(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 060 540 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
21.09.2022 Bulletin 2022/38

(21) Application number: **21163036.3**

(22) Date of filing: **17.03.2021**

(51) International Patent Classification (IPC):
G06F 21/60 *(2013.01)* ***G06F 21/64*** *(2013.01)*
G06F 21/77 *(2013.01)*

(52) Cooperative Patent Classification (CPC):
G06F 21/602; G06F 21/64; G06F 21/77

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(71) Applicant: **Armleder, Sebastien**
1227 Carouge (CH)

(72) Inventor: **Armleder, Sebastien**
1227 Carouge (CH)

(74) Representative: **Stellbrink & Partner**
Patentanwälte mbB
Widenmayerstrasse 10
80538 München (DE)

(54) **DEVICES, SYSTEMS, AND METHODS FOR PERFORMING A DIGITAL SIGNATURE**

(57) The present invention relates to a data processing device for performing a digital signature. The data processing device comprises a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key. The data processing device further comprises an authorization protocol. The data processing device is configured to digitally sign a data element with a private data processing device key in the secure portion in response to successful completion of the authorization protocol. The present invention also relates to a system comprising the data processing device, and to corresponding methods.

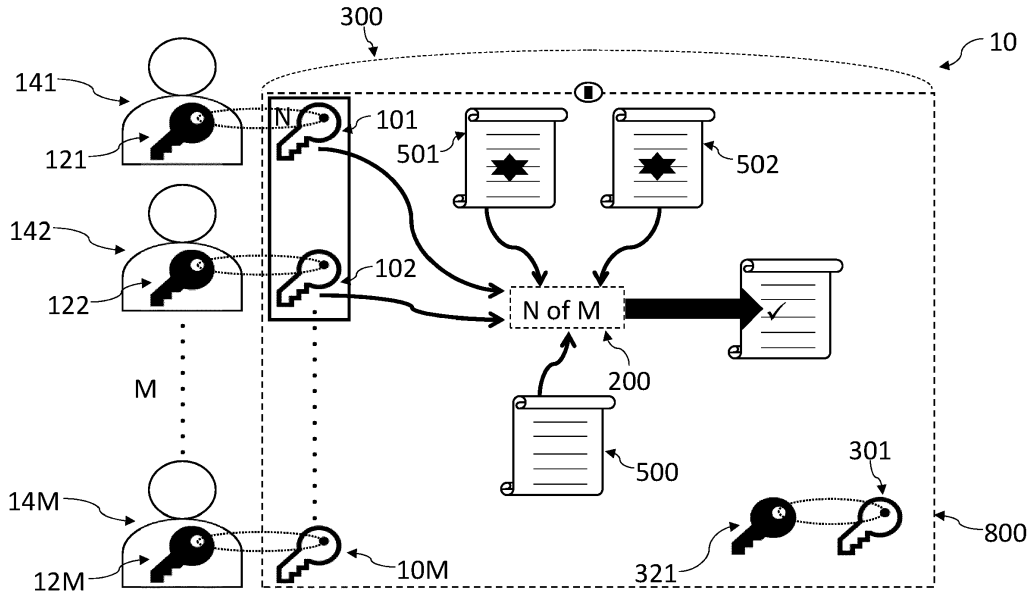

Fig. 3

EP 4 060 540 A1

Description

[0001] The present invention relates generally to cryptography and in particular to digital signing. More particularly, the present invention relates to a method for digitally signing a data element, such as a transaction.

[0002] Digital signature functionalities may be of particular interest for blockchain technologies. Blockchain technology has seen a spurt of growth in recent years. It has been used in healthcare, public service, financial services, and even video games. Among its most prominent uses have been cryptocurrencies, such as Bitcoin and Ethereum, and non fungible tokens, or NFTs, for proving ownership of various digital assets, such as digital art prints. Cryptocurrencies offer high security, accountability, and anonymity for transactions. Similarly, NFTs allow possession and trade of digital assets with a proof of authenticity linked to them. For example, an artist may put up their digital work for sale, with a proof of it being their original work, using an NFT which they may upload to a blockchain. The NFT may then be traded on the blockchain network with each transaction being recorded in a ledger of the blockchain. Thus, ownership of the "original" digital asset may be verified. Despite their attractive features however, neither has adoption of cryptocurrencies been as widespread as that of paper-based currencies, nor are digital assets as widely traded as physical ones.

[0003] One possible reason for this may be that each blockchain technology uses its own language, execution platform, and encryption system. Blockchains typically operate by distributing copies of a ledger to various 'nodes' in a network and any new transaction (for e.g., transferring a defined amount in the Bitcoin network) has to be verified and updated in the copy of the ledger (the Bitcoin ledger in the example cited above) at each node.

[0004] The verification process may comprise two steps. In a first step, proposed transactions may typically be signed digitally using an asymmetric encryption protocol, wherein the generator of the transaction uses their private key (accessible only to them) to digitally sign a transaction. For example, with regard to Bitcoin, the private key is Elliptic Curve (curve P256k1) Cryptography based, and provides control (and therefore ownership) to all the bitcoins associated with this private key, as well as allows for digitally signing transactions.

[0005] In a second step, the digitally signed transaction may then be verified by a plurality of the nodes using a public key, of the Bitcoin blockchain for example, accessible to everyone. Once a threshold number of nodes (which may depend on the size of the transaction) verifies a particular transaction, it can be included in an immutable block in the blockchain. The above procedure applies not only to transactions of cryptocurrencies but also to transactions related to NFTs.

[0006] Some popular asymmetric encryption schemes used are the Rivest-Shamir-Adleman (RSA) scheme designed by Ron Rivest, Adi Shamir and Leonard Adleman and Elliptic Curve Cryptography (ECC) designed by Neal Koblitz and Victor S. Miller independently. Digital signature algorithms are typically based on these asymmetric encryption schemes. A variant of digital signature algorithms based on elliptic curve cryptography is the Elliptic Curve Digital Signature Algorithm (ECDSA).

[0007] Each blockchain may use its own algorithm to generate private and public keys, and keys that may be used on one blockchain may not be used on another, depending on the level of security and the execution platform supported by the blockchain. For example, a transaction signed by an Ethereum blockchain private key may only be verified by an Ethereum blockchain public key and thus may not be suitable for verification by a public key of the Bitcoin blockchain.

[0008] While the presently known technology for signing transactions (or, more generally, a data element) may be sufficient in some regards, there are certain drawbacks and limitations. In particular, if a user intends to use more than one blockchain based network (e.g., the Ethereum and the Bitcoin network), they are typically required to have access to private keys of both networks, which is far from optimal as regards simplicity and ease of use. Embodiments of the present invention seek to overcome or at least alleviate the shortcomings and disadvantages of the prior art.

[0009] In a first aspect, the present invention relates to a data processing device for performing a digital signature, wherein the data processing device comprises a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key, an authorization protocol, wherein the data processing device is configured to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol. For example, the data processing device keys may correspond to the Bitcoin network in case the data processing device is used to sign a digital transaction from Ethereum to Bitcoin.

[0010] In certain embodiments, the private data processing key may never be extracted from the data processing device and the data processing device may be provided with a mechanism to self-destruct in case a limited number of failed attempts are made to tamper with the private data processing device key.

[0011] The authorization protocol may be used to restrict access to the digital signing functionality of the data processing device.

[0012] The authorization protocol may comprise the data processing device comprising M public keys, wherein M is a natural number, an N of M scheme, wherein N is a natural number not exceeding M. The data processing device may be configured to digitally sign a data element with a private data processing device key in the secure portion in response to receiving at least N versions

of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

[0013] For example, the M public keys may be the public keys of an Ethereum smart contract that may have been signed between M users. Each of those M users may hold their own private keys corresponding to the M public keys provided to the data processing device.

[0014] The secure portion of the data processing device may comprise the M public keys.

[0015] The secure portion may further comprise the N of M scheme.

[0016] M may be greater than 1. N may also be greater than 1. Preferably, N is strictly greater than 1 to allow for greater security. For example, if M is 3, N may be 2. Thus, access to digital signing functionality of the data processing device may only be possible if the owners of 2 private keys corresponding to the 2 public keys intend to sign the data element. This would disallow misuse of the data processing device by, for example, 1 malicious person.

[0017] The data processing device may be a card. This may allow it to be carried with ease and be simple to use.

[0018] Receiving the data element may also be a requirement for digitally signing the data element. This may also help to improve security. It may further be a necessary input for verification of the digital signatures by N of M private keys described above. Additionally, in some embodiments, it may not be possible to use the versions of the signed data element to retrieve the unsigned data element, and the unsigned data element may be needed to sign on it with the private data processing device key.

[0019] The data processing device may be configured to, in response to receiving the at least N versions of the data element, verify the at least N versions of the data element by using at least N of the M public keys, and to digitally sign the data element with the private data processing device key in the secure portion after a successful verification. Thus, a digital signature functionality of the data processing device may only be accessed after confirmation of the identity of N of M owners of the private keys corresponding to the M public keys stored in the data processing device and may add to the security of the data processing device.

[0020] The secure portion may comprise the seed, and the data processing device may be configured to receive a key derivation parameter. The secure portion may be further configured to generate a pair of a private data processing device key and a public data processing device key based on the key derivation parameter. This may be particularly advantageous if a backup device is provided for the data processing device. The key derivation parameter may then be used to sign a data element with a particular key using the backup device in case the data processing device is lost or malfunctions.

[0021] The data processing device may be configured to send the data element digitally signed with the private data processing device key.

[0022] In embodiments, the data processing device may also be configured to send the public data processing device key. For example, when the public data processing device key is used to sign a data element that may correspond to a transaction between two blockchains, e.g., from Ethereum to Bitcoin, the public data processing device key may be used to verify the authenticity of the transaction on the Bitcoin blockchain.

[0023] The data processing device may comprise a device identification code, and the successful completion of the authorization protocol may comprise receiving an identification code and comparing the identification code to the device identification code. This may provide for a simpler authorization protocol making it easier to use the data processing device. As may be appreciated, such a protocol may also make the data processing device more liable to misuse in case the device identification code is revealed. Thus, the authorization protocol comprising an N of M scheme as described above may be preferred.

[0024] The secure portion may comprise the device identification code and comparing the identification code to the device identification code may be performed in the secure portion.

[0025] The secure portion may further comprise the private data processing device key, and the data processing device may comprise a public data processing device key corresponding to the private data processing device key.

[0026] The secure portion may comprise the public data processing device key.

