage step, wherein a
reading result being output in the output step is stored into a block of a blockchain.

38. The method of claim 29, wherein the storage step comprises:
storing a first reading result comprising data representing the hash value generated in the
processing step into a block of a first blockchain; and
storing the second reading result obtained in the acquisition step of claim 29 into a block of
second blockchain being separate from the first blockchain.

39. The method of claim 38, wherein the storage step further comprises:
when storing the first reading result in a block of the first blockchain, including a crossblockchain
pointer, which logically maps the block of the first blockchain to a corresponding block of
the second blockchain into the block of the first blockchain; and
when storing the second reading result in a block of the second blockchain, including a crossblockchain
pointer, which logically maps the block of the second blockchain to a corresponding block
of the first blockchain into the block of the second blockchain.

40. A method of reading with a reader device a marking comprising a
physical unclonable function, PUF, comprising the following steps:
a stimulation step, wherein a physical challenge according to a predetermined challengeresponse
authentication scheme corresponding to the PUF is created and applied to a PUF;
a detection step, wherein a response generated by the PUF in accordance with the challengeresponse
authentication scheme in reaction to the challenge is detected and a digital signal representing

the response is generated;

a processing step, wherein the digital signal is processed in order to generate a hash value of the

response by application of a predetermined cryptographic hash function to the digital signal,

an output step, wherein data representing the generated hash value as a first reading result is

output;

a communication step, wherein a reading result is communicated over a communication link to

an opposing side;

an information monitoring step, wherein a security event is detected in information contained in

a signal received from the opposing side over the communication link; and

a security defense step, wherein one or more of the following security measures are performed

in reaction to detection of a security event:

locking the reader device such as to limit or prevent its further use;

self-destroying at least one functional part of the reader device or destroying data stored therein

in order to prevent its further use or access by a user;

outputting an error message.

41. A reader device for reading a marking comprising a physical unclonable function, PUF, wherein the reader device is adapted to perform the method of claim 40.

42. The reader device of claim 41 comprising:

a stimulator being configured to perform the stimulation step;

a PDF-detector being configured to perform the detection step;

a processing device configured to perform the processing step; and

an output generator being configured to perform the outputting step.

43. The reader device of claim 42, further comprising one or more of the following:

an acquisition device configured to perform the acquisition step wherein a composite security
marking comprising a PUF and a corresponding first digital signature or a pointer indicating a source
where such first digital signature can be accessed is read, and said first digital signature is acquired
from the marking or the source indicated by the pointer, respectively; and
in the output step a representation of the acquired first digital signature, and/or
a matching output indicating whether, according to at least one predetermined matching
criterion, a hash value provided and signed by the acquired first digital signature matches the hash
value generated from the response to the challenge, is output;
an authentication device configured to perform the authentication step wherein a user is
authenticated before permitting him or her to further operate the reader device in case of a successful
authentication;
a communication device configured to perform the communication step further comprises
capturing and sending security-related information to a predetermined opposing side over the
communication link;
a monitoring device configured to perform the information monitoring step wherein a security
event is detected in information contained in a signal received from the opposing side over the
communication link;
a security device comprising at least one sensor and being configured to perform the access
monitoring step wherein one or more of the following are detected by means of one or more sensors as
a security event:
an attempt or actual act of physical intrusion into the reader device;
an attempt or actual act of locally or remotely accessing an internal control functionality of the

reader device, wherein such access is not available to a user of the device in the course of its normal
operation;
a security defense arrangement being configured to perform the security defense step wherein
one or more of the following security measures are performed in reaction to detection of a security
event:
locking the reader device such as to limit or prevent its further use;
self-destroying at least one functional part of the reader device or destroying data stored therein
in order to prevent its further use or access by a user;
outputting an error message;
a blockchain storing device configured to perform the storage step wherein a reading result
being output in the output step is stored into a block of a blockchain.

44. A reader device for reading a marking comprising a physical unclonable function, PUF, comprising:
a simulator configured to create a physical challenge according to a predetermined challengeresponse
authentication scheme corresponding to the PUF and apply to a PUF;
a PDF-detector configured to detect a response generated by the PUF in accordance with the
challenge-response authentication scheme in reaction to the challenge, and generate a digital signal
representing the response;
a processor configured to process the digital signal in order to generate a hash value of the
response by application of a predetermined cryptographic has function to the digital signal;
an output generator configured to output data representing the generated hash value as a first
reading result; and
one or more of the following:
an acquisition device configured to perform an acquisition step wherein a composite

security marking comprising a PUF and a corresponding first digital signature or a pointer indicating a
source where such first digital signature can be accessed is read, and said first digital signature is
acquired from the marking or the source indicated by the pointer, respectively; and
the output generator outputs a representation of the acquired first digital signature,
and/or a matching output indicating whether, according to at least one predetermined matching
criterion, a hash value provided and signed by the acquired first digital signature matches the hash
value generated from the response to the challenge;
an authentication device configured to perform an authentication step wherein a user is
authenticated before permitting him or her to further operate the reader device in case of a successful
authentication;
a communication device configured to perform a communication step further
comprising capturing and sending security-related information to a predetermined opposing side over
the communication link;
a monitoring device configured to perform an information monitoring step wherein a
security event is detected in information contained in a signal received from the opposing side over the
communication link;
a security device comprising at least one sensor and being configured to perform an
access monitoring step wherein one or more of the following are detected by means of one or more
sensors as a security event:
an attempt or actual act of physical intrusion into the reader device;
an attempt or actual act of locally or remotely accessing an internal control
functionality of the reader device, wherein such access is not available to a user of the device in the
course of its normal operation;
a security defense arrangement being configured to perform a security defense step
wherein one or more of the following security measures are performed in reaction to detection of a

security event:

locking the reader device such as to limit or prevent its further use;

self-destroying at least one functional part of the reader device or destroying data stored

therein in order to prevent its further use or access by a user;

outputting an error message;

a blockchain storing device configured to perform a storage step wherein a reading result being

output in the output step is stored into a block of a blockchain.

45. The method of claim 1, wherein the digital signature or the pointer is implemented by

one or more of the following: (i) an alphanumeric string; (ii) a graphical or image representation; (iii) aone-dimensional or multi-dimensional barcode; (iv) a device transmitting a signal carrying the

representation of the digital signature or pointer.

46. The method of claim 45, wherein said device is a short-range wireless chip.