[0027] The secure portion may comprise the authorization protocol.

[0028] For example, embodiments of the present technology (where it should be understood that this relates to the described methods, devices, and systems) may be used for non fungible tokens ("NFT") on a blockchain. An NFT may be used to identify ownership of a specific digital asset, generally via a digest (hash) of this specific asset that is recorded on the table of a smart contract on a blockchain, jointly with the owner's public key (or a blockchain account with a public kley). Thus, a digital "original" is created and only the owner of the public key can assign / move the ownership of the digest to another account or public key. It will thus be understood that NFT is the basis for collectibles on blockchain.

[0029] In embodiments of the present technology, as described, an identification code (e.g., a personal identification number, PIN) may be used to authorize a functionality of a data processing device, e.g., a card. On the data processing device, and more particularly in the secure portion of the data processing device, e.g., a pair of a public and private key is generated.

[0030] That is, in such embodiments, the private key is "on the chip & hidden forever".

[0031] This may also be combined with the creation of a backup device, e.g., by means of a Diffie Hellman protocol, wherein the backup device generally corresponds to the data processing device. Thus, one can achieve provable uniqueness of a pair of card (one for backup).

[0032] Afterward, a digital asset can be transferred to the extractable public key (or the account linked to it) of the cards for ownership. Thus, the holder of both devices (i.e., the data processing device and the backup deice) owns the asset. It will be understood that the code inside the data processing device (e.g., card) and its authenticity may be verified by a factory certificate.

[0033] The data processing device may be further configured to, when digitally signing the data element, register this digital signing.

[0034] The data processing device may be configured to register this digital signing in the secure portion.

[0035] The data processing device may be configured to change a counter when digitally signing the data element. The counter may be in the secure portion.

[0036] The data processing device described above may further comprise a log file configured to register the digital signing. The secure portion may comprise the log file. The log file may register the digital signing along with the counter number. The log file may be useful for verification purposes, for example to prevent misuse. In such a case, it may be useful to have a log of transactions that have been already been made using the data processing device. Alternatively, it may be advantageous to have the data processing device insured. In this case, it may have to be proved that the data processing device has not been used until the time of insurance, for which purpose the log file may also be used.

[0037] In other words, the data processing device (e.g., the secure element) may have a tamper proof log file with a list of signed transactions, along with their corresponding counter number for further verification. Thus, e.g., it can be proven that the data device has not been used before.

[0038] The data processing device may comprise a true random number generator, and the true random number generator may be used to generate the private data processing device key and/or the seed in the data processing device. The true random number generator may comprise a random process inherent to the data processing device, for example, a quantum mechanical process, such as shot noise in electronic circuits, that may be amplified and sampled at various intervals to determine a sequence of bits (based on the noise crossing a threshold, for example) from which a seed may be generated. It may further comprise any of thermal noise, avalanche noise, atmospheric noise, vacuum energy fluctuations, or any other sources of random noise.

[0039] Alternatively, random input may further be provided to the data processing device that may be used together with the inherent random process, such as thermal fluctuations, present in the data processing device to generate the private data processing device key and/or the seed. By using a source of randomness inherent to the data processing device the uniqueness of the generated seed may be ensured.

[0040] Such an implementation may be used to provide a proof of uniqueness. In other words, the seed and/or the private data processing device key (which may also be referred to as the unique key) may generated inside the chip. If the chip has such a "true randomness" functionality, it can be demonstrated together with a code review that the key and/or the seed generated inside the chip is unique and was never extracted. In addition, entropy(randomness) can be injected inside the chip via random characters, to add to the internal randomness generation of the secure micro controller at the moment of seed generation.

[0041] Thus one can generate a unique key that you can prove nobody has ever seen. Furthermore, a backup of this key may be generated, e.g., by using a Diffie Hellman secret exchange, and a shared secret before, e.g., to prevent a man in the middle attack.

[0042] The data processing device may be configured to provide data stored in the secure portion by means of a cryptographic information exchange protocol only a limited number of times, wherein the limited number is preferably 1. The cryptographic information exchange protocol may be a Diffie-Hellmann information exchange protocol, further preferably an Elliptic Curve Diffie-Hellman information exchange protocol.

[0043] That is, the data processing device (i.e., the "original" device) may be designed by code on the secure element to only perform a backup once. Thus, it can be ensured that only one copy or "clone" of the data processing device may be generated.

[0044] In a second aspect, the present invention relates to a system comprising the data processing device as discussed before and a backup device comprising a backup secure portion, wherein the backup secure portion comprises the private data processing device key and/or the seed, the authorization protocol, and wherein the backup device is configured to digitally sign a data element with a private data processing device key in the backup secure portion in response to successful completion of the authorization protocol. A backup device may be helpful in case the data processing device gets lost or damaged.

[0045] The data processing device of the system as described above may comprise M public keys, and the N of M scheme, wherein the backup device may be configured to digitally sign a data element with the private data processing device key in the backup secure portion in response to receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

[0046] The private data processing device key and/or the seed and the authorization protocol may be provided to the backup secure portion by a cryptographic information exchange protocol, preferably by a Diffie-Hellmann information exchange protocol, further preferably by an Elliptic Curve Diffie-Hellman information exchange protocol. The information exchange protocol may be used to generate a shared private key prior to the exchange of information. For example, the data processing device

and the backup device may each comprise the shared private key, and information may be exchanged after symmetric encryption such that the shared private key may be used to both encrypt the data before sending it from the secure portion of the data processing device and decrypt the data after receiving it in the secure portion of the backup device. This may help to secure the information exchange against any men in the middle attacks.

[0047] The backup device may further comprise any of the features of the data processing device described above.

[0048] In particular, the data processing device may comprise a device identification code as described above and the backup secure portion may also comprise the device identification code.

[0049] The backup secure portion may also comprise the authorization protocol.

[0050] The backup device may be configured not to provide data stored in the backup secure portion by means of a cryptographic information exchange protocol. In other words, the backup device may have its "copying" or "cloning" functionality disabled.

[0051] In particular in combination with a data processing device that only allows data in its secure portion to be provided once, this may guarantee that the combination of the data processing device and the backup device is unique and no further copies can be generated.

[0052] In a third aspect, the present invention relates to a method of initializing a data processing device, wherein the method comprises providing the data processing device, wherein the data processing device comprises a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key, providing an authorization protocol to the data processing device, configuring the data processing device to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

[0053] The method may further comprise providing M public keys to the data processing device, wherein M is a natural number, providing an N of M scheme to the data processing device, wherein N is a natural number not exceeding M, configuring the data processing device to digitally sign a data element with a private data processing device key in the secure portion in response to receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

[0054] The data processing device may digitally sign the data element only when it receives the data element as well.

[0055] The method may further comprise the data processing device verifying the at least N versions of the data element by using at least N of the M public keys, and digitally signing the data element with the private data processing device key in the secure portion after a successful verification, in response to receiving the at least N versions of the data element.

[0056] The secure portion may comprise the seed, and the method may comprise providing a key derivation parameter to the data processing device and the secure portion generating a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

[0057] The method may further comprise sending the data element digitally signed with the private data processing device key.

[0058] The method may further comprise sending the public data processing device key.

[0059] The method may comprise providing a device identification code to the data processing device, and configuring the data processing device to, in response to receiving an identification code, compare the identification code to the device identification code, and successfully complete the authorization protocol when the identification code matches the device identification code.

[0060] The device identification code may be provided to the secure portion, and the data processing device may be configured to perform the comparison in the secure portion.

[0061] The authorization protocol may be provided to the secure portion.

[0062] The method may further comprise configuring the data processing device to when digitally signing the data element, register this digital signing, preferably in the secure portion.

[0063] The method may further comprise configuring the data processing device to change a counter when digitally signing the data element, wherein the counter preferably is in the secure portion.

[0064] The method may further comprises registering the digital signing in a log file, wherein the log file preferably is in the secure portion.

[0065] The method may further comprise providing a random input to the data processing device.

[0066] The method may further comprise the data processing device generating the private data processing device key and/or the seed using the true random number generator.

[0067] The method may also comprise configuring the data processing device to provide data stored in the secure portion by means of a cryptographic information exchange protocol only a limited number of times, wherein the limited number is preferably 1.

[0068] In a fourth aspect, the present invention relates to a method of generating a backup device, wherein the method comprises providing a data processing device according as discussed before, providing a second data processing device comprising a backup secure portion, and providing the private data processing device key and/or the seed, the authorization protocol to the second data processing device and thereby generating the back-

up device, and configuring the backup device to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

[0069] The method may further comprise providing the device identification code to the backup secure portion.

[0070] The method may comprise providing the device identification code to the backup secure portion by the cryptographic information exchange protocol.

[0071] The method may further comprise configuring the backup device to when digitally signing the data element, register this digital signing, preferably in the backup secure portion.

[0072] The method may further comprise configuring the backup device to change a counter when digitally signing the data element, wherein the counter is preferably stored in the backup secure portion.

[0073] The method may further comprise configuring the backup device to register a digital signing in a log file, wherein the log file is preferably stored in the backup secure portion.

[0074] The method may also comprise configuring the backup device not to provide data stored in the backup secure portion by means of a cryptographic information exchange protocol.

[0075] In a fifth aspect, the present invention relates to a method, wherein the method uses the data processing device as discussed before, wherein the method comprises successfully completing the authorization protocol, in response thereto, the data processing device digitally signing the data element with a private data processing device key in the backup secure portion.

[0076] The method may comprise signing at least each of N versions of a data element with a distinct private key corresponding to one of the M public keys, the data processing unit receiving the at least N signed versions of the data element, and in response thereto, the data processing unit digitally signing the data element with a private data processing device key in the secure portion.

[0077] In a sixth aspect, the present invention relates to a method, wherein the method uses the system discussed before, wherein the method comprises successfully completing the authorization protocol on the backup device, in response thereto, the backup device digitally signing the data element with a private data processing device key in the backup secure portion.

[0078] The method may further comprise signing at least each of N versions of a data element with a distinct private key corresponding to one of the M public keys, the backup device receiving the at least N signed versions of the data element, and in response thereto, the backup device digitally signing the data element with a private data processing device key in the backup secure portion.

[0079] The method may further comprise the backup device verifying the at least N versions of the data element by using at least N of the M public keys, and digitally signing the data element with the private data processing device key in the backup secure portion after a successful verification, in response to receiving the at least N versions of the data element.

[0080] The backup secure portion may comprise the seed, and the method may further comprise providing a key derivation parameter to the backup device and the backup secure portion generating a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

[0081] Below, device embodiments will be discussed. These embodiments are abbreviated by the letter "D" followed by a number. Whenever reference is herein made to device embodiments, these embodiments are meant.

D1. A data processing device for performing a digital signature, wherein the data processing device comprises
a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key,
an authorization protocol,
wherein the data processing device is configured to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

D2. The data processing device according to the preceding embodiment, wherein the data processing device comprises
M public keys, wherein M is a natural number,
an N of M scheme, wherein N is a natural number not exceeding M,
wherein the successful completion of the authorization protocol comprises
receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

D3. The data processing device according to the preceding embodiment,
wherein the secure portion comprises the M public keys.

D4. The data processing device according to any of the 2 preceding embodiments,
wherein the secure portion comprises the N of M scheme.

D5. The data processing device according to any of the 3 preceding embodiments, wherein M is greater than 1.

D6. The data processing device according to the preceding embodiment, wherein N is greater than 1.

D7. The data processing device according to any of the preceding embodiments, wherein the data processing device is a card.

D8. The data processing device according to any of the preceding embodiments, wherein receiving the data element is also a requirement for digitally signing the data element.

D9. The data processing device according to any of the preceding embodiments with the features of embodiment D2,
wherein the data processing device is configured to in response to receiving the at least N versions of the data element, verify the at least N versions of the data element by using at least N of the M public keys, and to digitally sign the data element with the private data processing device key in the secure portion after a successful verification.

D10. The data processing device according to any of the preceding embodiments, wherein the secure portion comprises the seed, and wherein the data processing device is configured to receive a key derivation parameter and wherein the secure portion is configured to generate a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

D11. The data processing device according to any of the preceding embodiments, wherein the data processing device is configured to send the data element digitally signed with the private data processing device key.

D12. The data processing device according to any of the preceding embodiments with the features of embodiment D10, wherein the data processing device is configured to send the public data processing device key.

D13. The data processing device according to any of the preceding embodiments, wherein
the data processing device comprises a device identification code, and
wherein the successful completion of the authorization protocol comprises
receiving an identification code and comparing the identification code to the device identification code.

D14. The data processing device according to the preceding embodiment,
wherein the secure portion comprises the device identification code and wherein comparing the identification code to the device identification code is performed in the secure portion.

D15. The data processing device according to any of the preceding embodiments,
wherein the secure portion comprises the private data processing device key, and
wherein the data processing device comprises a public data processing device key corresponding to the private data processing device key.

D16. The data processing device according to the preceding embodiment,
wherein the secure portion comprises the public data processing device key.

D17. The data processing device according to any of the preceding embodiments, wherein the secure portion comprises the authorization protocol.

D18. The data processing device according to any of the preceding embodiments,
wherein the data processing device is further configured to,
when digitally signing the data element, register this digital signing.

D19. The data processing device according to the preceding embodiment, wherein the data processing device is configured to register this digital signing in the secure portion.

D20. The data processing device according to any of the preceding embodiments, wherein the data processing device is configured to change a counter when digitally signing the data element.

D21. The data processing device according to the preceding embodiment, wherein the counter is in the secure portion.

D22. The data processing device according to any of the preceding embodiments and with the features of embodiment D18, wherein the data processing device comprises a log file configured to register the digital signing.

D23. The data processing device according to the preceding embodiment, wherein the secure portion comprises the log file.

D24. The data processing device according to any of the 2 preceding embodiments and with the features of embodiment D20, wherein the log file registers the digital signing along with the counter number.

D25. The data processing device according to any of the preceding embodiments, wherein the data

processing device comprises a true random number generator, and wherein the true random number generator is used to generate the private data processing device key and/or the seed in the data processing device.

D26. The data processing device according to the preceding embodiment, wherein the true random number generator is further provided with random input generated outside the data processing device to generate the private data processing device key and/or the seed.

D27. The data processing device according to any of the preceding embodiments, wherein the data processing device is configured to provide data stored in the secure portion by means of a cryptographic information exchange protocol only a limited number of times, wherein the limited number is preferably 1.

[0082] Below, system embodiments will be discussed. These embodiments are abbreviated by the letter "S" followed by a number. Whenever reference is herein made to system embodiments, these embodiments are meant.

S1. A system comprising the data processing device according to any of the preceding device embodiments and a backup device comprising a backup secure portion, wherein the backup secure portion comprises
the private data processing device key and/or the seed,
the authorization protocol,
wherein the backup device is configured to
digitally sign a data element with a private data processing device key in the backup secure portion in response to a successful completion of the authorization protocol.

S2. The system according to the preceding embodiment, wherein the data processing device is according to any of the preceding device embodiments with the features of embodiments D2, D3, and D4,
wherein the backup secure portion comprises

the M public keys, and
the N of M scheme,

and wherein the successful completion of the authorization protocol comprises
receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

S3. The system according to any of the preceding system embodiments, wherein the private data processing device key and/or the seed, and the authorization protocol are provided to the backup secure portion by a cryptographic information exchange protocol, preferably by a Diffie-Hellmann information exchange protocol, further preferably by an Elliptic Curve Diffie-Hellman information exchange protocol.

S4. The system according to the preceding embodiment and with the features of embodiment S2, wherein the M public keys, and the N of M scheme are provided to the backup secure portion by the cryptographic information exchange protocol.

S5. The system according to any of the preceding embodiments, wherein the data processing device is according to any of the preceding device embodiments with the features of embodiment D14, wherein the backup secure portion comprises the device identification code.

S6. The system according to the preceding embodiment and with the features of embodiment S3, wherein the device identification code is provided to the backup secure portion by the cryptographic information exchange protocol.

S7. The system according to any of the preceding system embodiments, wherein the data processing device is according to embodiment D17, wherein the backup secure portion comprises the authorization protocol.

S8. The system according to the preceding embodiment and with the features of embodiment S3, wherein the authorization protocol is provided to the backup secure portion by the cryptographic information exchange protocol.

S9. The system according to any of the preceding system embodiments, wherein the backup device comprises the features described according to any of the preceding device embodiments.

S10. The system according to any of the preceding embodiments, wherein the backup device is configured not to provide data stored in the backup secure portion by means of a cryptographic information exchange protocol.

[0083] Below, method embodiments will be discussed. These embodiments are abbreviated by the letter "M" followed by a number. Whenever reference is herein made to method embodiments, these embodiments are meant.

M1. A method of initializing a data process device, wherein the method comprises providing the data

processing device, wherein the data processing device comprises a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key,

providing an authorization protocol to the data processing device,
configuring the data processing device to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

M2. The method according to the preceding embodiment, wherein the method comprises
providing M public keys to the data processing device, wherein M is a natural number,
providing an N of M scheme to the data processing device, wherein N is a natural number not exceeding M,
wherein the successful completion of the authorization protocol comprises
receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

M3. The method according to the preceding embodiment, wherein
the M public keys are provided to the secure portion.

M4. The method according to any of the preceding method embodiments with the features of embodiment M2, wherein
the N of M scheme is provided to the secure portion.

M5. The method according to any of the preceding method embodiments with the features of embodiment M2, wherein M is greater than 1.

M6. The method according to any of the preceding method embodiments with the features of embodiment M2, wherein N is greater than 1.

M7. The method according to any of the preceding method embodiments, wherein the data processing device is a card.

M8. The method according to any of the preceding method embodiments, wherein the method further comprises the data processing device digitally signing the data element only when it receives the data element as well.

M9. The method according to any of the preceding method embodiments with the features of embodiment M2, wherein the method comprises
the data processing device verifying the at least N versions of the data element by using at least N of the M public keys, and
digitally signing the data element with the private data processing device key in the secure portion after a successful verification,
in response to receiving the at least N versions of the data element.

M10. The method according to any of the preceding method embodiments, wherein the secure portion comprises the seed, and wherein the method comprises providing a key derivation parameter to the data processing device and wherein the secure portion generates a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

M11. The method according to any of the preceding method embodiments, wherein the method further comprises sending the data element digitally signed with the private data processing device key.

M12. The method according to the penultimate embodiment, wherein the method further comprises sending the public data processing device key.

M13. The method according to any of the preceding method embodiments, wherein the method comprises
providing a device identification code to the data processing device, and configuring the data processing device to, in response to receiving an identification code, compare the identification code to the device identification code, and successfully complete the authorization protocol when the identification code matches the device identification code.

M14. The method according to the preceding embodiment, wherein the device identification code is provided to the secure portion, and wherein the data processing device is configured to perform the comparison in the secure portion.

M15. The method according to any of the preceding method embodiments, wherein the authorization protocol is provided to the secure portion.

M16. The method according to any of the preceding method embodiments, wherein the method further comprises
configuring the data processing device to when digitally signing the data element, register this digital signing, preferably in the secure portion.

M17. The method according to any of the preceding method embodiments, wherein the method further comprises configuring the data processing device to change a counter when digitally signing the data element, wherein the counter preferably is in the secure portion.

M18. The method according to any of the preceding method embodiments and with the features of embodiment M16, wherein the method further comprises registering the digital signing in a log file, wherein the log file preferably is in the secure portion.

M19. The method according to any of the preceding method embodiments, wherein the method further comprises providing a random input to the data processing device.

M20. The method according to any of the preceding method embodiments, wherein the data processing device has the features of embodiment D25, and wherein the method further comprises the data processing device generating the private data processing device key and/or the seed using the true random number generator.

M21. The method according to any of the preceding method embodiments, wherein the method comprises
configuring the data processing device to provide data stored in the secure portion by means of a cryptographic information exchange protocol only a limited number of times, wherein the limited number is preferably 1.

N1. A method of generating a backup device, wherein the method comprises
providing a data processing device according to any of the preceding device embodiments,
providing a second data processing device comprising a backup secure portion, and
providing the private data processing device key and/or the seed, the authorization protocol, to the second data processing device and thereby generating the backup device, and
configuring the backup device to
digitally sign a data element with a private data processing device key in the backup secure portion in response to a successful completion of the authorization protocol.

N2. The method according to the preceding embodiment, wherein the private data processing device key and/or the seed are provided to the backup secure portion by a cryptographic information exchange protocol, preferably by a Diffie-Hellmann information exchange protocol, further preferably by an Elliptic Curve Diffie-Hellman information exchange protocol.

N3. The method according to any of the 2 preceding embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiments D2, D3, and D4,
wherein the method further comprises providing the M public keys, and the N of M scheme to the second data processing device, and
configuring the backup data device to digitally sign a data element with a private data processing device key in the secure portion in response to
receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

N4. The method according to the preceding embodiment and with the features of embodiment N2, wherein the M public keys, and the N of M scheme are provided to the backup secure portion by the cryptographic information exchange protocol.

N5. The method according to any of the 4 preceding embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiment D17, and wherein the method comprises providing the authorization protocol to the backup secure portion.

N6. The method according to the preceding embodiment and with the features of embodiment N2, wherein the authorization protocol is provided to the backup secure portion by the cryptographic information exchange protocol.

N7. The method according to any of the 6 preceding embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiment D14, and wherein the method comprises providing the device identification code to the backup secure portion.

N8. The method according to the preceding embodiment and with the features of embodiment N2, wherein the device identification code is provided to the backup secure portion by the cryptographic information exchange protocol.

N9. The method according to any of the preceding 8 embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiment D18, wherein the method further comprises configuring the backup device to when digitally signing the data element, register this digital signing, preferably in the backup secure portion.

N10. The method according to any of the preceding 9 embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiment D20, wherein the method further comprises configuring the backup device to change a counter when digitally signing the data element, wherein the counter is preferably stored in the backup secure portion.

N11. The method according to any of the preceding 10 embodiments, wherein the provided data processing device is according to any of the preceding device embodiments with the features of embodiment D23,
wherein the method further comprises configuring the backup device to register a digital signing in a log file, wherein the log file is preferably stored in the backup secure portion.

N12. The method according to any of the preceding 11 embodiments, wherein the method further comprises
configuring the backup device not to provide data stored in the backup secure portion by means of a cryptographic information exchange protocol.

O1. A method, wherein the method uses the data processing device according to any of the preceding device embodiments, wherein the method comprises
successfully completing the authorization protocol,
in response thereto, the data processing unit digitally signing the data element with a private data processing device key in the secure portion.

O2. The method according to the preceding embodiment, wherein the method comprises
signing at least each of N versions of a data element with a distinct private key corresponding to one of the M public keys,
the data processing unit receiving the at least N signed versions of the data element.

O3. A method, wherein the method uses the system according to any of the preceding system embodiments, wherein the method comprises successfully completing the authorization protocol on the backup device,
in response thereto, the backup device digitally signing the data element with a private data processing device key in the backup secure portion.

O4. The method according to the preceding embodiment,
wherein the method comprises
signing at least each of N versions of a data element with a distinct private key corresponding to one of the M public keys,
the backup device receiving the at least N signed versions of the data element.

O5. The method according to the preceding embodiment, wherein the method further comprises
the backup device verifying the at least N versions of the data element by using at least N of the M public keys, and digitally signing the data element with the private data processing device key in the backup secure portion after a successful verification,
in response to receiving the at least N versions of the data element.

O6. The method according to any of the 2 preceding embodiments, wherein the backup secure portion comprises the seed, and wherein the method further comprises providing a key derivation parameter to the backup device and wherein the backup secure portion generates a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

O7. The method according to any of the 6 preceding method embodiments, wherein the method further comprises sending the data element digitally signed with the private data processing device key.

O8. The method according to any of the 7 preceding embodiments, wherein the method further comprises sending the public data processing device key.

[0084] Embodiments of the present technology will now be described with reference to the accompanying figures.

Figure 1 depicts an initialization of a data processing device with M public keys, an N of M scheme, and a private and public data processing device key;
Figure 2 depicts signing of N versions of a data element using N distinct private keys corresponding to the N public keys;
Figure 3 depicts the data processing device verifying the N signed elements;
Figure 4 depicts the data processing device digitally signing the data element using the private data processing device key;
Figure 5 depicts a data processing device according to another embodiment of the present technology;
Figure 6 depicts the data processing device of Fig. 5 digitally signing a data element using the private data processing device key upon successful completion of an authorization protocol;
Figure 7 depicts the data processing device further comprising a log file of digital signings and a counter.

[0085] Figure 1 depicts one embodiment of a system 10 of the present technology, where there are M pairs of public keys 101, 102, 10M and private keys 121, 122,

(...) 12M. In particular, in embodiment 10, M is 3. Each pair of public and private key may be associated with a user or owner 141, 142, ... 14M. Thus, in the example depicted in Figure 1, there are 3 pairs of public keys and private keys.

[0086] More particularly, there may be keys 101 and 121 forming a first key pair, keys 102 and 122 forming a second key pair and keys 10M, 12M forming a third key pair. For example, each of these key pairs may be associated with a first functionality, e.g., they may be associated with a smart contract and/or blockchain relating to Ethereum. In the depicted embodiments, a key filled with black color indicates a private key (see, e.g., keys 121, 122, 12M, and 321) and a "white" key indicates a public key (see, e.g., keys 101, 102, 10M, and 301).

[0087] Furthermore, in the discussed system 10, a data processing device 800 is provided. For example, the data processing device may be a card. The data processing device comprises a secure portion 300. In the depicted embodiments, all the discussed functionalities are realized in the secure portion 300, which is why the secure portion 300 substantially coincides with the data processing device 800. However, it should be understood that it is also possible that at least some functionalities of the data processing device 800 are realized outside of the secure portion 300.

[0088] Figure 1 depicts a first step, wherein the data processing device 800 may be initialized. The initialization may comprise providing the M public keys 101, 102, (...) 10M of the described key pairs to the data processing device 800, and providing a number N, wherein N is not greater than M, to the data processing device. This scheme is depicted by the label 200 in Fig. 1. In embodiments, the scheme 200 may be provided in the secure portion 300 of the data processing device 800.

[0089] For example, where M is 3, N may be 2. N indicates the number of signatures by the key pairs 101, 121, 102, 122, (...) 10M, 12M necessary to access functionalities of the data processing device 800. As may be appreciated by a person skilled in the art, N and M are both natural numbers, and N may not exceed M. Furthermore, it may be advantageous to have N greater than 1.

[0090] After initialization, the data processing device 800 may be used to perform a signature functionality.

[0091] As a mere example, it will be described how the data processing device can be used to perform a signature of a Bitcoin transaction. To sign such a transaction, again a pair of a private key 321 and a public key 301 may be used.

[0092] This key pair is present on the data processing device 800. More particularly, the private key 321 and optionally also the public key 301 is present in the secure portion 300 of the data processing device 800. Alternatively, the secure portion 300 may only comprise the private key 321 and no corresponding public key 301 (not shown). The private key 321 may not be extracted from the secure portion 300. The public key 301 may, on the other hand, be extracted from the secure portion 300 once functionalities of the data processing device 800 are enabled.

[0093] Figure 2 depicts a second step of the method, that may comprise digitally signing each of a plurality of versions of the data element 500 with one each of a plurality of the private keys 121, 122, (...) 12M and providing the plurality of signed versions of the data element 500 to the data processing device 800. Preferably, the plurality of signed versions of the data element 500 may be provided to the secure portion 300 of the data processing device 800. Further preferably, the data element 500 may be a hash relating to a transaction, for example, a Bitcoin transaction. Providing a hash may have the advantage that its length (in terms of bits) is fixed.

[0094] As described above, for the embodiment depicted in Figure 2, functionalities of the data processing device 800 may only be enabled when a defined number N of signatures (in the example: 2) is provided to the data processing device 800. More particularly, to enable functionalities, the data element 500 (e.g., the hash of the Bitcoin transaction) may be provided to the secure portion 300 of the data processing device 800, and at least N versions of the data element 500 digitally signed with different of the private keys 121, 122, (...) 12M.

[0095] For example, the data element 500 (which will be called "data"), a version of the data element signed with key 121 (which is labelled 501) and a version of the data element signed with 122 (which is labeled 502) can be provided to the secure portion 300 of the data processing device 800. This is depicted in Fig. 2, where a subset N of M is chosen which in this case is a subset 2 of 3. The chosen subset of private keys 121, 122, (...) 12M, which in this case is 121 and 122 are used to digitally sign copies of the data element 500. The signed copies are labelled 501 and 502 in Fig. 2. As described above, the digitally signed data elements 501 and 502 may correspond to one blockchain, for example Ethereum (depicted with a 6-sided star).

[0096] Figure 3 depicts a further step, that may be called a verification step, according to one embodiment of the present technology, wherein the digitally signed elements 501 and 502 are provided to the secure portion 300 of the data processing device 800. The data element 500 may also be provided to the secure portion 300 in this step. In the secure portion 300 of the data processing device 800, the signed versions 501 and 502 can be verified by using the public keys 101 and 102 and the data element 500.

[0097] When the correspondingly verified data elements 501, 502 correspond to the data element 500, this is indicative of 2 owners (namely the owners of keys 121 and 122) having agreed to enable the functionalities of the data processing device 800. In line with the N out of M agreement scheme 200 described above, this may trigger functionalities of the data processing device 800 and more particularly of the secure portion 300 of the data processing device 800.

[0098] Figure 4 depicts a further step, that may be

called a signing step. Once verification of the signed elements 501, 502 is completed, in response thereto, the secure portion 300 of the data processing device 800 may sign the data element 500 with its private key 321 to thereby generate a signed data element 600.

[0099] As described in the above example, this signed data element 600 is signed with a private key 321 of the Bitcoin network (depicted by a 7-sided star), and can be verified by the respective public key 301, which may also be extracted from the data processing device 800.

[0100] In embodiments, the key pair 301, 321 may be generated in the secure portion 300 of the data processing device 800. For example, the secure element 300 may have a random source of entropy to generate a seed, which may also be referred to as a pseudo random seed. Based on this seed, which may also be referred to as the private master key, a plurality of key pairs 301, 321 (...), 30S, 32S can be derived by a key derivation function. A key derivation parameter may then be additionally supplied to the secure portion 300 of the data processing device 800 to generate a particular set of keys.

[0101] The secure portion 300 may comprise computational processing means. For example, the secure portion 300 of the data processing device 800 may comprise a tamperproof secure microcontroller, such as, a NXP SmartMX secure microcontroller family, e.g., the NXP SmartMX3 P71D321. The use of secure microcontrollers may be particularly advantageous for increasing the security of transactions (i.e., data communications) between the secure portion 300 and an external device (for e.g., when sending out the signed data element 600 or the public key 301) or an unsecure portion of the data processing device 800 (for e.g., when receiving the signed elements 501 or 502). A secure microcontroller may facilitate hiding the private key 321 even in case of malware presence. Further, the secure microcontroller may be configured to mitigate side channel attack to discover the private key 321, may be sandboxed from the rest of the data processing device 800, and may be brute force resistant (e.g., self-destroys after a limited number of failed verifications).

[0102] Preferably, the secure portion 300 may provide hardware and software protection for maintaining the secrecy of the private key 321 (and any other data that may be stored in the secure portion 300). The secure portion 300 may comprise one or more secure microcontrollers and one or more secure memory components. Further, the data processing device 800 may comprise further components external to the secure portion 300. These can for example be, a general processor, general microcontroller, general memory devices and I/O interfaces. Said components may facilitate receiving and sending data to/from an external device or storing data such as the public keys 101, 102, (...) 10M.

[0103] It will be appreciated that the technology described above allows inter blockchain operability. More particularly, the users can use their key pairs of a first blockchain network (e.g., the Ethereum network in the above example) to authorize transactions in a second blockchain network (in the above example, in the Bitcoin network). By requiring at least N of M signatures to verify a transaction, it may help decentralize the method of digitally signing inter blockchain transactions. Further, by keeping the private (master) key 321 in a secure portion that may never be accessed by an external device, it may allow the method to also be trustless.

[0104] In the embodiment 10 described above, it will be understood that only the data processing device 800, and more particularly the secure portion 300 thereof, comprises the private key 321, which may thus never be visible.

[0105] Thus, when only the above discussed data processing device 800 is provided, and the private key 321 is required, this requires the use of the discussed data processing device 800. However, in case the data processing device 800 is lost or damaged, in the embodiment described above, there is no means of performing such a functionality. This may have severe consequences, e.g., in case the private key 321 is necessary to access, e.g., a Bitcoin account.

[0106] To overcome such problems, embodiments of the present technology also relate to "cloning" the data processing device 800 and more particularly the secure portion 300 thereof.

[0107] In such embodiments, the secure portion 300 of the data processing device 800 comprises the M public keys 101, 102 (...), 10M, the rule 200 relating to the N of M accessing scheme, and the private key 321 with or without its public key 301, or alternatively a seed, the so-called pseudo random seed or private master key.

[0108] This information may be cloned to another data processing device 800b, which will be referred to as a backup device. More particularly, it may be cloned to a secure portion 300b of the backup device 800b. In this regard, it is noted that the information may only be transferred to the secure portion of the backup device 800b, without being visible in the open.

[0109] More particularly, an information exchange protocol, such as the Diffie-Hellmann exchange protocol, more particularly the Elliptic Curve Diffie-Hellmann exchange protocol may be used to clone the information from the secure portion 300 in the data processing device 800 to the secure portion 300b in the backup device 800b.

[0110] The information exchange protocol may only allow all data described above, i.e., the M public keys 101, (...), 10M, the rule 200 relating to the N of M accessing scheme, and the seed to be exchanged together, but may prohibit that only a part of the data is exchanged (without the other data).

[0111] If, for example, the protocol would allow that only the seed and the public keys 101, (...), 10M be transferred (without requiring transfer of the rule 200 relating to the N of M accessing scheme), another accessing scheme could be implemented on the backup device 800b. For example, in such a scenario, a 1 of M accessing scheme could be implemented, which would allow a sin-

gle user to enable the functionalities of the backup device 800b, which would be detrimental to safety.

[0112] Both the original data processing device 800 and the backup device 800b may be originally implemented with a shared secret (which may also be referred to as shared encryption secret, shared signature secret or factory shared secret). This may prevent an emulated card to simulate the backup device 800b, and it may thus be prevented that an emulated card can extract information (e.g., the seed or a hidden key) from the secure portion 300 of the data processing device 800.

[0113] To validate the data exchange protocol, the original data processing device 800 and the backup device 800b may exchange a signature of each other's content (or a hash thereof), and the exactitude of the exchanged information may then be validated. In particular, the backup device 800b may be implemented to only enable its functionality if the exactitude of information compared to the original data processing device 800 has been validated.

[0114] Thus, the backup device 800b may be an exact clone of the data processing device 800, such that also the backup device 800b can be used, e.g., in case the data processing device 800 is lost or damaged.

[0115] Typically, when sending a data element 500 to be signed to the data processing device 800 (or to the backup device), a key derivation parameter may also be sent together with the data element 500. For example, the key derivation parameter may be "use the third key pair generated by the seed". Thus, by having the identical information stored in the secure portion 300b (and by means of the key derivation parameter), the original data processing device 800 and the backup device 800b would return the same signature if provided with the same request.

[0116] In the above, particular embodiments of the present technology have been described with reference to Figs. 1 to 4. However, it should be understood that these embodiments were merely exemplary and should not limit the scope of the present invention. For example, while in the above, an authorization protocol employing an N of M scheme and using M public keys was described, this authorization protocol was a mere example and also other authorization protocols can be used, as will be discussed below in conjunction with Figs. 4 and 5.

[0117] Fig. 5 depicts another exemplary data processing device 800 according to embodiments of the present technology. Again, the data processing device 800 may be a card. The data processing device 800 comprises a secure portion 300.

[0118] Similar to the data processing device 800 discussed above, the data processing device 800 comprises a pair of a private data processing device key 321 and a public data processing device key 301 in the secure portion 300. Furthermore, the secure portion 300 also comprises an authorization protocol 250. The authorization protocol 250 stores data and/or instructions relating to authorizing a functionality of the secure portion 300 and in particular a signing functionality in the secure portion 300.

[0119] In the embodiments discussed before, the authorization protocol 250 included the N of M scheme 200 and the private keys 101 to 10M.

[0120] However, the authorization protocol 250 may also be realized differently. For example, in the embodiment depicted in Fig. 5, the authorization protocol 250 may include a device identification code (which may also be referred to as a device PIN). For example, the device identification code may be an alphanumerical string.

[0121] With regard to Fig. 6, similar to the embodiments discussed above, a data element 500 may again be provided to the data processing device 10 and more particularly to the secure portion 300 thereof. However, in the embodiments of Figs. 5 and 6, a signing of the data element 500 may be triggered by a user entering an identification code 700 (e.g., a PIN).

[0122] Once this identification code 700 has been entered, assessed in the secure portion 300. More particularly, it is compared to the device identification code. If the two match, this indicates a successful authorization, i.e., a successful completion of the authorization protocol.

[0123] In response thereto, the data element 500 is signed by means of the private key 321, and thus a signed data element 600 is generated, which can then be output.

[0124] Furthermore, additional functionalities may be realized in the data processing device 800, and more particularly in the secure portion 300 thereof, as depicted in Fig. 7. It should be understood that the functionality discussed in conjunction with Fig. 7 is independent on the exact realization of the authorization protocol 250. For example, it may be used with an authorization protocol using an N of M scheme 200 and M public keys 101 to 10M as discussed above in conjunction with Figs. 1 to 4, but also in conjunction with the authorization protocol 250 based on a device identification code as discussed in conjunction with Figs. 5 and 6.

[0125] According to one potential additional functionality, a log file 920 for digital signatures is provided. The log file 920 may also be referred to as signature database or register. In the register, whenever a digital signature is performed by the device, details of this digital signature (e.g., the signed hashes) are stored, i.e., registered in the log file 920. Additionally, or alternatively, the secure portion 300 may comprise a counter 940. This counter may be changed (and more particularly increased by 1) whenever a digital signature is performed by means of the data processing device 800. The log file may additionally record the number on the counter with details of each digital signature recorded.

[0126] That is, in embodiments of the present technology, transaction logging and counters can be used. That is, the following functionality can be added to the data processing device 800 (e.g., the card): the data processing device can, e.g., register all the last 100 signed hashes. This opens up the possibility to verify the use of the card in the future.

[0127] Thus, it can be verified if and how the data processing device 800 was used. In particular, unintended use or hacking can also be documented, thereby increasing the security of the data processing device 800. More particularly, proof can be established that the card was not used for a specific transaction.

[0128] Furthermore, also a signature counter 940 can be implemented. This may be a simple way of storing and documented if and how often the data processing device 800 has been used.

[0129] For example, the transaction logging mechanism and/or counter mechanism of signed transactions to prove the past use of the hidden key, may also be applied in case of providing an insurance contract by an insurance company in case of the unlikely use of the "ever hidden" key by, e.g., side channel attack on the chip. For the insurance to cover a damage, the chip would have to be provided to be able to check the past transactions. By means of the transaction logger 920 and/or counter 940, it can thus be proven that the chip was not used to sign, such that an insurance may cover a potential damage.

[0130] Such functionalities may be of particular interest for non fungible tokens ("NFT"). For example, consider that a data processing device 800 and a corresponding backup device have been generated, and both of them have the respective data processing device private key 321 stored in their secure portion 300, wherein this data processing device private key 321 can be used to sign a data element to indicate (or transfer) ownership of an NFT.

[0131] In such a case, if both the data processing device and the backup device have a signature counter equaling 0, one can be confident that the NFT is still linked to the data processing device and no transaction of it has been performed by means of the data processing device. Without such a counter and register, it would be possible to receive the data processing device and the backup device, but a malicious agent may have used one of the data processing devices before transfer of ownership of the devices to generate a signed data element (indicative of a transaction of the NFT), and then publish this data element (i.e., finalize the transaction) later, such that the NFT would no longer be linked to the data processing device and the backup device. This is not possible if a register 920 and/or a counter 940 is provided in the secure portion 300 of the data processing device 800, such that these embodiments add to the security of the data processing device 800.

[0132] As described above for one embodiment of the data processing device 800 depicted in Fig. 1, a backup device 800b may also be provided for the data processing device 800 according to the embodiments depicted in Figs. 5 to 7.

[0133] More particularly, the backup device 800b may be a clone of the data processing device 800 according to any of the embodiments described above. For example, in the embodiment depicted in Fig. 5, where the data processing device 800 comprises a secure portion 300 and an authorization protocol 250 and a pair of a public data processing device key 301 and private data processing device key 321 in the secure portion 300, the backup device 800b may also comprise a backup secure portion 300b and a backup authorization protocol 250b and a pair of public data processing device key 301b and private data processing device key 321b in the backup secure portion 300b.

[0134] Additionally, the backup device 300b may comprises features of the embodiment depicted in Fig. 7, where the backup device 300b may comprise a backup secure portion 300b with an authorization protocol 250b according to any of the embodiments depicted in Fig. 1 or Fig. 5, and a backup log file 920b and a backup counter 940b may be further provided in the backup secure portion 300b.

[0135] The backup device 800b may be generated from the data processing device 800 by using a secure information exchange protocol, such that no information is visible in the open. For example, information may be exchanged using a protocol such as the Diffie-Hellmann exchange protocol, or more particularly the Elliptic Curve Diffie-Hellmann exchange protocol.

[0136] The information exchange protocol may further only allow all of the data comprised by the data processing device 800, for example the authorization protocol 250 and the pair of private and public data processing device keys 301, 321 to be exchanged, but may prohibit exchange of only a part of the data (without the other data).

[0137] Whenever steps were recited in the above or also in the appended claims, it should be noted that the order in which the steps are recited in this text may be accidental. That is, unless otherwise specified or unless clear to the skilled person, the order in which steps are recited may be accidental. That is, when the present document states, e.g., that a method comprises steps (A) and (B), this does not necessarily mean that step (A) precedes step (B), but it is also possible that step (A) is performed (at least partly) simultaneously with step (B) or that step (B) precedes step (A). Furthermore, when a step (X) is said to precede another step (Z), this does not imply that there is no step between steps (X) and (Z). That is, step (X) preceding step (Z) encompasses the situation that step (X) is performed directly before step (Z), but also the situation that (X) is performed before one or more steps (Y1), ..., followed by step (Z). Corresponding considerations apply when terms like "after" or "before" are used.

[0138] While in the above, preferred embodiments have been described with reference to the accompanying drawings, the skilled person will understand that these embodiments were provided for illustrative purpose only and should by no means be construed to limit the scope of the present invention, which is defined by the claims.

Claims

1. A data processing device for performing a digital signature, wherein the data processing device comprises
a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key,
an authorization protocol,
wherein the data processing device is configured to digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

2. The data processing device according to the preceding claim, wherein the data processing device comprises
M public keys, wherein M is a natural number,
an N of M scheme, wherein N is a natural number not exceeding M,
wherein the data processing device is configured to digitally sign a data element with a private data processing device key in the secure portion in response to
receiving at least N versions of the data element, wherein each of the N versions is signed by a distinct private key corresponding to one of the M public keys.

3. The data processing device according to the preceding claim, wherein the secure portion comprises the M public keys, and wherein the secure portion comprises the N of M scheme.

4. The data processing device according to any of the preceding claims,
wherein the data processing device is configured to in response to receiving the at least N versions of the data element, verify the at least N versions of the data element by using at least N of the M public keys, to digitally sign the data element with the private data processing device key in the secure portion after a successful verification, and
to send the data element digitally signed with the private data processing device key.

5. The data processing device according to any of the preceding claims, wherein the secure portion comprises the seed, and wherein the data processing device is configured to receive a key derivation parameter and wherein the secure portion is configured to generate a pair of a private data processing device key and a public data processing device key based on the key derivation parameter.

6. The data processing device according to the preceding claim, wherein the data processing device is configured to send the public data processing device key.

7. The data processing device according to any of the preceding claims, wherein the secure portion comprises the authorization protocol and wherein
the data processing device comprises a device identification code, and
wherein the successful completion of the authorization protocol comprises
receiving an identification code and comparing the identification code to the device identification code, preferably in the secure portion of the data processing device.

8. The data processing device according to any of the preceding claims, wherein the data processing device is further configured to, when digitally signing the data element, register this digital signing, and wherein the data processing device comprises a log file configured to register the digital signing.

9. The data processing device according to any of the preceding claims, wherein the data processing device is configured to change a counter when digitally signing the data element.

10. The data processing device according to any of the preceding claims, wherein the data processing device is a card.

11. A system comprising the data processing device according to any of the preceding claims, and a backup device comprising a backup secure portion, wherein the backup secure portion comprises
the private data processing device key and/or the seed,
the authorization protocol,
wherein the backup device is configured to
digitally sign a data element with a private data processing device key in the backup secure portion in response to a successful completion of the authorization protocol.

12. The system according to the preceding claim, wherein the private data processing device key and/or the seed, and the authorization protocol are provided to the backup secure portion by a cryptographic information exchange protocol, preferably by a Diffie-Hellmann information exchange protocol, further preferably by an Elliptic Curve Diffie-Hellman information exchange protocol.

13. The system according to any of the 2 preceding claims, wherein the backup device comprises the features described according to any of the claims 1

to 10.

14. A method of initializing a data processing device, wherein the method comprises
providing the data processing device, wherein the data processing device comprises a secure portion, wherein the secure portion comprises a private data processing device key and/or wherein the secure portion comprises a seed configured to generate at least one pair of a private data processing device key and a public data processing device key,
providing an authorization protocol to the data processing device,
configuring the data processing device to
digitally sign a data element with a private data processing device key in the secure portion in response to a successful completion of the authorization protocol.

15. A method of generating a backup device, wherein the method comprises
providing a data processing device according to any of the claims 1 to 10,
providing a second data processing device comprising a backup secure portion, and
providing the private data processing device key and/or the seed, the authorization protocol, to the second data processing device and thereby generating the backup device, and
configuring the backup device to
digitally sign a data element with a private data processing device key in the backup secure portion in response to a successful completion of the authorization protocol.

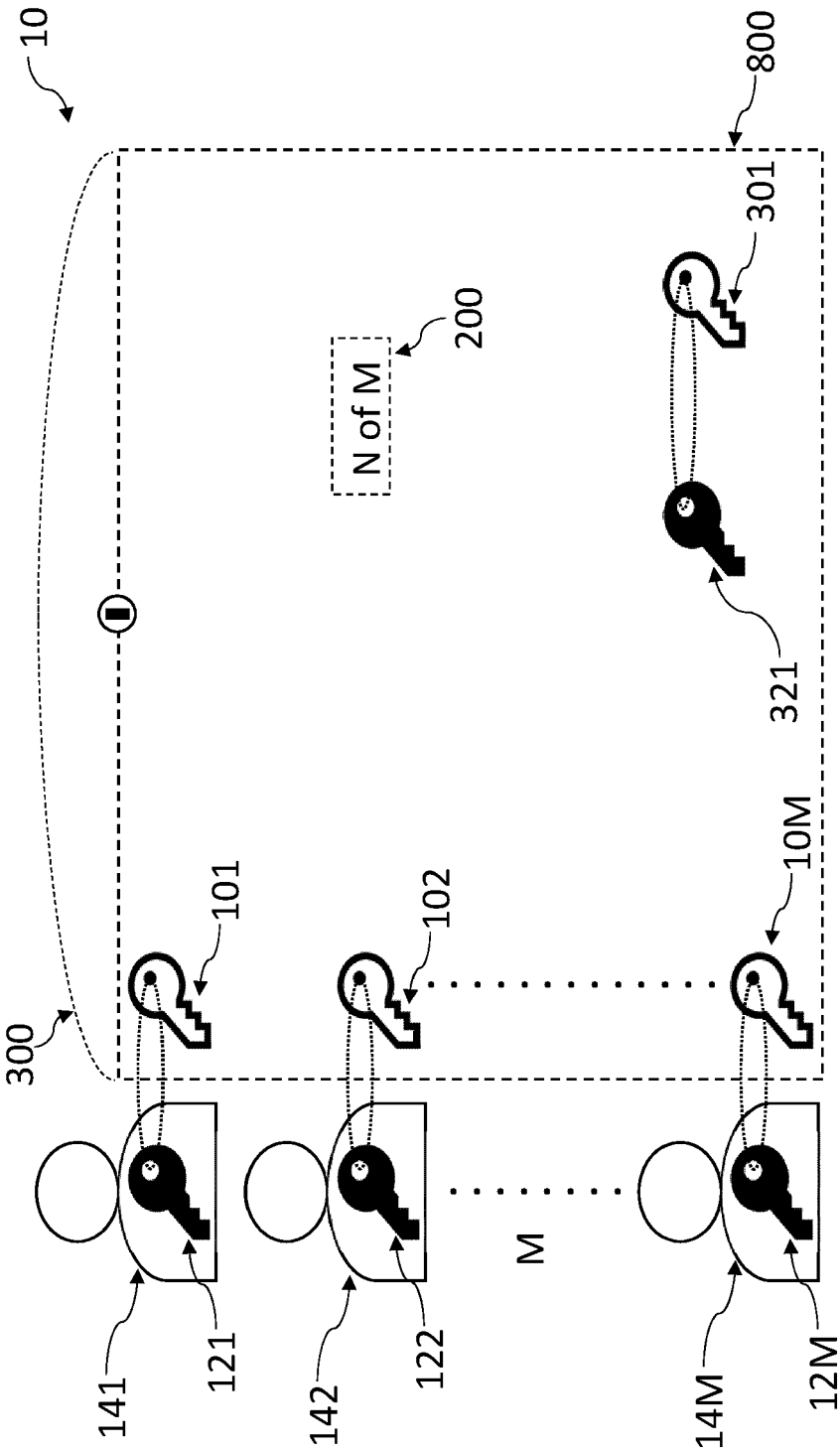

Fig. 1

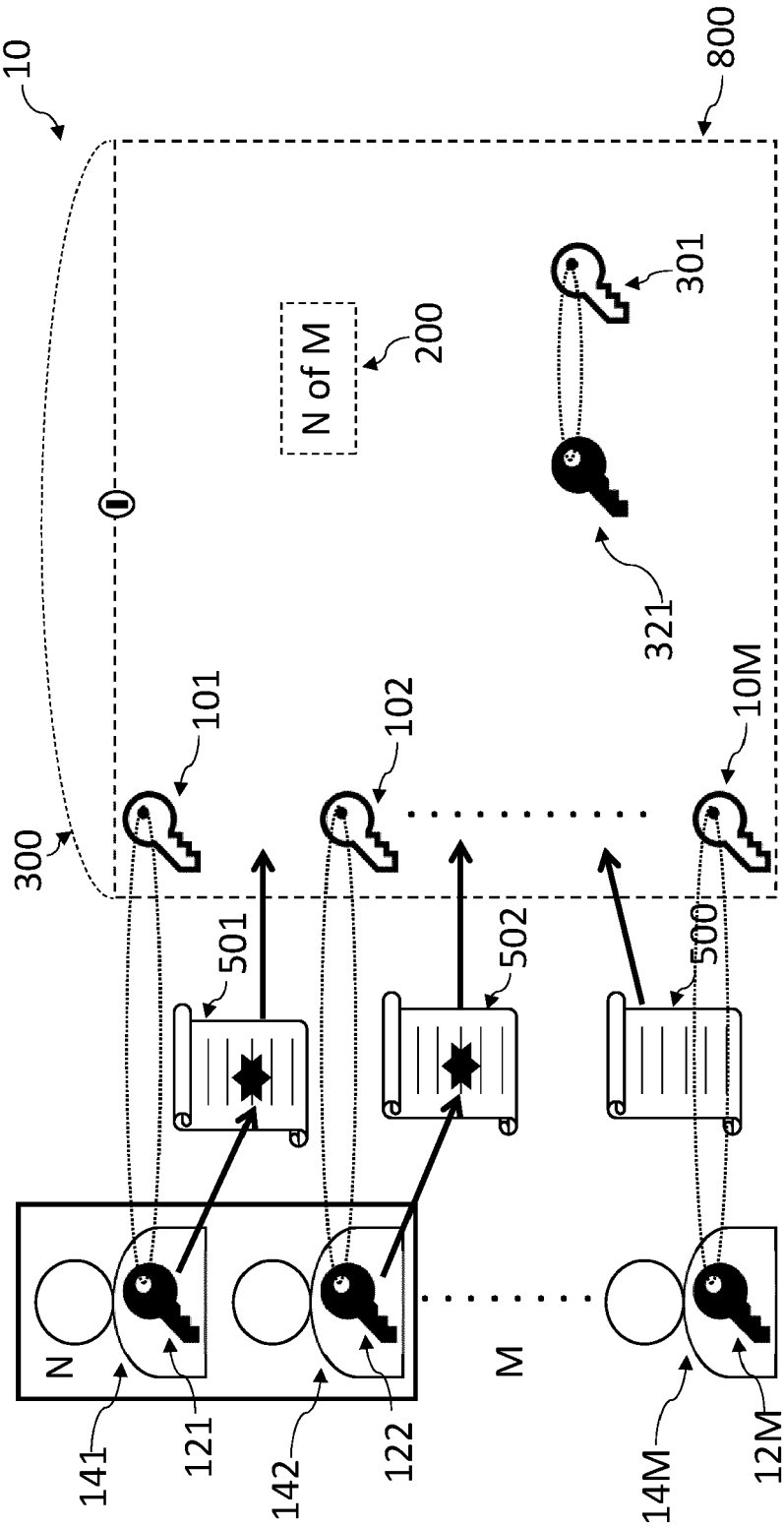
10
800
N of M
200
301
321
101
102
10M
300
501
502
500
N
M
141
121
142
122
14M
12M

Fig. 2

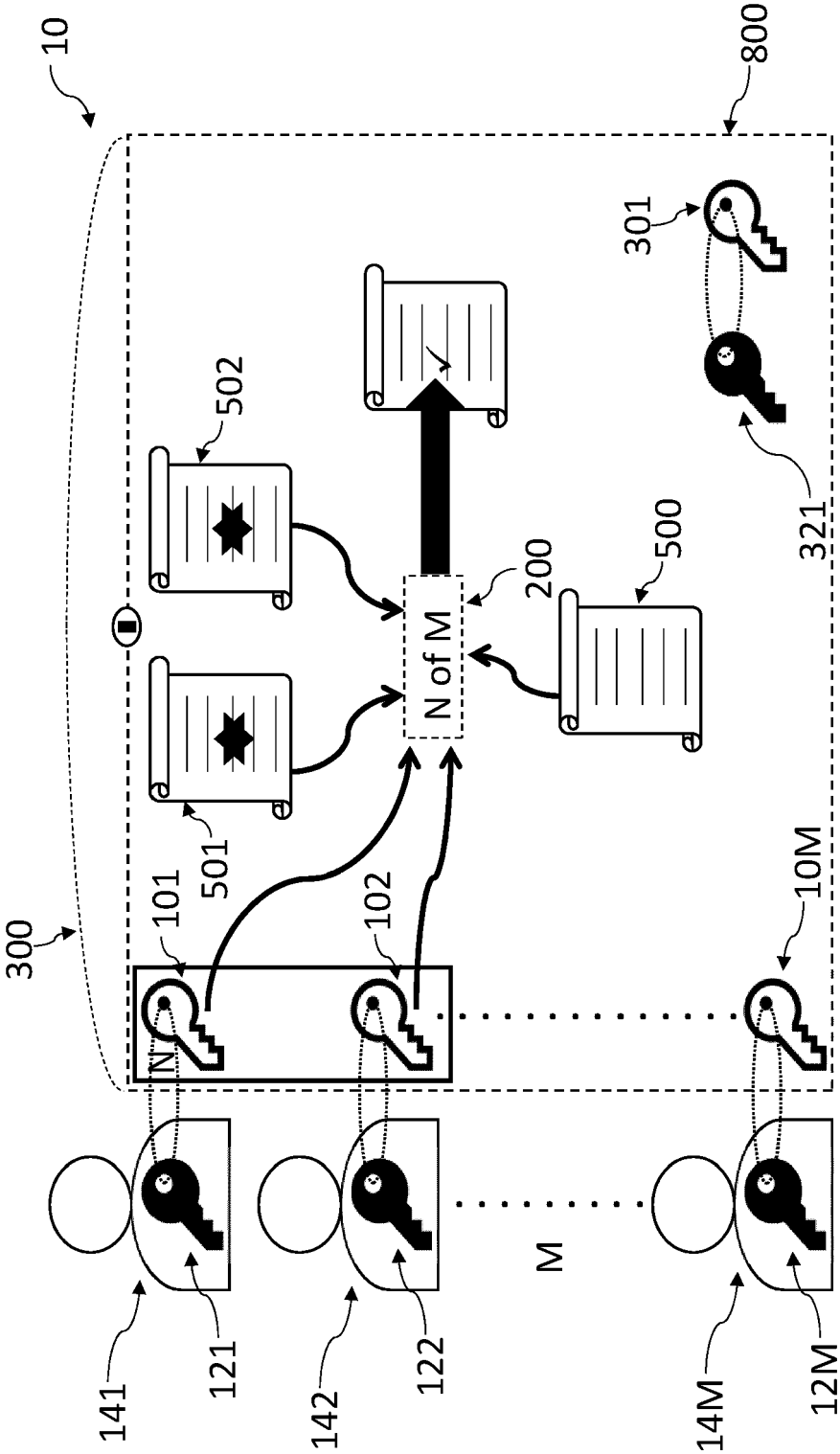
10
800
301
321
502
500
200
N of M
501
101
102
10M
300
N
141
121
142
122
M
14M
12M

Fig. 3

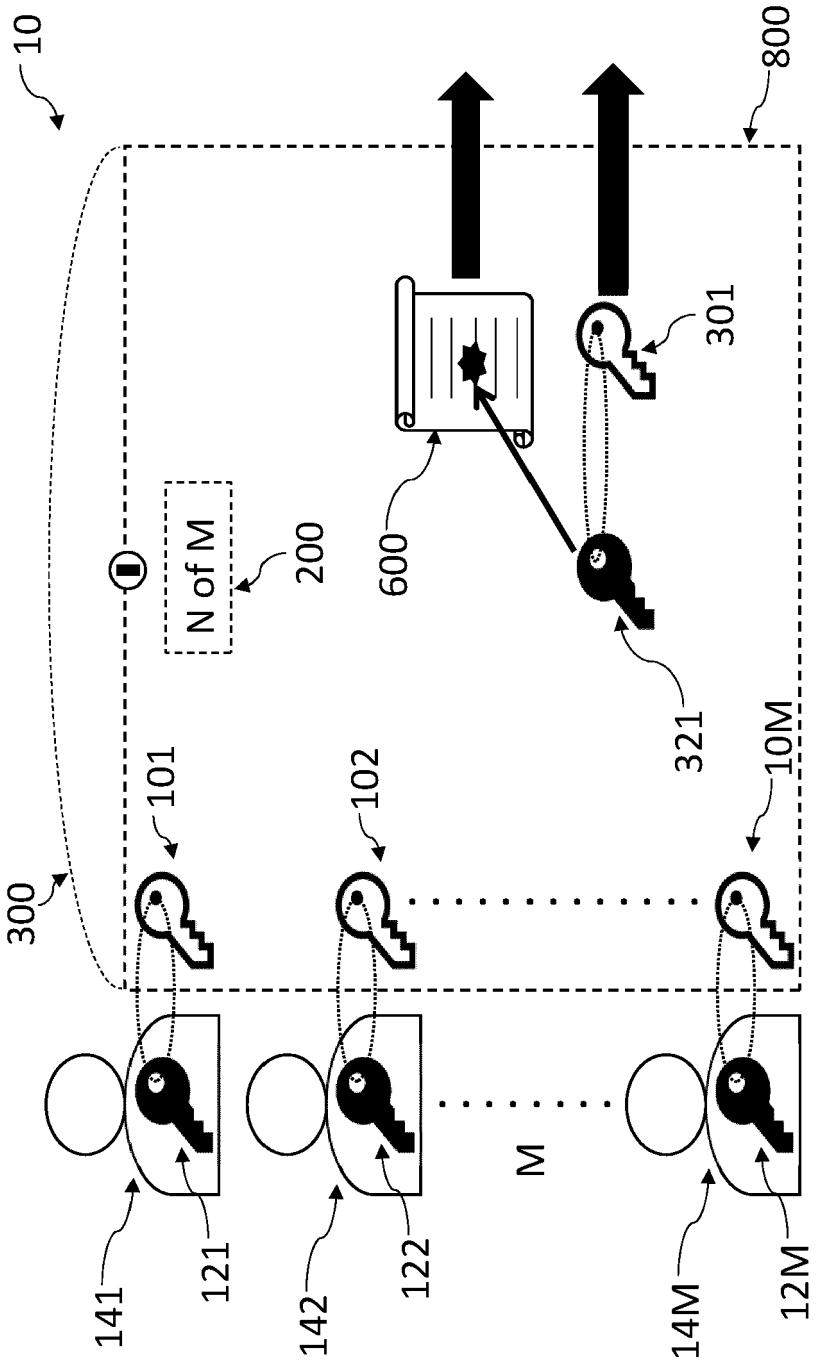
10
800
N of M
200
600
301
321
300
101
102
10M
141
121
142
122
M
14M
12M

Fig. 4

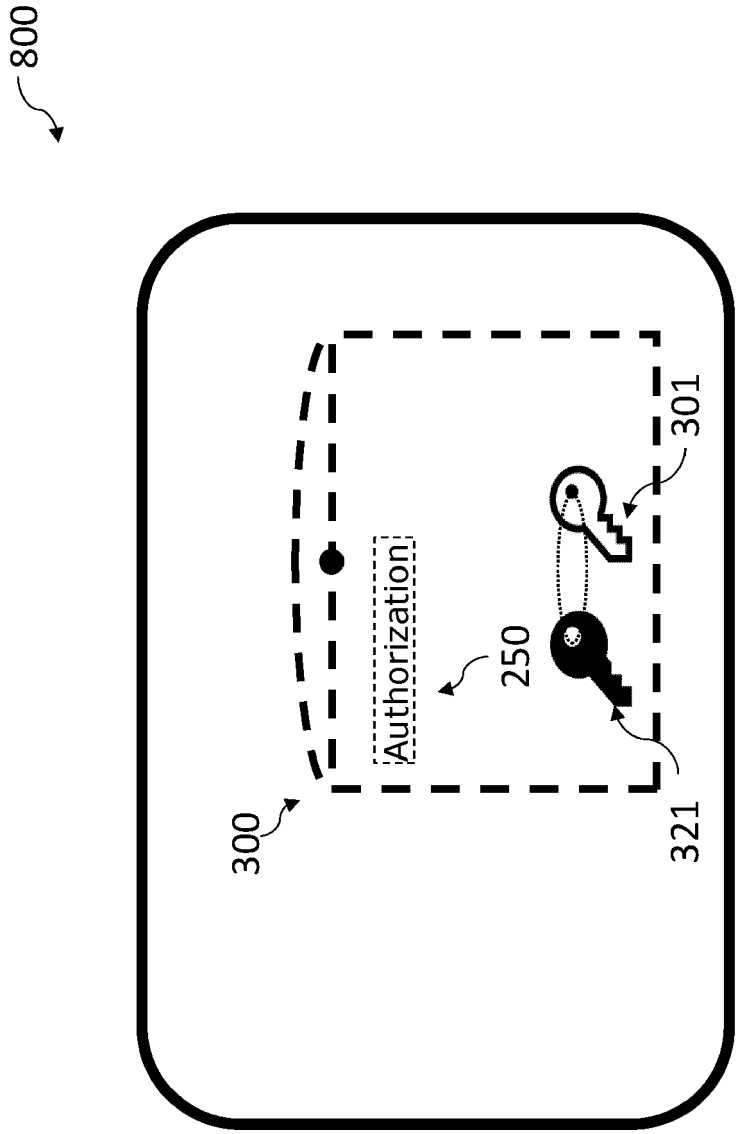

Fig. 5

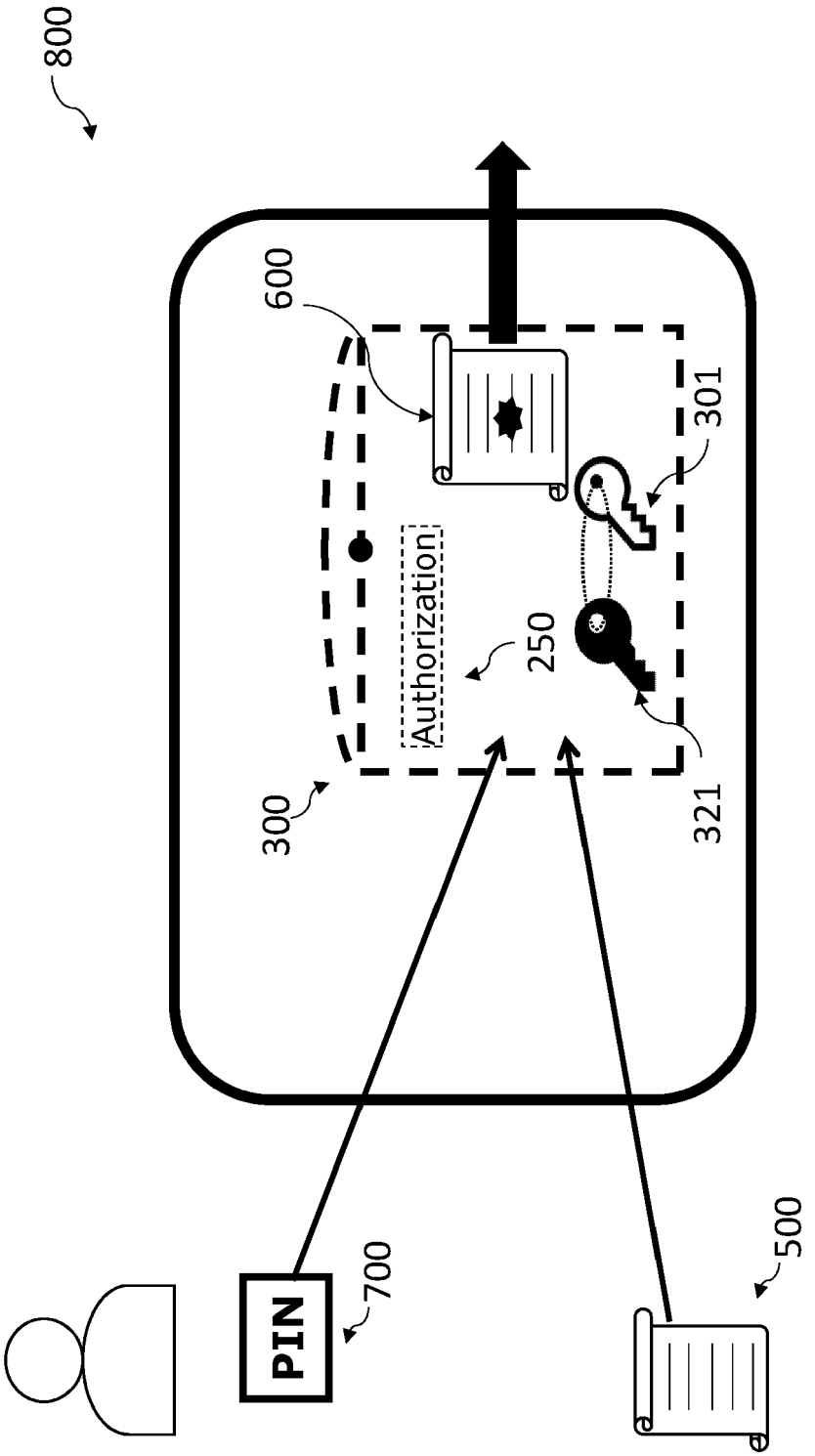

Fig. 6

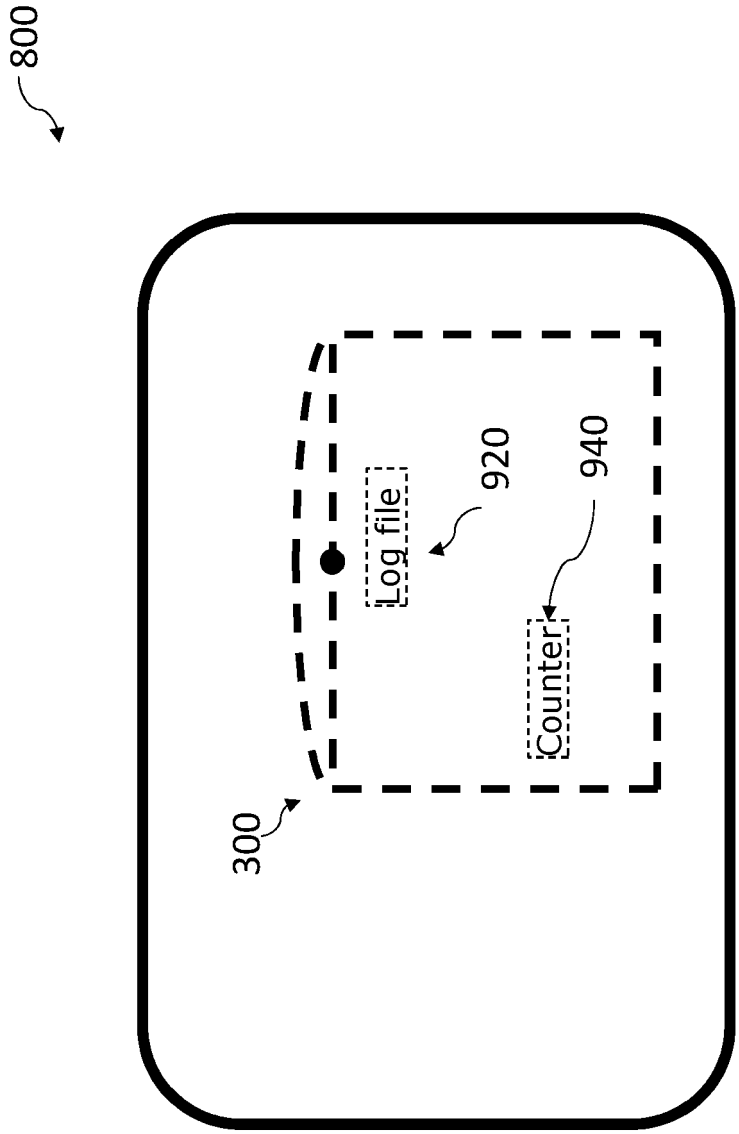

Fig. 7

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 16 3036

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2019/032659 A1 (GRIDPLUS INC [US]) 14 February 2019 (2019-02-14) * paragraph [0015] - paragraph [0158] *	1-15	INV. G06F21/60 G06F21/64 G06F21/77
A	US 2003/014632 A1 (VANSTONE SCOTT A [CA]) 16 January 2003 (2003-01-16) * paragraph [0024] - paragraph [0039] *	1-15	
A	US 2011/247057 A1 (BAENTSCH MICHAEL [CH] ET AL) 6 October 2011 (2011-10-06) * paragraph [0020] - paragraph [0046] *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	1 September 2021	Pinto, Raúl

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 16 3036

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-09-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019032659 A1	14-02-2019	EP 3665863 A1	17-06-2020
		US 2019052461 A1	14-02-2019
		WO 2019032659 A1	14-02-2019
US 2003014632 A1	16-01-2003	CA 2453853 A1	30-01-2003
		EP 1413157 A1	28-04-2004
		EP 2408170 A1	18-01-2012
		JP 2005509334 A	07-04-2005
		JP 2010200381 A	09-09-2010
		US 2003014632 A1	16-01-2003
		US 2007214362 A1	13-09-2007
		WO 03009619 A1	30-01-2003
US 2011247057 A1	06-10-2011	CN 102844763 A	26-12-2012
		EP 2553621 A1	06-02-2013
		TW 201211818 A	16-03-2012
		US 2011247057 A1	06-10-2011
		WO 2011121530 A1	06-10-2011

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82